No. 23-55375

IN THE UNITED STATES COURT OF APPEAL

FOR THE NINTH CIRCUIT

MICHAEL TERPIN, *Plaintiff-Appellant*,

v.

AT&T MOBILITY, LLC, *Defendant-Appellee*.

On Appeal from the United States District Court
for the Central District of California
Case No. 2:18-cv-06975-ODW-KS

APPELLANT'S OPENING BRIEF

FILED PROVISIONALLY UNDER SEAL

Pierce O'Donnell
Timothy J. Toohey
Paul A. Blechner
Emily Avazian
GREENBERG GLUSKER FIELDS
CLAMAN & MACHTINGER LLP
2049 Century Park East, Suite 2600
Los Angeles, California 90067
Telephone: (310) 553-3610
Email: POdonnell@ggfirm.com
TToohey@ggfirm.com
PBlechner@ggfirm.com
EAvazian@ggfirm.com

Attorneys for Plaintiff-Appellant
MICHAEL TERPIN

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

OTHER AUTHORITIES

INTRODUCTION

This appeal presents an issue of first impression arising from a telecommunication carrier's violation of its statutory duty to protect its customers' confidential communications, including private text messages, by knowingly turning over control of a customer's mobile telephone account to thieves. The carrier, Appellee AT&T Mobility, LLC ("AT&T"), did so by conducting an unauthorized "SIM swap" on Appellant Michael Terpin's mobile telephone account, which is a form of identity theft which swaps the subscriber identity module (or "SIM") in a customer's mobile phone to one in a phone under the control of a bad actor.

On January 7, 2018, Jahmil Smith ("Smith"), an employee of an authorized retailer of AT&T, accessed AT&T's account management systems and, without Terpin's permission, transferred control of Terpin's phone number to Ellis Pinsky ("Pinsky"), the teenager hacker. Pinsky then used password reset messages to access Terpin's online accounts and files and to steal almost $24 million worth of cryptocurrency.

AT&T knew that Smith had turned over the accounts of at least two other customers to unauthorized parties within a month prior to Terpin, yet took no steps to ensure that Smith did not hack again. AT&T also knew that its employees had previously allowed thieves to access Terpin's account and steal his cryptocurrency

through a prior June 11, 2017 "SIM swap." Because of that theft, AT&T had promised Terpin expanded or "extra security" on his account to secure his account against being turned over again to unauthorized parties. All of AT&T's promises were knowingly false when made and its vaunted "extra security" was worthless.

The district court erroneously found that, notwithstanding AT&T's clear duties to protect its customers from these types of crimes, including under Section 222 of the Federal Communications Act ("FCA"), AT&T would not be held liable for Terpin's losses. The district court's decisions were wrong and this Court should reverse them in their entirety.

Despite the fact that AT&T's actions were in direct violation of its statutory obligations to protect its customers' confidential proprietary information under Section 222 of the FCA and also violated its promises to Terpin to secure his account, the district court dismissed all of Terpin's claims against AT&T under Fed. R. Civ. Proc. 12(b)(6) and granted summary judgment to AT&T on Terpin's remaining claims. The district court thus left Terpin (and other victims of unauthorized SIM swaps) without any recourse against telecommunication carriers violating customers' statutory rights.

Throughout the almost five-year history of this case, AT&T has refused to acknowledge any responsibility for conducting the unauthorized SIM swaps on Terpin's account. Indeed, AT&T absurdly claims to have had no involvement in

the events that harmed Terpin despite the fact that Pinsky has admitted under oath that without the SIM swap he would not have been able to access Terpin's accounts. AT&T instead has attempted to hide behind unconscionable provisions in its contracts of adhesion and concocted convoluted versions of events that omit its involvement in the unauthorized SIM swaps. If the district court's orders are not reversed by this Court, Terpin will be left without any recourse against AT&T for the losses he suffered for its violating the protection of his confidential communications.

This case is also of wider importance because it relates to the ubiquitous practice of carriers' customers using mobile phones as a means of identification to access online accounts, including through password reset or two-factor authentication (2FA) messages. When a telecommunications behemoth like AT&T fails to protect that gateway and turns control of a customer's mobile phone over to thieves, customers, like Terpin, will predictably suffer disastrous consequences, including financial losses, takeover of social media accounts and identity theft. Therefore, the Court should reverse the district court's grant of summary judgment and its prior dismissal of Appellant's claims for deceit, misrepresentation and punitive damages.

JURISDICTIONAL STATEMENT

Terpin invoked the district court's jurisdiction under 28 U.S.C. § 1331 because the case arose under federal question jurisdiction under the FCA. The district court had supplemental jurisdiction under 28 U.S.C. § 1367 over Appellant's state law claims because the claims were derived from a common nucleus of operative facts. The district court also had jurisdiction over this matter under 28 U.S.C. § 1332 because of diversity of citizenship.

On March 30, 2023, the district court entered judgment for Defendants. 1-ER-1. Terpin filed a timely notice of appeal. *See* Fed. R. App. P. 4(a)(1)(A). This Court has jurisdiction under 28 U.S.C. § 1291.

STATUTORY AND REGULATORY AUTHORITIES

All relevant statutory and/or regulatory authorities, including 47 U.S.C. §§ 206 and 222 and orders and regulations of the Federal Communications Commission ("FCC") appear as exhibits in the Addendum to this brief and are cited in the following form **[vol]-ADD-[page number]**. The Addendum also includes unpublished decisions.

ISSUES PRESENTED

The issues presented in this appeal are as follows:

Whether the district court erred in granting AT&T's motion for summary judgment on Terpin's claim that AT&T violated Section 222(a) of the FCA by disclosing to unauthorized third parties Terpin's confidential proprietary information, including the content of his communications;

Whether the district court erred in granting AT&T's summary judgment motion on Terpin's claim that AT&T violated Section 222(c) of the FCA by disclosing, through the January 7, 2018 unauthorized SIM swap, Terpin's Customer Proprietary Network Information ("CPNI"), including the configuration of his accounts and details of his communications, to unauthorized parties, including Pinsky;

Whether the district court erred in granting AT&T's summary judgment motion on Terpin's claim that AT&T allowed its agent Smith to have unauthorized access to Terpin's CPNI when Smith bypassed AT&T's procedures and improperly authenticated Terpin on AT&T's system, reconfigured Terpin's accounts and transferred control of Terpin's phone account and messages to Pinsky through the January 7, 2018 SIM swap;

Whether the district court erred in granting summary judgment on Terpin's claims for negligence, negligent hiring, and negligent supervision and retention by

finding that the economic loss rule in *Sheen v. Wells Fargo*, 12 Cal. 5th 905, 943 (2022) ("*Sheen*") barred these claims despite the fact that AT&T had a duty to Terpin "independent of the contract arising from principles of tort law," including AT&T's statutory duties under FCA Section 222, the CPNI Rules, and its 2015 AT&T consent decree with the FCC;

Whether the district court erred in finding on summary judgment that the economic loss rule in *Sheen* is applicable to the AT&T Wireless Customer Agreement ("WCA") despite the fact that the WCA is an unconscionable and unenforceable contract of adhesion that Terpin had no power to negotiate;

Whether the district court erred in finding on summary judgment that Terpin's breach of contract claim, including AT&T's promise of extra security after his June 11, 2017 unauthorized SIM swap, was barred by the limitation of damages provision in the WCA despite the fact that AT&T contemporaneously knew that its promises to Terpin regarding security were false because its security could not prevent financial losses to its customers through unauthorized SIM swaps;

Whether the district court erred in finding that Terpin could not bring claims for consequential or special damages under his claim for breach of contract for AT&T's breaches of its promises to provide extra security on Terpin's account because of the limitation of damages provision in the WCA, despite the fact that

AT&T knew at the time it made those promises that Terpin had suffered such damages, including financial losses resulting from his June 11, 2017 unauthorized SIM swap;

Whether the district court erred in dismissing Terpin's claim for declaratory relief because there was still a live controversy between the parties and Terpin's claims were not moot;

Whether there are triable disputed material facts regarding the foreseeability of the harm resulting from Terpin's January 7, 2018 unauthorized SIM swap and the fact that such damages were proximately caused by the SIM swap so as to preclude summary judgment on that ground for AT&T on any of Terpin's claims;

Whether the district court incorrectly dismissed with prejudice Terpin's claim for deceit by concealment with prejudice by disregarding Terpin's allegations that AT&T had a duty to disclose material facts to Terpin regarding the inadequacy of AT&T's security and by also disregarding his allegations that AT&T engaged in active concealment of material facts regarding its security;

Whether the district court erred in dismissing with prejudice Terpin's claim for intentional misrepresentation against AT&T for its false or misleading statements regarding the security of Terpin's account that AT&T made with no intention to perform, including AT&T's promise that it would place "extra security" on Terpin's account to prevent future account takeovers; and

Whether the district court erred in dismissing Terpin's request for punitive damages by using a heightened pleading standard for allegations concerning the conduct of corporate officers, directors and managing agents that is inconsistent with the pleading standards of the Federal Rules of Civil Procedure.

STATEMENT OF THE CASE

I. FACTUAL SUMMARY[1]

A. SIMS and "SIM Swapping."

A "SIM" or "subscriber identity module" is a microchip that connects a specific phone to a cellular network. 9-ER-1599-1600 (Undisputed Facts 1-3). Unauthorized SIM swapping is a form of identity theft that occurs when a mobile telephone carrier associates a user's phone number with another phone in the possession of an unauthorized third party (such as a bad actor or thief) through transfer of a customer's "SIM" to the bad actor's phone. 2-ER-121-130 (AT&T Sept. 27, 2017 Cyber Aware Blog ("AT&T Blog")). As AT&T recognized in its September 27, 2017 Cyber Aware Blog (prior to Terpin's second SIM swap), once

---

[1] In opposition to AT&T's motion to summary judgment, Terpin filed a Statement of Genuine Disputes of Material Fact and Conclusions of Law ("Statement") containing 172 material disputed facts and referencing 50 exhibits in support of such facts, including excerpts from depositions. Almost all the facts in the statement were referenced in Terpin's opposition to the motion for summary judgment. *See* district court docket ("Dkt-") 133, 8-ER-1570-96; 4-ER-496-673 (redacted version of Statement); 9-ER-1598-1775 (unredacted version filed under seal in district court). Volumes 2 and 3 of the ER contain the unredacted exhibits in support of the Statement; the exhibits filed under seal with the district court are in Volume 10 of the ER. Appellant is concurrently filing with the Court a Notice of Intent to Unseal all documents filed under seal in the district court and filed provisionally under seal in this Court, including portions of this brief referencing sealed documents.

a SIM swap occurs, "the mobile network will start sending calls and texts to the new SIM card—which is really the thief's phone." 2-ER-124. This not only deactivates the phone of the legitimate user, but allows the thief to get a user's "calls and texts on his device, including authentication texts, one-time PINS or phone responses." *Id.* This in turn allows the thief "to gain access to [a legitimate user's] financial or social media accounts." *Id.* As the FCC has recognized, bad actors use SIM swaps to intercept text messages to "steal our identities and our money and take control of our digital lives." *See In the Matter of Protecting Consumers from SIM Swap and Port Out Fraud*, 36 FCC Rcd.. 14120 (2021), 3-ADD-542.

B. Terpin's June 2017 SIM Swap.

On June 11, 2017, Terpin suffered an unauthorized SIM swap on his AT&T mobile account ("June 2017 SIM Swap"). 9-ER-1658-59 (PF-26-28)[2]. The June 2017 SIM Swap occurred through social engineering when an AT&T employee through social engineering gave someone Terpin's e-mail address. *Id.*; 10-ER-1913, 1917-20 (Terpin AT&T account notes (hereinafter, "Account Notes")).

---

[2] References to the individual facts in the Statement follow the format used in Terpin's opposition to the summary judgment motion in regard to "Plaintiff's Facts" (Dkt-233): **"PF-##"** (Plaintiff's Facts). The ER location is given for exhibits referenced in the Statement.

Terpin promptly complained of fraud to AT&T, including informing it that his Skype (Microsoft) account had been compromised and that he had lost cryptocurrency due to the June 2017 SIM Swap. 9-ER-1659-1660 (PF-29-30,32-33), 10-ER-1916-17 (Account Notes) and 2-ER-235-38 (Terpin responses to interrogatories 3-4).

On June 13, 2007, Terpin met with AT&T representatives to express his concerns regarding the security of his AT&T account. At that meeting, AT&T offered him "celebrity" or "extra" security—an upgrade from a four-digit to a six-digit code that Terpin was told could not be changed by anyone other than himself (hereinafter, "extra security"). 9-ER-1660-64 (PF-33-43), 4-ER-684-87 (Terpin Decl. ¶ 4). AT&T promised that their "extra security" would be required to make account changes, including swapping his SIM to another phone. 9-ER-1661 (PF-35), 4-ER-685 (Terpin Decl. ¶¶ 2-4). AT&T placed the "extra security" on Terpin's account, adding a "special instruction" displayed in Terpin's account in red that AT&T was not to validate Terpin unless he came into a store. 9-ER-1661-62 (PF-36-37), 10-ER-1915 (Account Notes).

Terpin's account was referred to AT&T's fraud department which placed a "fraud note" on the account. 9-ER-1663 (PF-38, 40), 10-ER-1915 (Account Notes). Terpin accepted and believed AT&T's promises that his account would be protected against future unauthorized SIM swaps because of the "extra security"

and Terpin remained an AT&T customer based on those promises. 9-ER-1663-64 (PF-39, 41-43), 4-ER-685 (Terpin Decl. ¶¶ 2-4). AT&T's promises were consistent with AT&T's blog post to customers that the best way to protect themselves against unauthorized SIM swaps was to place "extra security" on their accounts. 9-ER-1664 (PF-44), 2-ER-124 (AT&T Blog).

C. Terpin's January 7, 2018 Unauthorized SIM Swap

On January 7, 2018, Smith, working alone at AT&T's Norwich store, committed the January 2018 SIM swap of Terpin's account. 9-ER-1720-1726, 9-ER-1743-1746 (PF-134-140,154-158). Smith used AT&T's OPUS system to access Terpin's account and conduct the SIM swap. 9-ER-24 (PF-136), 10-ER-1897 (Account Notes), 10-ER-1794-95, 1798-99 (Hill Dep.)[3]. Because AT&T had authentication procedures in place to identify customers making account changes, it may be inferred for purposes of summary judgment that Smith viewed Terpin's CPNI and other confidential information when he improperly accessed Terpin's account. Smith did not follow AT&T's "M&Ps" or authentication procedures, which AT&T had acknowledged were ineffective. Instead, Smith bypassed a scan of Terpin's driver's license (who was not in the store but at his home in Nevada),

[3] "Dep." references are to ER cites containing excerpts of deposition with the name of the deponent.

and "validated" him with the last 4 digits of the SSN, using the access to Terpin's account via AT&T's system to transfer the SIM for Terpin's account as requested by Pinsky. 9-ER-1724-25 (PF-137-139), 10-ER-1897 (Account Notes). The SIM transferred by Smith was immediately active in an iPhone controlled by Pinsky's "holder" in Lake Charles, Louisiana. 9-ER-1725-27, 9-ER-1743, 1746 (PF-140-141,153,159), 10-ER-1896 (Account Notes), 10-ER-1794-95 (Hill Dep.), 10-ER-1931, 1936-41 (Call Detail), 10-ER-1993 (SIM spreadsheet), 2-ER-92, 94, 101 (Pinsky Dep.)

After the SIM swap, Terpin's wife, Maxine Hopkinson, attempted repeatedly to get AT&T to reverse the SIM swap and transfer the number back to Terpin's device. She was transferred to AT&T's fraud department, which twice did not pick up her calls. 9-ER-1727-1738 (PF-142-145), 2-ER-55-71 (Hopkinson Dep). Incredibly, even though Terpin's account was previously noted for fraud and Ms. Hopkinson complained about "fraud issues," 9-ER-1736-41 (PF-143-150), AT&T never investigated the January 2018 SIM Swap. 9-ER-1741-43 (PF-151-152). *See also* 2-ER-55-71 (Hopkinson Dep.), 10-ER-1894-95 (Account Notes), 10-ER-1805-07 (Morella Dep.).

Shortly after the SIM for Terpin's account was transferred to Pinsky's "holder," the perpetrators changed the password for Terpin's Microsoft account. 9-ER-1757-58 (PF-168), 10-ER-1897 (Account Notes), 2-ER-179-182 (password

changes), 2-ER-117-18 (Pinsky Dep.). This password reset via the January 2018 SIM Swap allowed the perpetrators to access Terpin's Microsoft account. 9-ER-PF-162-166. AT&T's records corroborate Pinsky's testimony. 9-ER-1743 (PF-153), 10-ER-1938 (Call Detail).

Pinsky confirmed the details of the January 2018 SIM Swap and that he and others performed the SIM swap and theft. 9-ER-1743-1761 (PF-154-172), 2-ER-92-96, 98-103, 110-112, 114-118 (Pinsky Dep.). A critical step in the SIM swap was Pinsky contacting Smith, who received a payment of between $100 and $500. 9-ER-1745-46 (PF-156-158), 2-ER-93-96 (Pinsky Dep.). Having obtained access to Terpin's accounts through password reset messages which he used to change Terpin's passwords, Pinsky searched and eventually found a file in the trash of Terpin's Microsoft online account to access Terpin's cryptocurrency accounts. 9-ER-1746-52 (PF-161-163), 2-ER-90, 95-98 (Pinsky Dep.). Pinsky used this information to steal cryptocurrency then worth roughly $24 million. 9-ER-1752-54 (PF-164), 2-ER-100-102, 110-111, 114, 116 (Pinsky Dep.). Pinsky testified that he would not have been able to access Terpin's cryptocurrency accounts without the January 2018 SIM Swap because he had no way to access Terpin's Microsoft accounts. 9-ER-1754-46 (PF-165-166), 2-ER-101-102, 111-113 (Pinsky Dep.).

D. Harm to AT&T Customers such as Terpin from Increased SIM Swap Activity Was Foreseeable to AT&T.

AT&T never disclosed to Terpin before the January 7, 2018 SIM swap that it knew the "extra security" it promised would not protect his account, that it knew it was experiencing increased SIM swap activity, and that it knew such activity was resulting in financial losses even to AT&T customers who had elected "extra security" protection because employees were bypassing such protections. Thus, long before the January 7, 2018 unauthorized SIM swap of Terpin's account, AT&T had substantial knowledge about how SIM swaps were occurring and how they were harming customers financially.

AT&T knew the following before January 7, 2018:

- By January 2016, AT&T knew that unauthorized SIM swaps occurred on customers' accounts due to compromised authentication credentials. 9-ER-1665-66 (PF-46-47) 10-ER-1833, 1855 (7/26/17 and 1/21/16 AT&T e-mails);
- By May 2016, AT&T knew that its authorized retailers (ARs)[4] were bypassing "extra security," even when customers had such protection.

[4] "Authorized retailers" are third party vendors with exclusive agreements to sell AT&T services and equipment. 9-ER-1884 (PF-87) and 10-ER-1798-99 (Hill Dep.). Two examples of ARs are Spring Communications ("Spring"), whose

9-ER-166 (PF-47-48), 10-ER-1833, 1849 (1/21/16 and 5/26/16 AT&T e-mail);

- By March 2017, AT&T recognized that it had no "systematic" means of preventing unauthorized SIM swaps, and that its written methods and procedures, or "M&Ps" were not preventing fraud. 9-ER-1666-67 (PF-49); 10-ER-1942, 1844 (3/27/16 and 3/27/17 AT&T e-mails). *See also* 9-ER-1672-74 (PF-62-64), 2-ER-183 (AT&T My CSP Article), 10-ER-1874 (1/11/18 AT&T e-mail); and
- By December 2017, the head of AT&T's fraud department noted that AT&T's approach to authentication was "fragmented" and "fraud prone" and that customers were subject to fraud because of "lack of compliance by store personnel" or "lack of training." 9-ER-1674-75 (PF-65-68), 10-ER-1840-48, 10-ER-1862 (12/13/17 AT&T e-mail and attachment; fraud department presentation).

---

employee Smith performed the January 2018 SIM Swap, and Spring's successor Prime Communications ("Prime"). 9-ER-1685-86 (PF-88) and 10-ER-1789-90 (Hill Dep.). AR employees use AT&T's systems (like OPUS), display AT&T logos on their stores, sell only AT&T products and are indistinguishable from AT&T owned and operated stores. 9-ER-1687-93 (PF-90-92) and 10-ER-1787, 1796 (Hill Dep.). AR employees are supposedly required to follow AT&T procedures in authenticating customers. 9-ER-1693 (PF-92) and 10-ER-1800 (Hill Dep.).

AT&T also knew that unauthorized SIM swaps were causing financial harm to customers through irreversible wire transfers, including its agents validating customers only by using the last four digits of a social security number ("SSN") and ignoring the "extra security" on customers' accounts. 9-ER-1676 (PF 70) and 10-ER-2004 (5/5/17 AT&T e-mail).

Well before the January 2018 SIM Swap, AT&T also knew or should have known that unauthorized SIM swaps were targeting cryptocurrency holders because thefts of cryptocurrency were irreversible. Indeed, AT&T was obligated to track such emerging fraud by a 2015 consent decree with the FCC, which required AT&T to pay a $25 million fine and implement an "Information Security Program" to both "identify and respond to emerging risks or threats" to its customers' privacy. (PF-8-14) *citing In the Matter of AT&T Inc.: Notice of Apparent Liability for Forfeiture and Admonishment* (Feb. 28, 2020), FCC 20-26, ("AT&T Consent Decree"), 2-ADD-494-535.

AT&T also must have known that regulatory agencies, including the FTC, had warned consumers against losses from unauthorized SIM swaps. 9-ER-1667-68 (PF-50-52), 2-ER-131-40 (N.Y. state and FTC warnings) and that a December 12, 2016 *Forbes* article highlighted that SIM swaps led to thefts of cryptocurrency from customers and that carriers were being blamed for not safekeeping their customers' telephone numbers. 9-ER-1668-69 (PF-53-56) and 2-ER-145 (*Forbes*

article). *See also* 2-ER-141, 190 (August 21, 2017 *New York Times* and September 28, 2017 Revision/Legal articles, regarding thefts of cryptocurrency through SIM swaps).

On September 27, 2017, AT&T through its Cyber Aware Blog warned its customers about what they should know about "SIM Swap Scams." 9-ER-1677 (PF-73), 2-ER-122 (AT&T Blog). AT&T detailed how a "thief" will convince a service provider to replace a victim's SIM which will have the effect of "the mobile network . . . sending calls and texts to the new SIM card—which is really the thief's phone," after which the victim's phone is deactivated and "the thief may be able to gain access to your financial or social media accounts." 9-ER-1676 (PF-74-75), 2-ER-124 (AT&T Blog). AT&T warned that this "could happen to anyone." 9-ER-1679 (PF-76), 2-ER-126 (AT&T Blog). AT&T's chief recommendation to customers to protect themselves was to add "extra security" to their accounts—a PIN that the customer must provide "before any significant [account] changes can be made." 9-ER-1679 (PF-77), 2-ER-126 (AT&T Blog).

The problem of unauthorized SIM swaps (which AT&T knew had grown 140% by mid-2017) was exacerbated both by the proliferation of personal information to the dark web caused by the 2017 Equifax breach (such as SSNs which could be used by perpetrators of fraud) and the rise of cryptocurrency. 9-ER-1677, 1679-81 (PF-72,78-81), 10-ER-1953, 1945-52 (7/17 Fraud Review,

10/3/17 AT&T e-mail). Indeed, in 2017, cryptocurrency had "joined the global financial system" and had a market capitalization of $100.1 billion dollars. 9-ER-1681 (PF-80-81) and 3-ER-483-94 (articles on growth of cryptocurrency). And, consistent with what AT&T was seeing and what was being publicly reported, the chief perpetrator of the January 2018 SIM Swap—Pinsky—became aware of and began SIM swapping for the purpose of stealing cryptocurrency in 2017. 9-ER-1682-85 (PF-82-85) and 2-ER-105-109 (Pinsky Dep.).

E. Smith's December 2017 Unauthorized SIM Swaps.

Foreshadowing what would occur to Terpin during the January 2018 SIM Swap, Smith, the Spring employee at an AT&T branded store in Norwich, Connecticut who conducted Terpin's SIM swap, conducted at least two unauthorized SIM swaps involving other customers on December 9, 2017 (the "Prior Smith SIM Swaps"). 9-ER-1693-1711 (PF-93-118).

AT&T received calls from the two customers SIM swapped by Smith on December 9 and 12, 2017. 9-ER-1694 (PF-94), 10-ER-1991 (SIM swap calls). Under AT&T's policies, this should have triggered an investigation by AT&T's fraud or asset protection departments. 9-ER-1694 (PF-95), 10-ER-1827 (Morella Dep.). Yet, AT&T did not refer either of the Prior Smith SIM Swaps to its fraud department, investigate them, or refer the SIM swaps to Smith's employer Spring.

9-ER-1696-1707 (PF-99-111), 10-ER-1808, 1813-22, 1824, 1828-29 (Morella Dep.); 2-ER-252 (AT&T interrogatory response); 2-ER-78-80 (Prime Dep.).

AT&T has admitted that if the incidents had been referred and investigated, AT&T "wouldn't have allowed [Smith's] access to [AT&T's] system to remain." 9-ER-1701-02 (PF-106-107, 10-ER-1821 (Morella Dep.). Instead, Smith was allowed to continue working in AT&T's Norwich store without other employees or supervisors being present both during and after the January 2018 SIM Swap. 9-ER-1707-09 (PF-113-115), 2-ER-77, 81-83 (Prime Dep.), 10-ER-1812 (Morella Dep.); 2-ER-195-98 (Spring documents re Smith).

A few weeks after the Prior Smith SIM Swaps, a Norwich Police Department report reveals that Smith (while working alone) reported a robbery in the AT&T branded store on January 1, 2018, with the Spring regional manager detailing the cash and inventory losses. It was suspected that the robbery was an inside job. 9-ER-1713-15 (PF-119-127), 2-ER-199 (Norwich police report), 2-ER-76, 88 (Prime Dep.). Smith subsequently acknowledged his involvement, was arrested and charged, and made restitution payments to AT&T in 2021. 9-ER-1715-16 (PF-127-130). Spring did not inform AT&T about Smith's January 1, 2018 robbery. 9-ER-1717-19 (PF-131), 10-ER-1812-13 (Morella Dep.).

Despite the Prior Smith SIM Swaps and Spring's immediately stated concerns about Smith's involvement in the January 1, 2018 robbery, AT&T did not

revoke Smith's access to its computer system, Spring imposed no restrictions on Smith, and Smith continued to process SIM swaps, including Terpin's January SIM Swap. 9-ER-1720-21, 1708-09 (PF-132-133,114-115).

II. PROCEDURAL HISTORY

Terpin filed his initial complaint in the United States District Court for the Central District of California ("District Court") on August 15, 2018 against AT&T Inc. and AT&T Mobility, LLC. 8-ER-1418-1569.

On August 23, 2018, Terpin dismissed AT&T Inc. as a defendant. Dkt-9. On October 22, 2018 the remaining defendant, AT&T Mobility, LLC ("AT&T"), moved to dismiss the complaint and strike portions of the complaint. Dkt-14-15.

After two motions to dismiss were granted in part with leave to amend, Terpin filed the operative Second Amended Complaint ("SAC") on March 16, 2020. 6-ER-999-1191. The SAC contained eight claims for (1) Declaratory Relief; (2) Violation of Section 222 of the FCA; (3) Deceit by Concealment; (4) Misrepresentation; (5) Negligence; (6) Negligent Supervision and Training; (7) Negligent Hiring; and (8) Breach of Contract. AT&T moved to dismiss the SAC on March 31, 2020. Dkt-43. On September 8, 2020 the district court granted in part and denied in part AT&T's motion to dismiss. 1-ER-26-39. The district court dismissed Claim 3 for deceit by concealment and Claim 4 for misrepresentation with prejudice. *Id*. The court also dismissed Terpin's claim for punitive damages

without leave to amend but subject to Terpin's motion to add a request for punitive damages no later than twenty-one days after the discovery cutoff. *Id*. This appeal encompasses the district court's dismissal of Claims 3-4 and its dismissal of his request for punitive damages in the SAC.

AT&T answered the SAC on September 23, 2020. Dkt-50.

On December 16, 2020 AT&T moved for summary judgment on all the remaining six claims in the SAC. Dkt-140. Because of the parties' confidentiality designations, the district court granted requests to file certain documents under seal. 4-ER-674; 6-ER-974. On March 30, 2023 the district court granted AT&T's motion as to the remaining six claims in a sealed opinion. 1-ER-6. The district court did not reach AT&T's proximate cause argument because it dismissed the six claims on other grounds. *Id.* The Judgment was issued on April 4, 2023. 1-ER-2. The summary judgment order was unsealed on April 10, 2023. Dkt-247. The Notice of Appeal from the Judgment was filed on April 19, 2023. Dkt-248.

This appeal encompasses the district court's grant of summary judgment as to Terpin's claims for declaratory relief, violation of Section 222 of the FCA, negligence, negligent supervision and training, negligent hiring and breach of contract in the SAC. It also addresses AT&T's argument in the motion for summary judgment that the entire SAC should be dismissed because Terpin has

not properly alleged that his losses were proximately caused by the January 7, 2018 unauthorized SIM swap.

SUMMARY OF THE ARGUMENT

A. The Court should reverse the district court's March 30, 2023 grant of summary judgment pursuant to Fed. R. Civ. Proc. 56(a) on the six claims for relief in Terpin's Second Amended Complaint ("SAC").

1. The district court erred in granting summary judgment to AT&T on the grounds that the customer privacy provision of the FCA, 47 U.S.C. § 222(a) was not implicated when Smith accessed Terpin's account protected by AT&T's authentication procedures and "extra security" and processed the unauthorized SIM swap to divert future calls and texts to a different phone and when AT&T disclosed to unauthorized parties, including Pinsky, Terpin's proprietary information through its January 7, 2018 unauthorized SIM swap, including the content of password reset messages for Terpin accounts.

2. The district court erred in granting summary judgment to AT&T by finding that AT&T did not disclose Terpin's CPNI protected by 47 U.S.C. § 222(c) on January 7, 2018 to unauthorized parties, including Smith and Pinsky, through an unauthorized SIM swap on Terpin's authentication-protected account, because the information disclosed by AT&T related to the quantity, technical configuration, type, destination and location of Terpin's AT&T telecommunication service.

3. The district court erred in granting summary judgment to AT&T on Terpin's three negligence claims on the basis of the economic loss rule in *Sheen* because AT&T had a duty independent of its contract with Terpin under Section 222 of the FCA, the CPNI Rules, and the AT&T Consent Decree to protect Terpin's proprietary information and CPNI from disclosure to unauthorized parties.

4. The district court erred in granting summary judgment in AT&T's favor on Terpin's three negligence claims on the basis of the economic loss rule in *Sheen* because Terpin's contract with AT&T was an unconscionable and unenforceable contract of adhesion that Terpin had no power to negotiate and through which AT&T sought to exculpate itself from any liability to customers.

5. The district court erred in granting summary judgment in AT&T's favor on Terpin's breach of contract claim on the grounds that consequential or special damages are barred by the WCA because the district court ignored material disputed facts demonstrating that Terpin is seeking damages contemplated by AT&T's agreements, including AT&T's promise in June 2017 after his first unauthorized SIM swap that it would implement "extra security" to prevent future takeovers of Terpin's mobile phone account.

6. The district court erred in granting summary judgment in AT&T's favor on Terpin's breach of contract claims because the exculpatory

provision in AT&T's WCA is substantively unconscionable and unenforceable under California law because it seeks to absolve AT&T of all liability for any misconduct, including willful conduct and statutory violations.

7. The district court erred in granting summary judgment in AT&T's favor and dismissing Terpin's declaratory relief claim because the claim is not moot because the district court improperly granted AT&T's motion for summary judgment on Terpin's other claims.

8. Although the district court did not reach the claim, material disputed facts prevent granting summary judgment in favor of AT&T on the grounds that all of Terpin's claims in the SAC are barred on proximate cause grounds, because material disputed facts show that AT&T knew that unauthorized SIM swaps were causing economic losses to its customers, that its agents were bypassing its authentication and security procedures, including "extra security," that AT&T knew or should have known that customers were suffering cryptocurrency and other financial losses due to unauthorized SIM swaps, and because Terpin's losses were the direct and predictable result of the January 7, 2018 unauthorized SIM swap.

B. The Court should reverse the September 8, 2020 dismissal by the district court under Fed. R. Civ. Proc 12(b)(6) of Terpin's claims for deceit and misrepresentation and his request for punitive damages.

1. The district court erred in dismissing with prejudice Terpin's claim for deceit because Terpin properly pleaded that AT&T had exclusive knowledge of its security practices, which it actively concealed from Terpin when it promised and purported to implement "extra security" on his AT&T account after his initial unauthorized SIM swap on June 11, 2017.

2. The district court erred in dismissing with prejudice Terpin's claim for deliberate misrepresentation of AT&T's promises for future performance without intent to perform because Terpin properly pleaded that AT&T made promises to him after his initial unauthorized SIM swap on June 11, 2017 regarding "extra security" on his AT&T account that it had no intention of fulfilling because it knew that such security was ineffective.

3. The district court erred in dismissing Terpin's request for punitive damages because it applied a heightened pleading standard for averments of intent and malice by corporate officers, directors and managing agents that is inconsistent with the requirements of the Federal Rules of Civil Procedure.

STANDARD OF REVIEW

This Court reviews "de novo a district court's order granting a motion to dismiss under Rule 12(b)(6)." *Coal. to Defend Affirmative Action v. Brown*, 674 F.3d 1128, 1133 (9th Cir. 2012). "Dismissal without leave to amend is improper unless it is clear, upon de novo review, that the complaint could not be saved by any amendment." *Polich v. Burlington N. Inc.*, 942 F.2d 1467, 1472 (9th Cir. 1991). "A complaint should not be dismissed under this rule 'unless it appears beyond doubt that plaintiff can prove no set of facts in support of his claim which would entitle him to relief.'" *Baker v. McNeil Island Corrections Center*, 859 F.2d 124, 127 (9th Cir. 1988), quoting *Conley v. Gibson*, 355 U.S. 41, 45-46 (1957). Moreover, "[a]ll allegations of material fact are taken as true and construed in the light most favorable to the non-moving party." *Id.*

This Court reviews de novo a district court's grant of summary judgment. *Wallis v. Princess Cruises, Inc.*, 306 F.3d 827, 832 (9th Cir. 2002). The Court "determine[s], viewing the evidence in the light most favorable to the nonmoving party, whether there are any genuine issues of material law and whether the district court correctly applied the relevant substantive law." *Id*.

This Court also reviews de novo a district court's interpretation of a federal statute. *Peck v. Cingular Wireless, LLC*, 535 F.3d 1053, 1055 (9th Cir. 2008).

ARGUMENT

I. THE DISTRICT COURT ERRED IN GRANTING SUMMARY JUDGMENT ON ALL OF TERPIN'S CLAIMS WITHOUT A HEARING.

A. The District Court incorrectly interpreted Section 222 of the FCA.

The district court's grant of summary judgment on Terpin's FCA claim under 47 U.S.C. §§ 206 and 222 ignores the plain language of Section 222 and the FCC's interpretation of the scope of that provision. *See* 1-ADD-6-10.

Section 206 of the FCA provides a private right of action for consumers injured by carriers' violation of the FCA, including Section 222. Section 222 of the FCA governs the "privacy of customer information." In enacting this provision, "Congress created a framework to govern telecommunication carriers' protection and use of information obtained by virtue of providing a telecommunications service." *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd. 6927, 6930 (2007) ("2007 CPNI Order"), 1-ADD-40.

Section 222 requires telecommunications carriers to protect "consumers' sensitive personal information to which they have access as a result of their unique position as network operators." *In the Matter of Implementation of the*

Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information ("2013 Declaratory Ruling"), 28 FCC Rcd. 9609 (2013), 9612 ¶ 9, 1-ADD-159. Section 222 permits carriers' disclosure and access to such information "only in limited circumstances." *Id.* It places the greatest restrictions on carriers' "dissemination of more sensitive information the carrier has gathered about particular customers." 2007 CPNI Order at 6930, 1-ADD-40. Carriers may not disseminate such information to unauthorized persons without customer approval. *Id.* at 6931, 1-ADD-41. *See also* 47 C.F.R. § 64.2001 *et seq.* (CPNI Rules), 1-ADD-16 *et seq.*

The district court committed manifest error in interpreting the meaning and scope of proprietary information protected by Section 222(a) and CPNI protected by Section 222(c) and in finding that AT&T did not disclose such information through Terpin's SIM swap.

1. AT&T is liable for violating Section 222(a) of the FCA for exposing Terpin's "confidential proprietary information," including the content of text messages, to unauthorized parties through the January 7, 2018 unauthorized SIM swap.

In granting summary judgment, the district court found that the unauthorized SIM swap only gave access to Terpin's telephone number on a going forward basis and did not disclose online account information. 1-ER-19. The district court erred

by ignoring the fact that when AT&T gave unauthorized persons access to Terpin's telephone number it also gave those same unauthorized individuals access to the content of communications sent to or from that number, including the password reset texts that Pinsky used to gain access to Terpin's Microsoft and other online accounts. Factual Summary II(C), *supra.* The district court reached its erroneous conclusion not only by misconstruing the mechanics of an unauthorized SIM swap but also by misinterpreting the unambiguous language of Section 222(a), as interpreted by the FCC. The court also ignored the fact that Section 222(a) protects a wide variety of confidential proprietary information, including the content of calls and text messages. Exercising de novo review, the Court should reverse the district court's decision that the access of Terpin's account and AT&T's unauthorized SIM swap did not disclose Terpin's proprietary information under Section 222(a).

Section 222(a) of the FCA provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier." 1-ADD-6. Based on this provision's plain and unambiguous language, AT&T's disclosure to unauthorized parties of password-reset messages is encompassed by Section 222(a) because they constitute

customer proprietary information that a customer intends to keep confidential. *See* Black's Law Dictionary (11th ed. 2019) (defining "confidential" information as information which is "meant to be kept secret"); *id.* (defining "proprietary information" as "information in which the owner has a protectable interest").

The term "relating to" as used in Section 222 should be interpreted broadly. As the Supreme Court has found, "relating to" has the "broad" meaning of "to stand in some relation; to have bearing or concern; to pertain; refer; to bring into association with or connection with." *See Morales v. Trans World Airlines*, 504 U.S. 374, 383-84 (1992) ("relating to" is "deliberately expansive" and "conspicuous for its breadth"), *cited in In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd.. 13911, 14055 (2016) ("Broadband Rulemaking"), 2-ADD-343, *superseded on other grounds by* 33 FCC Rcd. 311, *In the Matter of Restoring Internet Freedom*. Interpreting "relating to" in Section 222 in this broad manner, the section clearly encompasses protection of the content of communications, including text messages.

Even if Section 222(a) were ambiguous (which it is not), the district court should have deferred to the FCC's interpretation of the FCA as encompassing the obligation to protect a broad range of proprietary information, including the content of communications. *Chevron USA, Inc. v. National Resources Defense*

Council, Inc., 467 U.S. 837, 843-44 (1984) (deference to agency interpretation of ambiguous statutes within their jurisdiction). Indeed, both the Supreme Court and this Court have deferred to the FCC's interpretation of the FCA. *See, e.g., National Cable and Telecommunications Ass'n v. Brand X Internet Services*, 545 U.S. 967, 980 (2005); *Metrophones Telecommunication, Inc. v. Global Crossing Telecommunications, Inc.*, 423 F.3d 1056, 1065 (9th Cir. 2005).

The FCC has interpreted the proprietary information protected by Section 222(a) as protecting a wide range of sensitive financial and personal information, as well as the contents of communications. For example, in *In the Matter of TerraCom, Inc. and YourTel America, Inc.* 29 FCC Rcd. 13325 (2014), 1-ADD-180, the FCC found that Section 222(a) imposed a duty on a carrier to protect the "proprietary information" submitted by customers in applying for telephone service. The FCC found that "[i]n the context of Section 222, it is clear that Congress used the term 'proprietary information' broadly to encompass all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy." *Id.* ¶ 14, 1-ADD-182. Proprietary information in Section 222(a) "clearly encompass[ed] private information that customers have an interest in protecting from public exposure" including "sensitive private information." *Id.*, 1-ADD-183.

The FCC also found the scope of proprietary information protected by Section 222(a) is "broader than the statutorily defined term 'customer proprietary network information.'" *Id.* ¶ 15, 1-ADD-183. As the FCC has found, "[h]ad Congress wanted to limit the protections of subsection (a) to CPNI, it could have done so." *Id*. *See also In the Matter of Terracom, Inc. and YourTel America, Inc.*, 30 FCC Rcd. 7075, 7079-80 (2015) ¶ 3, 1-ADD-229; *In the Matter of Cox Communications, Inc.*, 30 FCC Rcd.. 12302, 12307 (2015), 1-ADD-248 (cited by Terpin in opposition to summary judgment).

The FCC has also found that Section 222(a) protects the unauthorized disclosure by telephone carriers of the content of communications. *See* Broadband Rulemaking, 31 FCC Rcd. at 13928 (¶ 46), 2-ADD-277 ("customer proprietary information" includes non-mutually exclusive categories of individually identifiable CPNI, personal identifiable information (PII), and content of communications). The FCC so concluded because "[c]ontent is the quintessential example of a type of 'information that should not be exposed widely to the public . . . that customers expect their carriers to keep private.' Content is highly individualistic, private and sensitive." *Id.* at 13949 ¶ 101, 2-ADD-288. The FCC further defined "content" as "any part of the substance, purport or meaning of a communication . . . ." *Id.* at ¶ 102, 2-ADD-288.

Under Section 222(a)'s plain and unambiguous meaning and as interpreted by the FCC, AT&T's act of transferring control of Terpin's phone to an unauthorized third party, including transmittal to that third party of the content of password reset messages, violated AT&T's duty to protect Terpin's confidential proprietary information.[5] Factual Summary II(C), *supra*. Indeed, the district court's interpretation of Section 222(a) would deprive Terpin and other victims of SIM swaps of privacy protection for their most intimate communications.

2. AT&T violated Section 222(c) of the FCA by exposing Terpin's Customer Proprietary Network Information to unauthorized parties, including network information relating to the quantity, technical configuration, type, destination and location of Terpin's telecommunications service.

Section 222(c) of the FCA requires carriers to protect from disclosure CPNI without customer permission. 2013 Declaratory Ruling at 9661 ¶ 9, 1-ADD-159. Section 222(h)(1)(A) defines CPNI as "information that relates to the quantity,

---

[5] The FCC continues to interpret unauthorized SIM swaps as implicating confidential personal information protected by carriers' unauthorized SIM swap frauds. *See In the Matter of Protecting Consumers from SIM Swap and Port Out Fraud*, 36 FCC Rcd. 14120 (2021), 3-ADD-541. The FCC's proposed rules regarding SIM swapping rest upon the foundation of the protections afforded by Section 222. Moreover, the FCC refers to the Terpin case in its proposed SIM-swap rulemaking. 36 FCC Rcd. 14122, n.4, 3-ADD-543, 568.

technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 1-ADD-9.

In reviewing the district court's interpretation of Section 222(c) de novo this Court should find that Terpin's unauthorized SIM swap in fact exposed his CPNI to unauthorized parties. In reaching a contrary conclusion, the district court erroneously reasoned that the details of Terpin's calls were not exposed (but only his telephone number on a going forward basis) and that AT&T was relieved of any liability for such disclosure because Pinsky and others undertook additional steps to use the communications that were sent to a phone under their control to accomplish the theft. 1-ER-19-20. The district court further found that Smith, who perpetrated the SIM swap, did not have access to CPNI despite the fact that he bypassed AT&T authentication procedures and saw and manipulated Terpin's CPNI to conduct the unauthorized SIM swap. *Id.*; Factual Summary I(C), *supra*. The district court's holdings are also inconsistent with the meaning of Section 222(c) and ignore material disputed facts and reasonable inferences in Terpin's favor from such facts.

AT&T is well aware that a telecommunications carrier is not absolved of liability under Section 222 to protect its customers' information because

unauthorized third parties use the information after the carrier wrongfully discloses it. As the FCC found in a case in which AT&T disclosed the geolocation information of hundreds of thousands of customers and the FCC imposed a record $57 million fine on AT&T for violating Section 222 of the FCA, the "ultimate responsibility" for the disclosure of CPNI rests with the carrier. *In the Matter of AT&T Inc.*, FCC 20-26 ¶ 45, 2-ADD-510-11 ("AT&T Geolocation Order"). The fact that a third party (Pinsky) received CPNI and had to take additional steps to steal cryptocurrency, does not mean that AT&T is not liable to Terpin for its unauthorized disclosure of CPNI to Pinsky.

In addressing AT&T's massive disclosure of consumers' location information in its order, the FCC found that "[t]o allow a telecommunications carrier to share CPNI with an entity that is not subject to section 222 without sufficient controls could deprive [AT&T] customers of the statutory protections of section 222." *Id*. at ¶ 46, 2-ADD-511. Since 2007, the FCC has consistently found that customers must provide opt-in approval for sharing of CPNI "'because a carrier is no longer in a position to personally protect the CPNI once it is shared.'" *Id.* (*quoting* 2007 CPNI Order, 22 FCC Rcd. at 6948 ¶ 39), 1-ADD-47. Needless to say, there is no evidence that Terpin gave such opt-in approval. Indeed, AT&T told Terpin it would implement "extra security" to prevent unauthorized SIM swaps.

The district court also erred in finding that no CPNI was disclosed to Pinsky and his confederates. 1-ER-20. Under Section 222(c) AT&T was obligated not to disclose any *network* information "relating to" a customer, including "what calls were made to and/or from a particular telephone number and the duration of such calls . . ." 2007 CPNI Order, 222 FCC Rcd. 6928 ¶ 2, 1-ADD-39. Although CPNI is a narrower category than proprietary information, it encompasses a wide swath of information that relates to the customer's use of the network, including information regarding calls and text messages made on a customer's mobile account. The FCC in 2007 enacted increased protections for CPNI (in the context of a scam called pretexting) because it had found "concrete evidence that the dissemination of this private information does inflict specific and significant harm on individuals, including harassment and the use of the data to assume a customer's identity." *Id.*, 22 FCC Rcd.. 6947, ¶ 39, 1-ADD-47.

Terpin suffered similar harm. When AT&T turned CPNI over to unauthorized third parties, including the ability to receive and make calls to a phone with Terpin's number connected to the AT&T network through a SIM, third parties, including Pinsky, were able by this means to steal Terpin's identity and almost $24 million in cryptocurrency. Factual Summary II(C), *supra.* Under the broad language of 222(c) the unauthorized parties thus received "information *that relates to*" (i.e., "to stand in some relation; to have bearing or concern; to pertain;

refer; to bring into association with or connection with") the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service."

Terpin also adequately pleaded that AT&T's agent Smith, who conducted the SIM swap without Terpin's authorization (and bypassed Terpin's "extra security"), accessed and manipulated Terpin's CPNI. As shown in Terpin's Account Notes, Smith used the AT&T OPUS system after accessing Terpin's authentication-protected customer account to make the unauthorized SIM swap, which required him to see or input information regarding the SIM numbers for Terpin's phone and the phone controlled by Pinsky, as well as the IMEI or unique identifier for the phones. *See* Factual Summary II(C), *supra,* citing 10-ER-1896-97 (Account Notes); 10-ER-1794-95, 1798-99 (Hill Dep.). By definition, such information is CPNI because it relates to the technical configuration of a telecommunications service.

Further, while the district court stated that "[a]bsent any evidence regarding what information was revealed during the SIM swap, no jury could reasonably infer that Terpin's protected information was disclosed to Smith in violation of the FCA," the fact that AT&T had authentication protections on Terpin's account requires—at least for summary judgment—the inference that the account contained CPNI and proprietary confidential information which Smith would have had access

to "authenticate" Terpin when he made the SIM swap. Bypassing proper authentication procedures and gaining access to Terpin's account itself constitutes a violation of the FCA.

B. The Economic Loss Rule Does Not Apply to Terpin's Claims.

The district court dismissed Terpin's claims for negligence, negligent supervision and training, and negligent hiring on the economic loss rule in *Sheen* which held that a plaintiff in privity with a defendant could not bring tort claims against the defendant for losses encompassed by its contract claims because there was no independent statutory or common law duty giving rise to tort liability in regard to loan modifications. *Sheen,* 12 Cal. 5th at 942. The district court erred because there is in fact here such an "independent statutory" duty.

1. The economic loss rule does not apply to Terpin's fraud claims.

California has long recognized that the economic loss rule does not apply where a defendant's conduct violates "a duty independent of the contract arising from principles of tort law." *Ehrlich v. Menezes*, 21 Cal. 4th 543, 551 (1999). One instance is "where the plaintiff was fraudulently induced to enter a contract." *Id*. at 551-52. *See also Sheen*, 12 Cal. 5th at 943. In the SAC, Terpin made claims for deceit by concealment and promissory fraud that were dismissed by the district court. 1-ER-26. Upon reversal of the district court's dismissal, these claims will not be subject to the economic loss rule.

2. The economic loss rule does not apply to Terpin's negligence claims because AT&T had a duty independent of the contract to protect Terpin's communications.

Invoking *Sheen*, the district court found that Terpin's negligence claims were barred by the economic loss doctrine because Terpin was in contractual privity with AT&T through the WCA. The district court further found that there was no independent statutory duty within the exception recognized by *Sheen* because claims under AT&T's statutory duty were inconsistent with the WCA.[6] The district court erred in reaching both conclusions.

The economic loss rule applies only where the "litigants are in contractual privity and the plaintiff's claim is not 'independent of the contract arising from principles of tort law.'" *Sheen*, 12 Cal. 5th at 942 (quoting *Ehrlich,* 21 Cal. 4th at 551). Moreover, "California public policy . . . strongly favors" holding that principles of tort law apply when they arise independent of the contract. *Robinson Helicopter Co., Inc. v. Dana Corp.*, 34 Cal. 4th 979, 991 (2004). "'[C]ourts will generally enforce the breach of a contractual promise through contract law, except when the actions that constitute the breach violate a social policy that merits the

[6] The district court entirely ignored the third potential basis for the independent duty cited by Terpin, 47 CFR § 64.2001 *et seq.* (FCC CPNI Rules). 1-ADD-16 *et seq.*

imposition of tort remedies.'" *Id*. (quoting *Freeman & Mills v. Belcher Oil Co.,* 11 Cal. 4th 85, 107 (1995) (Mosk, J., concurring in part and dissenting in part). Moreover, "courts should be careful to apply tort remedies only when the conduct in question is so clear in its deviation from socially useful business practices that the effect of enforcing such tort duties will be . . . to aid rather than discourage commerce." *Freeman & Mills*, 11 Cal. 4th at 109.

Allowing tort remedies based on AT&T's statutory duty to protect its customers' communications fulfills both a "social policy" and "aid[s] . . . commerce" because allowing such remedies promotes the fundamental policy of protecting customers' confidential communications. The duties imposed upon AT&T are complimentary to the WCA, including AT&T's privacy policy and Code of Business Conduct ("COBC"), which specifically reference AT&T's duty to protect the confidentiality of customer communications.

As noted in Argument Section I(A), AT&T has an undoubted and important obligation to protect its customers' communications. AT&T cannot absolve itself of this statutory duty by deflecting blame to third parties (such as Pinsky) or citing boilerplate disclaimers in its customer agreements. AT&T Geolocation Order, 2-ADD-510-11. Indeed such a disclaimer of a statutory duty is against California public policy. *Halliday v. Greene*, 244 Cal. App. 2d 482, 488 (1966).

Consistent with its statutory duties, AT&T makes "commitments" in its privacy policy to protect the privacy of customers' communications. 2-ER-160-176. For example, AT&T commits to "keep [a customer's] information safe using encryption or other appropriate security controls" and to protect [customers'] information." 2-ER-172. AT&T also promises customers its employees are subject to its COBC and "all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, *the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records*. We take this seriously, and any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action. That includes dismissal." *Id.* (emphasis added). AT&T further commits to "[*l*]*imiting access to Personal Information to only those with jobs requiring such access*" and "[*r*]*equiring caller/online authentication before providing Account Information* so that only you or someone who knows your Account Information will be able to access or change the information." *Id*. (emphasis added).

Despite these clear "commitments," the district court found that AT&T's obligations under the FCA were "contrary" to the WCA because the WCA limited AT&T's liability for consequential damages and because AT&T stated that it could not guarantee security of personal information. 1-ER-16, quoting 2-ER-172

(privacy policy) and referencing 3-ER-291-92 (WCA limitation of damages)). The district court's approach to the economic loss rule thus read out of existence AT&T's commitments to its customers.

The district court's finding that a contractual limitation on damages prevents imposition of a tort remedy for violation of independent (but consistent) statutory duties, ignores the fact that AT&T's limitation of damages would be unenforceable in California because it would absolve AT&T of its own gross negligence and statutory violations. *See In re Yahoo! Inc. Customer Data Security Breach Litig*., 313 F. Supp. 3d 1133, 1135 (N.D. Cal. 2018) (Koh, J.). Exculpatory provisions cannot relieve AT&T of its violation of the law "whether the violation be willful or negligent." *Halliday,* 244 Cal. App. 2d at 488 (citing Cal. Civ. Code § 1668 for public policy against allowing a party to exempt itself from its own "violation of law, whether willful or negligent").

The district court also reached the inexplicable conclusion that the WCA was not compatible with AT&T's statutory obligation to protect Terpin's private communications because "Terpin and AT&T did *not* agree that, should a third party bribe a retail employee to SIM swap Terpin's phone number, then hack Terpin's email and online accounts, root through Terpin's digital garbage to discover an unknown cache of cryptocurrency access credentials, and ultimately use those credentials to steal million in cryptocurrency, AT&T would be liable for

Terpin's loss." (Emphasis in original). 1-ER-16. The district court's convoluted statement (which appears to adopt AT&T's characterization of the Terpin SIM swap) ignores AT&T's commitments to maintain the privacy of customers' communications under Section 222 of the FCA. It also ignores the facts of what happened in Terpin's January 7, 2018 SIM swap. Factual Summary II(C), *supra.* As noted, the FCA also does not absolve AT&T of its statutory liability to protect confidential communications by not disclosing them to unauthorized parties because those unauthorized parties have to take additional steps to use the information. *See* AT&T Geolocation Order ¶ 46, 2-ADD-511.

The district court also erred in finding that the AT&T Consent Decree did not impose additional obligations on AT&T consistent with the WCA because "it did not involve SIM swaps or cryptocurrency." 1-ER-15 n.4. In fact, the AT&T Consent Decree arose under the very statute at issue here—FCA Section 222. In addition to assessing a $25 million penalty on AT&T, the FCC's consent decree also imposed an obligation on AT&T to implement an "Information Security Program" (ISP) to guard against emerging threats to its customers' privacy. Unauthorized SIM swaps were precisely such an emerging threat. *See* AT&T Consent Decree at 2816-20 ¶¶ 18(b)-(c) and ¶ 22, 1-ADD-217-19 (AT&T "to identify and respond to *emerging risks or threats, and to comply with the*

requirements of Section 222 of the Act, the CPNI Rules, and this Consent Decree"). (Emphasis added.)

The district court also distorts the economic loss rule by making contractual privity the only significant point of its analysis. This is contrary to *Sheen* and would render meaningless the separate duty exception expressly recognized in *Sheen* as it would apply in virtually every case. As the court in *Warren v. PNC Bank Nat'l Ass'n*, 2023 WL 3182952, *9-10 (N.D.Cal. Apr. 30, 2023) found, even in the context of lender liability cases (such as *Sheen*), statutory violations may give rise to the requisite separate duty permitting tort damages. Although the parties in *Warren* were in contractual privity (homeowner and lender), the court found that statutory violations of the California Homeowner Bill of Rights allowed the plaintiff to state a valid negligence claim based on the defendant's statutory duty of care.

3. The economic loss rule does not apply to the WCA as a contract of adhesion.

The district court also erred in dismissing Terpin's argument that *Sheen* is not applicable to contracts of adhesion, such as the WCA, and that Terpin had not properly raised the argument. The fact that an individual consumer cannot negotiate an agreement with a wireless provider is well established, as is the fact that such agreements are contracts of adhesion. *See, e.g., Ting v. AT&T,* 182 F.

Supp. 2d 902, 928 (N.D. Cal. 2002) (AT&T consumer service agreement contract of adhesion); *Ting v. AT&T,* 319 F.3d 1126 and 1149 (9th Cir. 2003) (affirming that AT&T contract is one of adhesion); *Gatton v. T-Mobile-USA, Inc.*, 2003 WL 21530185, *10 (C.D. Cal. Apr. 18, 2003) (T-Mobile customer agreement is a contract of adhesion because plaintiffs "had to sign the agreement in order to obtain service from T-Mobile"); *Lozano v. AT&T Wireless*, 216 F. Supp. 2d 1071, 1075 (C.D. Cal. 2022) (AT&T "welcome guide" with legal limitations contract of adhesion).

Applying the economic loss rule to contracts of adhesion is contrary to its rationale of "'protect[ing] the bargain the parties have made against disruption by a tort suit'" and allowing the parties "'to make dependable allocations of financial risk without fear that tort law will be used to undo them later.'" *Sheen*, 12 Cal. 5th at 923 (quoting Restatement 3d. Torts, Liability for Economic Harm (June 2020) § 3, com. B., p. 13). Given this rationale, the doctrine does not apply here because there was no negotiated bargain between Terpin and AT&T.

C. Terpin properly alleged a claim for breach of contract.

The district court improperly granted summary judgment on Terpin's breach of contract claim on the ground that Terpin could not establish consequential damages for the unauthorized SIM swap because of AT&T's disclaimer of such damages in the WCA. 1-ER-20-23, 3-ER-291-92 (WCA limitation of damages

provision). The court also found that consequential damages were improper because the parties did not contemplate Terpin's investments in cryptocurrency when he established service with AT&T in 2011. *Id.* The district court further rejected Terpin's claim that AT&T breached an oral contract with him that was separate from the WCA that he entered into with AT&T after his June 2017 unauthorized SIM swap in which AT&T promised that implementing "extra security" on his accounts would prevent future unauthorized SIM swaps. *Id.* Each of the district court's rationales for granting summary judgment on Terpin's contract claim fundamentally misreads applicable law and ignores material disputed facts and inferences from such facts in Terpin's favor.

Terpin's breach of contract claim references both AT&T's breach of its promises in the WCA and privacy policy and AT&T's breach of its separate promise to provide extra security to prevent future takeover of his account. *See* Factual Summary II(B), *supra,* 6-ER-1065-1068 and 6-ER-1032-37 (SAC ¶¶ 205-211 incorporating by reference AT&T's promises for "extra security" (SAC ¶¶ 88-90, 94, 98-99)). Terpin alleges and has shown through discovery that AT&T's promises were false and that AT&T breached its promises in the WCA and its privacy policy by not providing any (let alone "extra") security to prevent the January 7, 2018 unauthorized SIM swap. 6-ER-1034-37 (SAC ¶¶ 93-94, 98-99); *see also* Factual Summary II(B)-(C), *supra*.

As outlined above, an agent of AT&T's authorized retailer (Smith) was bribed to perform the January 7, 2018 unauthorized SIM swap, thus leading to the theft of almost $24 million in cryptocurrency. *Id*., II(B). The "extra security" did nothing to prevent Smith from doing this and AT&T knew well before that time that such security was not effective because employees were readily bypassing it by purporting to authenticate customers through the highly inadequate means of utilizing the last four digits of a SSN. *Id.* Indeed, Smith himself had committed unauthorized SIM swaps on at least two other customers the month before Terpin. *Id.,* II(E).

Although the district court framed the damages sought by Terpin as "consequential damages," it ignored the fact that AT&T was indeed aware in *2017*—which is the date not only of the WCA and privacy policy[7] but also of AT&T's promises of extra security--that its customers could suffer significant financial damages from unauthorized SIM swaps.

Consequential or "special" damages are recoverable when the "special or particular circumstances from which they arise were *actually communicated to or*

---

[7] The privacy policy attached to the SAC as Exhibit C, 2-ER-160, is dated May 2, 2017. The WCA attached as Exhibit D to the SAC, 3-ER-275, was the then-current version of that document attached to the original complaint filed on August 15, 2018. 8-ER-1418-1569.

known by the breaching party (a subjective test) *or were matters of which the breaching party should have been aware at the time of contracting* (an objective test). *Lewis Jorge Constr. Mgmt.,* 34 Cal. 4th 960, 968-69 (2004) (emphasis added). Such was the case here. In 2017, Terpin informed AT&T that he had suffered losses of cryptocurrency due to the June 11, 2017 unauthorized SIM swap. *See* Factual Summary II(B), *supra.* Moreover, AT&T was aware well before January 7, 2018 that its customers had suffered financial consequences from unauthorized SIM swaps. *Id.,* II(D). Indeed, AT&T customers suffered unauthorized SIM swaps at the hands of Smith before Terpin did. *Id.*, II(E). On that basis alone, there are disputed material facts that prevent a grant of summary judgment on the issue of consequential damages.

The district court further erred in finding without evidence that the intent of the parties regarding damages should have been judged in *2011*, when Terpin transferred his wife's AT&T account to himself, rather than *2017* when AT&T made promises regarding extra security. Indeed, there was no evidence in the record regarding Terpin's agreement with AT&T in 2011, because AT&T has never produced such an agreement (despite Terpin's request). 6-ER-1041 (SAC ¶ 112). The district court thus had no reasonable basis to conclude that the parties' relationship should be assessed in 2011.

The district court also erred in not properly recognizing that AT&T's promises regarding "extra security" on June 13, 2017 gave rise to a *separate contractual promise* and were not a modification of the WCA subject to its limitations provision. Factual Summary II(C), *supra.* As noted, AT&T made promises of "extra security" to Terpin when he expressed concerns after his June 11, 2017 unauthorized SIM swap. *Id.* AT&T promised that the "extra security" would prevent future account takeovers. *Id.* Terpin accepted the promise and remained an AT&T customer. *Id.; see also* 6-ER-106 (SAC ¶ 205 incorporating by reference ¶¶ 88-89 of the SAC).[8] There is no damages limitations provision associated with this separate promise.

D. The district court erred in dismissing Terpin's declaratory relief claim.

Because Terpin is entitled to reversal of the district court's order granting summary judgment as to his FCA Section 222, negligence, and breach of contract claims, his claim for declaratory judgment is not moot. The Court should therefore reinstate this claim.

---

[8] Although the district court relied on the allegations of the SAC regarding the supposed parameters of Terpin's breach of contract claim, it ignored Terpin's extensive allegations that his wireless agreement with AT&T was a contract of adhesion. *See* 6-ER-1041-48 (SAC ¶¶ 113-132). It further ignored Terpin's argument based on *Halliday,* 244 Cal. App. 2d, at 488, *supra*, that the limitations provision on which AT&T relies is unconscionable because it violates public policy, including Cal. Civ. Code §§ 1668, 1670.5.

E. Material disputed facts prevent entry of summary judgment on proximate cause grounds.

Although the district court did not rule on AT&T's proximate cause argument, it is before the Court on de novo review of the record. *Beck v. City of Upland*, 527 F.3d 853, 866-867 (9th Cir. 2008) (Court may consider issues on appeal not reached by the district court). For reasons of judicial economy, the Court on remand of this matter to the district court for trial should rule that there are no grounds to grant summary judgment to AT&T for lack of proximate cause because there are numerous disputed material facts regarding issues of the foreseeability of Terpin's harm on all of his claims.

In its motion for summary judgment, AT&T presented a tendentiously complicated multi-step account of the events leading to the January 7, 2018 unauthorized SIM swap. AT&T's account made no reference to the role that AT&T played in turning over control of Terpin's account to thieves nor to its disclosure of Terpin's proprietary information and private communications. Based on AT&T's convoluted account (which the district court appears to have adopted at least in part in framing its accounts of what the parties had "not agreed to," (Argument I(B)(2), *supra*)), AT&T argued that the unauthorized SIM swap was not the proximate cause of Terpin's losses. AT&T further argued that the theft was

so remote or attenuated that as a matter of law that the SIM swap was not the proximate cause of Terpin's losses. Dkt-140.

In its opposition to the motion for summary judgment, Terpin disputed both AT&T's description of the events leading to the SIM swap and AT&T's argument that the SIM swap was not the proximate cause of Terpin's losses. These facts are outlined above. *See* Factual Summary I(A)-(E), *supra*. Based on these material disputed facts, summary judgment should not be granted on these grounds.

Proximate cause and causation in fact are generally questions "of fact for the jury." *Desrosiers v. Flight Int'l*, 156 F.3d 952, 956 (9th Cir. 1988). There is "an element of foreseeability in the inquiry [of proximate cause], and a defendant owes no duty to prevent a harm that was not a reasonably foreseeable result of his negligent conduct." *Kumaraperu v. Felstad*, 237 Cal. App. 4th 60, 69 (2015). "[T]he question of 'the closeness of the connection between the defendant's conduct and the injury suffered' [citation] is strongly related to the question of foreseeability itself." *Cabral v. Ralph's Grocery Co.*, 51 Cal. 4th 764, 779 (2011), (quoting *Rowland v. Christian,* 69 Cal. 2d 108, 113 (1968)). The court must "evaluate more generally whether the category of negligent conduct at issue is sufficiently likely to result in the kind of harm experienced that liability may appropriately be imposed." *Cabral*, 51 Cal. 4th at 772. Moreover, foreseeability or harm is not based on plaintiff's specific injury (here, theft of cryptocurrency)

but rather on the general character of the event or harm (financial losses or identity theft to customers from unauthorized SIM swaps). *Williams v. Fremont Corners, Inc.*, 37 Cal. App. 5th 654, 671 (2019).

In his Statement, Terpin referenced numerous material facts demonstrating that his harm from the January 7, 2018 SIM swap was foreseeable and directly linked to the actions of AT&T in turning over his confidential proprietary information and CPNI to Pinsky and others, including the communications sent and received on that account. *See* Factual Summary I(C)-(E), *supra.* These material facts not only preclude summary judgment on the issues of proximate cause but at trial will establish proximate cause and foreseeability of harm in Terpin's favor. These facts also show that the cryptocurrency losses that followed the SIM swap were a "natural and continuous sequence" of plausible events. *State of California v. Superior Court*, 150 Cal. App. 3d 848, 857 (1984).

AT&T in its opposition (as it did in its motion) is likely to cite several inapposite cases where convoluted and unusual events led courts to find that there was no proximate causation as a matter of law. *See, e.g., Shih v. Starbucks Corp.*, 53 Cal. App. 5th 1063, 1070 (2020) (failure of Starbucks customer to use a protective sleeve did not increase the risk of customer losing her balance and suffering burns); *Wawanesa Mut. Ins. Co. v. Matlock*, 60 Cal. App. 4th 583 (1997) (lack of foreseeability when fortuitous purchase of cigarettes caused youngsters on

telephone poles to bump purchaser of cigarettes who dropped cigarette in inaccessible space that caused fire); *Steinle v. United States*, 17 F.4th 819, 822-23 (9th Circ. 2021) (no proximate cause because of fortuitous series of events where person broke into a locked vehicle, stole pistol from backpack and abandoned the pistol which was found by another person who shot the victim).

In contrast to these "Rube Goldbergesque" scenarios, the harm suffered by Terpin (financial losses) was the precise harm that AT&T had warned its customers would result from an unauthorized SIM swap in its September 27, 2017 Cyber Aware blog. Moreover, the harm occurred in precisely the manner that AT&T had predicted. 2-ER-121 (AT&T Blog). AT&T also knew or should have known by January 2018 that its customers were in danger of losing cryptocurrency to unauthorized SIM swaps. *See* Factual Summary I(D), *supra*. There was nothing "fortuitous" about these linkages—the same series of events had happened to numerous other cryptocurrency investors, as publicized by *Forbes* and *The New York Times*. *Id.* Indeed, another court considering an unauthorized SIM swap case found that allegations of proximate cause, where cryptocurrency was drained just an hour and eleven minutes after an unauthorized SIM swap, were "sufficiently direct and not comparable to the 'Rube Goldbergesque' system of fortuitous linkage' where California courts have held proximate cause lacking as a matter of

law." *Fraser v. Mint Mobile, LLC*, 2022 WL 1240864, *3 (N.D. Cal. Apr. 27, 2022).

In reversing the district summary judgment order, the Court should not remand the issue of proximate cause for consideration by the district court, but should deny AT&T's summary judgment motion on the additional ground that there are triable issues of fact relating to proximate cause and foreseeability that require denial of the motion as a whole.

II. THE DISTRICT COURT ERRED IN DISMISSING TERPIN'S FRAUD CLAIMS AND HIS REQUEST FOR PUNITIVE DAMAGES WITH PREJUDICE AND WITHOUT A HEARING.

A. The district court erred in dismissing Terpin's plausible claim that AT&T had engaged in deceit in June 2017 in promising to provide Terpin with extra security on his account to prevent future unauthorized SIM swaps.

In its September 8, 2020 order on AT&T's third motion to dismiss, the district court dismissed Terpin's deceit by concealment claim with prejudice on the grounds that AT&T's conduct did not meet the criteria for deceit under California law. 1-ER-26 (citing *LiMandri v. Judkins*, 52 Cal. App. 4th 326, 336 (1997)). *See also* Cal. Civ. Code § 1709 ("[o]ne who willfully deceives another with intent to induce him to alter his position to his injury or risk, is liable for any damage which

he thereby suffers"); Cal. Civ. Code § 1710 (defining "deceit" under §1709 as "either: 1. The suggestion, as a fact, of that which is not true, by one who does not believe it to be true; 2 . The assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true; 3. The suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact; or, 4. A promise, made without any intention of performing it). 1-ADD-13-14.

Construing the allegations of the SAC as true and in the light most favorable to Terpin, as it must, this Court should reverse the district court's dismissal because Terpin has adequately alleged a claim against AT&T for deceit under California law, including promissory fraud regarding its future actions, based on AT&T's assertions to Terpin and suppression of facts relating to the security it would provide on Terpin's accounts.

Under California law, AT&T had a duty to disclose known security flaws because it "had exclusive knowledge of material facts not known to plaintiff." *LiMandri*, 52 Cal. App. 4th at 336. In the SAC, Terpin alleges that AT&T had exclusive knowledge of its security practices which were of material importance to Terpin because the flaws in those security practices (including both AT&T's authentication procedures and its vaunted "extra security" protections) led to his

June 11, 2017 and January 7, 2018 unauthorized SIM Swaps. *See* 6-ER-999-1007 (SAC ¶¶ 143-156).

The district court rejected Terpin's argument that AT&T had exclusive knowledge regarding security on the ground that AT&T's privacy policy stated that it could not "guarantee that your Personal Information will never be disclosed . . . ." 1-ER-31. However, AT&T's boilerplate privacy policy qualification that it could not promise perfect security is not pertinent to the question of whether AT&T had a duty to disclose *known* security flaws, particularly when it separately promised to provide what it claimed was effective "extra security" to prevent future account takeovers. The privacy policy disclaimer also does not insulate AT&T from liability in making in June 2013 knowingly false or misleading promises particularly when it did not reference the disclaimer in those promises.

The court further erred when it found that AT&T did not have a duty to disclose since it had not actively concealed a material fact from plaintiff; the court erred as well by asserting that the allegations in the complaint are "mere nondisclosure" and not active concealment. 1-ER-31-32, (citing *LiMandri*, *supra*). The district court again misread the SAC. The SAC specifically alleges *active* concealment by AT&T to Terpin in regard to the promises it made in June 2017 regarding implementation of the six-digit "extra security" code on his account.

As alleged in the SAC, Terpin "expressed concern about AT&T's ineffective security protections and asked how he could protect the security of his phone number and account against future unauthorized access," including unauthorized SIM swaps. 6-ER-1032-33 (SAC ¶ 88). "In response . . . and in order to induce Mr. Terpin to continue as an AT&T customer, AT&T promised that it would place his account on a 'higher security level' with 'special protection.'" 6-ER-1033 (SAC ¶ 89). "AT&T told Terpin that this 'higher security level' would require anyone accessing or changing Terpin's account to provide a six-digit passcode to AT&T to access or change the account. Anyone requesting AT&T to transfer Terpin's telephone number to another phone must provide the code. AT&T promised Terpin at this meeting that the higher security that it was placing on his account, which it also called 'high risk' or 'celebrity' protection would ensure that Terpin's account was much less likely to be subject to SIM swap fraud. AT&T further told Terpin that the implementation of the increased security measures would prevent Terpin's number from being moved to a second phone without Terpin's explicit permission, because no one other than Terpin and his wife would know the secret code." *Id*. (SAC ¶ 89).

The allegations of the SAC--when read in a manner favorable to Terpin as they must be in a motion to dismiss--sufficiently allege an affirmative promise on the part of AT&T to implement "extra security" and a failure to disclose to Terpin

that such security was ineffective. For example, the SAC alleges that AT&T failed to disclose to Terpin in June 2017 "that the extra security measures were not adequate and could be overridden or ignored by its employees." 6-ER-1034-35 (SAC ¶ 93). Discovery has shown that this is precisely what happened. With Terpin not being present in the store, Smith was able to bypass or ignore the "extra security," falsely claim that he could not scan Terpin's driver's license, and "authenticate" Terpin with the widely available last four digits of his SSN. *See* Factual Summary II(B)-(E), *supra*.

The district court further erred in not construing the allegations of the SAC in Terpin's favor by finding that Terpin could not maintain his deceit by concealment claim on the basis of AT&T's partial representation because AT&T's promises in June 2017 regarding extra security were qualified by the disclosure in its privacy policy that its security was not perfect and could be compromised by "unauthorized acts by third parties." 1-ER-31. The district court ignored the fact that the SAC alleges that AT&T made numerous incomplete representations that relate not to the action of "third parties," but to itself and its employees. For example, the SAC alleges that AT&T represented that its employees were subject to its COBC whose violation could result in dismissal, that it required "caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or

change the information;" and that it would follow the "legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records." 6-ER-1018-22 (SAC ¶¶ 52-59) and 2-ER-17 (AT&T privacy policy). A disclaimer by AT&T that it did not have "perfect" security does not absolve it liability for deceit in making statements that were either false or incomplete.

B. The district court erred in dismissing Terpin's plausible claim that AT&T engaged in deliberate misrepresentation by making a promise for future conduct without an intent to perform.

The district court also erred in dismissing with prejudice Appellant's claim for misrepresentation by not accepting as true his well pleaded allegations and construing them in the light most favorable to him as the non-moving party, including his allegations that AT&T had made deliberate misrepresentations regarding its future conduct. Instead the district court found that AT&T may have been "overly optimistic" in making its promises, but that did not support a finding of fraud. 1-ER-33-34, (citing *Magpali v. Farmers Grp., Inc.*, 48 Cal. App. 4th 471, 481 (1996)).

In the SAC, Terpin alleges that AT&T flatly made *false* promises to him after his initial June 11, 2017 SIM swap—not "overly optimistic" ones. 6-ER-1032-35 (SAC ¶¶ 88-93). Such false promises support a claim for deliberate

misrepresentation under California law. *Id.* (citing Cal. Civ. Code § 1710 (subd.4) and *Tarmann v. State Farm Mut. Auto., Ins. Co.*, 2 Cal. App. 4th 153, 158-59 (1991)). Terpin alleged that on June 13, 2017 he told AT&T that he was concerned with the security of his account because of his June 11, 2017 SIM swap; he asked how he could protect his phone number "against future unauthorized access, including hackers attempting to perpetrate SIM swap fraud." 6-ER-1032-33 (SAC ¶ 88). In response, AT&T told him that he could protect his account by implementing "extra security" in the form of a six-digit code to prevent future account takeovers. 6-ER-1033 (SAC ¶ 89). Terpin further alleges that AT&T's promises were false because AT&T knew that the "extra security" "was easily evaded by AT&T's own employees, who it knew or should have known actively cooperated with hackers in SIM swap fraud." 6-ER-1034-35 (SAC ¶ 93), 6-ER-1055 (SAC ¶ 160).

Facts adduced in discovery demonstrate that the allegations in the SAC were well-founded. Before it made its promises to Terpin June 2017, AT&T knew that its employees were bypassing this "extra security" and were conducting unauthorized SIM swaps. *See* Factual Summary II(C)-(D), *supra*.

C. The district court improperly dismissed Terpin's request for punitive damages by applying an incorrect heightened pleading standard to the SAC.

The district court also erred in dismissing Terpin's punitive damages claims because it found that Terpin had not properly alleged that AT&T's officers had engaged in actions with the requisite malice and "conscious[] disregard" of risks. 6-ER-34-38. The court found that Terpin did not "provide factual allegations that show the ways in which Mr. O'Hern [head of AT&T security] and Mr. Huntley [head of AT&T compliance] deliberately avoided taking steps to remedy the security gaps at the time of his attack." The district court further found that Terpin's pleading was defective because he had not alleged "any specific steps Messrs. O'Hern and Mr. Huntley have failed to take to remedy AT&T's security flaws . . ." 6-ER-38.

The district court applied an incorrectly heightened pleading standard to the punitive damage allegations that conflicts with the notice pleading requirements of the Federal Rules of Civil Procedure. Although Cal. Civ. Code § 3294 (1-ADD-15) establishes the "governing substantive law for punitive damages [in federal court], California's heightened pleading standard irreconcilably conflicts with Rules 8 and 9 of the Federal Rules of Civil Procedure—the provisions governing the adequacy of pleadings in federal court." *Clark v. Allstate Ins. Co.*, 106 F.

Supp. 2d 1016, 1018 (S.D. Cal. 2000). As the Court has held, a plaintiff need not plead "any particularity in connection with an averment of intent, knowledge or condition of the mind." *In re GlenFed Sec. Litig.,* 42 F.3d 1541, 1547 (9th Cir.1994) (en banc), *superseded by statute on other grounds as stated in SEC v. Todd,* 642 F.3d 1207, 1216 (9th Cir.2011). Fed. R. Civ. Proc. 8(a) requires only "a short and plain statement of the claim showing that [Plaintiff] is entitled to relief, and . . . a demand for judgment for the relief [they] seek." Fed. R. Civ. Proc. 9(b) further provides that "[m]alice, intent, knowledge, and other conditions of mind of a person may be averred generally."

Terpin's allegations regarding the involvement of AT&T officers and managing agents were adequately pleaded given that discovery had yet to commence. 6-ER-1028-32, 1051 (SAC ¶¶ 75, 78-79, 83-84, 144). The allegations were based on publicly available information, including reports of SIM swaps subsequent to Terpin's own. Terpin also specifically alleges that Messrs. O'Hern and Huntley did not require AT&T to provide a SIM lockdown, as had T-Mobile, to remedy AT&T's security flaws. 6-ER-1050-51 (SAC ¶ 143).

Terpin alleged that because of their positions and responsibilities both Messrs. O'Hern and Huntley knew of the structural flaws and lapses that allowed AT&T employees to bypass security and conduct unauthorized SIM swaps. 6-ER-1038 (SAC ¶ 75). Terpin further alleged that Mr. Huntley had such knowledge

because he was specifically tasked to safeguard the privacy of customer information. 6-ER-1033-34 (SAC ¶¶ 90-91). Terpin also specifically alleged that Messrs. O'Hern and Huntley had such knowledge because they were responsible for ensuring that AT&T complied with its security obligations, including those under the AT&T Consent Decree. 6-ER-1015-1017, 1028 (SAC ¶¶ 46-49, 75).

Allegations similar to those found in the SAC were found to be adequate in a case cited by the district court. *See In re Yahoo! Inc.*, 313 F. Supp. 3d at (punitive damages allegation asserting involvement of corporate officers and directors sufficient when plaintiffs "include the names and titles of individual actors who are alleged to have committed malicious conduct supporting an award of punitive damages").

III. CONCLUSION

Terpin seeks reversal of the district court's orders because the court did not correctly interpret important protections afforded carriers' customers by the FCA, including carriers' duty to protect the privacy of their customers' communications, such as password reset text messages used for access to important online accounts. If the district court's orders are not reversed, customers, like Terpin, will be left without any remedy for violations of their privacy, including a carrier's disclosure of their private communications to bad actors. AT&T would also be given free rein to ignore its statutory duties to protect the security of its customers through

proper authentication, as required under the FCA and in FCC orders involving AT&T itself.

Accordingly, Appellant respectfully asks that the Court reverse the district court's orders on AT&T's Rule 12(b)(6) and summary judgment motions, enter an order that denies AT&T's motion on summary judgment on proximate causation, and remand this matter for trial.

Dated: July 26, 2023

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP

/s/ Timothy J. Toohey

Pierce O'Donnell
Timothy J. Toohey
Paul A. Blechner
Emily Avazian
Attorneys for Plaintiff-Appellant MICHAEL TERPIN

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 23-53375

I am the attorney or self-represented party.

This brief contains 13,895 **words,** including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- (●) complies with the word limit of Cir. R. 32-1.
- ( ) is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ( ) is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ( ) is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ( ) complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - [ ] it is a joint brief submitted by separately represented parties.
  - [ ] a party or parties are filing a single brief in response to multiple briefs.
  - [ ] a party or parties are filing a single brief in response to a longer joint brief.
- ( ) complies with the length limit designated by court order dated [ ].
- ( ) is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/Timothy J. Toohey **Date** July 26, 2023
*(use "*s/[typed name]*" to sign electronically-filed documents)*

No. 23-55375

IN THE UNITED STATES COURT OF APPEAL

FOR THE NINTH CIRCUIT

MICHAEL TERPIN, *Plaintiff-Appellant*,

v.

AT&T MOBILITY LLC, *Defendant-Appellee*.

On Appeal from the United States District Court
for the Central District of California
Case No. 2:18-cv-06975-ODW-KS

APPELLANT'S ADDENDUM OF AUTHORITIES

VOLUME 1

Pierce O'Donnell
Timothy J. Toohey
Emily Avazian
GREENBERG GLUSKER FIELDS
CLAMAN & MACHTINGER LLP
2049 Century Park East,
Suite 2600
Los Angeles, California 90067
Telephone: (310) 553-3610
Email: POdonnell@ggfirm.com
TToohey@ggfirm.com
EAvazian@ggfirm.com

Attorneys for Plaintiff-Appellant
MICHAEL TERPIN

INDEX

ADDENDUM OF STATUTES, REGULATIONS AND UNPUBLISHED OPINIONS ("ADD")

STATUTES

REGULATORY MATERIALS: FEDERAL COMMMUNICATOINS COMMISSION (FCC)

Document	Description	ADD Nos.
	and Other Customer Information (June 27, 2013)	
29 FCC Rcd 13325, 29 F.C.C.R. 13325, 2014 WL 5439575	*In the Matter of Terracom, Inc. and Yourtel America, Inc. Apparent Liability for Forfeiture* (October 24, 2014)	ADD-180 – ADD-211
30 FCC Rcd. 2808, 30 F.C.C.R. 2808, 2015 WL 1577197	*In the Matter of AT&T Services, Inc.* (April 8, 2015)	ADD-212 – ADD-225
30 FCC Rcd. 7075, 30 F.C.C.R. 7075, 2015 WL 4159266	*In the Matter of Terracom, Inc., and Yourtel America, Inc.* (July 9, 2015)	ADD-226 – ADD-244
30 FCC Rcd. 12302, 30 F.C.C.R. 12302, 2015 WL 6779864	*In the Matter of Cox Communications, Inc.* (November 5, 2015)	ADD-245 – ADD-260
31 FCC Rcd. 13911, 31 F.C.C.R. 13911, 2016 WL 6538282	*In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (November 2, 2016), superseded by Rule *In the Matter of Restoring Internet Freedom*, January 4, 2018	ADD-266 – ADD-493
FCC 20-26, File No.: EB-TCD-18-00027704	*In the Matter of AT&T Inc.: Notice of Apparent Liability for Forfeiture and Admonishment* (February 28, 2020)	ADD-494 – ADD-535
36 FCC Rcd 14120, 36 F.C.C.R. 14120, 2021 WL 4735472	*In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud* (September 30, 2021)	ADD-541 – ADD-587

UNPUBLISHED DECISIONS

United States Code Annotated
Title 47. Telecommunications (Refs & Annos)
Chapter 5. Wire or Radio Communication (Refs & Annos)
Subchapter II. Common Carriers (Refs & Annos)
Part I. Common Carrier Regulation

47 U.S.C.A. § 206

§ 206. Carriers' liability for damages

Currentness

In case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney's fee, to be fixed by the court in every case of recovery, which attorney's fee shall be taxed and collected as part of the costs in the case.

CREDIT(S)

(June 19, 1934, c. 652, Title II, § 206, 48 Stat. 1072.)

Notes of Decisions (64)

47 U.S.C.A. § 206, 47 USCA § 206
Current through P.L.118-7. Some statute sections may be more current, see credits for details.

End of Document

United States Code Annotated
Title 47. Telecommunications (Refs & Annos)
Chapter 5. Wire or Radio Communication (Refs & Annos)
Subchapter II. Common Carriers (Refs & Annos)
Part I. Common Carrier Regulation

47 U.S.C.A. § 222

§ 222. Privacy of customer information

Effective: July 23, 2008
Currentness

(a) In general

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) Confidentiality of carrier information

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) Disclosure on request by customers

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) Aggregate customer information

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

(d) Exceptions

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents--

(1) to initiate, render, bill, and collect for telecommunications services;

(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;

(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)--

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) Subscriber list information

Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) Authority to use location information

For purposes of subsection (c)(1), without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to--

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title), other than in accordance with subsection (d)(4); or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) Subscriber listed and unlisted information for emergency services

Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service or a provider of IP-enabled voice service (as such term is defined in section 615b of this title) shall provide information described in subsection (i)(3)(A)[1] (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

(h) Definitions

As used in this section:

(1) Customer proprietary network information

The term "customer proprietary network information" means--

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

(2) Aggregate information

The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) Subscriber list information

The term "subscriber list information" means any information--

(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

(4) Public safety answering point

The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

(5) Emergency services

The term "emergency services" means 9-1-1 emergency services and emergency notification services.

(6) Emergency notification services

The term "emergency notification services" means services that notify the public of an emergency.

(7) Emergency support services

The term "emergency support services" means information or data base management services used in support of emergency services.

CREDIT(S)

(June 19, 1934, ch. 652, Title II, § 222, as added Pub.L. 104-104, Title VII, § 702, Feb. 8, 1996, 110 Stat. 148; amended Pub.L. 106-81, § 5, Oct. 26, 1999, 113 Stat. 1288; Pub.L. 110-283, Title III, § 301, July 23, 2008, 122 Stat. 2625.)

Notes of Decisions (13)

Footnotes

1 So in original. Probably should be "(h)(3)(A)".

47 U.S.C.A. § 222, 47 USCA § 222
Current through P.L.118-7. Some statute sections may be more current, see credits for details.

End of Document

State of California

CIVIL CODE

Section 1668

1668. All contracts which have for their object, directly or indirectly, to exempt any one from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent, are against the policy of the law.

(Enacted 1872.)

State of California

CIVIL CODE

Section 1670.5

1670.5. (a) If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result.

(b) When it is claimed or appears to the court that the contract or any clause thereof may be unconscionable the parties shall be afforded a reasonable opportunity to present evidence as to its commercial setting, purpose, and effect to aid the court in making the determination.

(Added by Stats. 1979, Ch. 819.)

State of California

CIVIL CODE

Section 1709

1709. One who willfully deceives another with intent to induce him to alter his position to his injury or risk, is liable for any damage which he thereby suffers.

(Enacted 1872.)

State of California

CIVIL CODE

Section 1710

1710. A deceit, within the meaning of the last section, is either:

1. The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;

2. The assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true;

3. The suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact; or,

4. A promise, made without any intention of performing it.

(Enacted 1872.)

State of California

CIVIL CODE

Section 3294

3294. (a) In an action for the breach of an obligation not arising from contract, where it is proven by clear and convincing evidence that the defendant has been guilty of oppression, fraud, or malice, the plaintiff, in addition to the actual damages, may recover damages for the sake of example and by way of punishing the defendant.

(b) An employer shall not be liable for damages pursuant to subdivision (a), based upon acts of an employee of the employer, unless the employer had advance knowledge of the unfitness of the employee and employed him or her with a conscious disregard of the rights or safety of others or authorized or ratified the wrongful conduct for which the damages are awarded or was personally guilty of oppression, fraud, or malice. With respect to a corporate employer, the advance knowledge and conscious disregard, authorization, ratification or act of oppression, fraud, or malice must be on the part of an officer, director, or managing agent of the corporation.

(c) As used in this section, the following definitions shall apply:

(1) "Malice" means conduct which is intended by the defendant to cause injury to the plaintiff or despicable conduct which is carried on by the defendant with a willful and conscious disregard of the rights or safety of others.

(2) "Oppression" means despicable conduct that subjects a person to cruel and unjust hardship in conscious disregard of that person's rights.

(3) "Fraud" means an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury.

(d) Damages may be recovered pursuant to this section in an action pursuant to Chapter 4 (commencing with Section 377.10) of Title 3 of Part 2 of the Code of Civil Procedure based upon a death which resulted from a homicide for which the defendant has been convicted of a felony, whether or not the decedent died instantly or survived the fatal injury for some period of time. The procedures for joinder and consolidation contained in Section 377.62 of the Code of Civil Procedure shall apply to prevent multiple recoveries of punitive or exemplary damages based upon the same wrongful act.

(e) The amendments to this section made by Chapter 1498 of the Statutes of 1987 apply to all actions in which the initial trial has not commenced prior to January 1, 1988.

(Amended by Stats. 1992, Ch. 178, Sec. 5. Effective January 1, 1993.)

Code of Federal Regulations
Title 47. Telecommunication
Chapter I. Federal Communications Commission (Refs & Annos)
Subchapter B. Common Carrier Services
Part 64. Miscellaneous Rules Relating to Common Carriers (Refs & Annos)
Subpart U. Customer Proprietary Network Information (Refs & Annos)

47 C.F.R. § 64.2001

§ 64.2001 Basis and purpose.

Effective: September 21, 2017
Currentness

<Text of section effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

(a) Basis. The rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.

(b) Purpose. The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222.

<Subpart effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the amendatory final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

<The final rule at 82 FR 44118-01, eff. Sept. 21, 2017, states in the summary information that "by operation of the Congressional Review Act, the rule submitted by the FCC shall be treated as if it had never taken effect. However, because the Congressional Review Act does not direct the Office of the Federal Register to remove the voided regulatory text and reissue the pre-existing regulatory text, the FCC issues this document to effect the removal of any amendments, deletions, or other modifications made by the nullified rule, and the reversion to the text of the regulations in effect immediately prior to the effect date of the Report and Order relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.' ">

SOURCE: 56 FR 18523, April 23, 1991; 56 FR 25372, June 4, 1991; 56 FR 36731, Aug. 1, 1991; 57 FR 4740, Feb. 7, 1992; 57 FR 21040, May 18, 1992; 57 FR 48335, Oct. 23, 1992; 57 FR 54331, Nov. 18, 1992; 58 FR 44773, Aug. 25, 1993; 61 FR 24903, May 17, 1996; 61 FR 50246, Sept. 25, 1996; 61 FR 52323, Oct. 7, 1996; 61 FR 59366, Nov. 22, 1996; 62 FR 39779, July 24, 1997; 62 FR 45588, Aug. 28, 1997; 62 FR 47237, Sept. 8, 1997; 62 FR 64758, Dec. 9, 1997; 63 FR 20338, April 24, 1998; 63 FR 43041, Aug. 11, 1998; 64 FR 51469, Sept. 23, 1999; 64 FR 51718, Sept. 24, 1999; 65 FR 38435, June 21, 2000; 65 FR 48396, Aug. 8, 2000; 65 FR 54804, Sept. 11, 2000; 67 FR 9616, March 4, 2002; 67 FR 22007, May 2, 2002; 68 FR 6355, Feb. 7, 2003; 69 FR 62816, Oct. 28, 2004; 76 FR 24400, May 2, 2011; 76 FR 26647, May 9, 2011; 76 FR 43205, July 20, 2011; 76 FR 65969, Oct. 25, 2011; 76 FR 67073, Oct. 31, 2011; 76 FR 73882, Nov. 28, 2011; 77 FR 30919, May 24, 2012; 77 FR 34246, June 11, 2012; 77 FR 71137, Nov. 29, 2012; 81 FR 62825, Sept. 13, 2016; 81 FR 87343, Dec. 2, 2016; 82 FR 7707, Jan. 23, 2017; 82 FR 19325, April 27, 2017; 82 FR 44119, Sept. 21, 2017; 83 FR 1577, Jan. 12, 2018; 83 FR 21737, May 10, 2018; 83 FR 33143, July 17, 2018; 83 FR 47308, Sept. 19, 2018; 83 FR 48963, Sept. 28, 2018; 84 FR 8461, March 8,

2019; 84 FR 45678, Aug. 30, 2019; 85 FR 22043, April 21, 2020; 85 FR 67461, Oct. 23, 2020; 86 FR 40731, July 28, 2021; 87 FR 75513, Dec. 9, 2022, unless otherwise noted.

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401–1473, unless otherwise noted; Pub.L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Current through July 17, 2023, 88 FR 45372. Some sections may be more current. See credits for details.

End of Document

Code of Federal Regulations
Title 47. Telecommunication
Chapter I. Federal Communications Commission (Refs & Annos)
Subchapter B. Common Carrier Services
Part 64. Miscellaneous Rules Relating to Common Carriers (Refs & Annos)
Subpart U. Customer Proprietary Network Information (Refs & Annos)

47 C.F.R. § 64.2003

§ 64.2003 Definitions.

Effective: September 21, 2017
Currentness

<Text of section effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

(a) Account information. "Account information" is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

(b) Address of record. An "address of record," whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

(c) Affiliate. The term "affiliate" has the same meaning given such term in section 3(1) of the Communications Act of 1934, as amended, 47 U.S.C. 153(1).

(d) Call detail information. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

(e) Communications-related services. The term "communications-related services" means telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

(f) Customer. A customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service.

(g) Customer proprietary network information (CPNI). The term "customer proprietary network information (CPNI)" has the same meaning given to such term in section 222(h)(1) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(1).

(h) Customer premises equipment (CPE). The term "customer premises equipment (CPE)" has the same meaning given to such term in section 3(14) of the Communications Act of 1934, as amended, 47 U.S.C. 153(14).

(i) Information services typically provided by telecommunications carriers. The phrase "information services typically provided by telecommunications carriers" means only those information services (as defined in section 3(20) of the Communication Act of 1934, as amended, 47 U.S.C. 153(20)) that are typically provided by telecommunications carriers, such as Internet access or voice mail services. Such phrase "information services typically provided by telecommunications carriers," as used in this subpart, shall not include retail consumer services provided using Internet Web sites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.

(j) Local exchange carrier (LEC). The term "local exchange carrier (LEC)" has the same meaning given to such term in section 3(26) of the Communications Act of 1934, as amended, 47 U.S.C. 153(26).

(k) Opt-in approval. The term "opt-in approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

(l) Opt-out approval. The term "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described in § 64.2008(d)(1) after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart.

(m) Readily available biographical information. "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

(n) Subscriber list information (SLI). The term "subscriber list information (SLI)" has the same meaning given to such term in section 222(h)(3) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(3).

(o) Telecommunications carrier or carrier. The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3(44) of the Communications Act of 1934, as amended, 47 U.S.C. 153(44). For the purposes of this subpart, the term "telecommunications carrier" or "carrier" shall include an entity that provides interconnected VoIP service, as that term is defined in section 9.3 of these rules.

(p) Telecommunications service. The term "telecommunications service" has the same meaning given to such term in section 3(46) of the Communications Act of 1934, as amended, 47 U.S.C. 153(46).

(q) Telephone number of record. The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

(r) Valid photo ID. A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

Credits

[67 FR 59211, Sept. 20, 2002; 72 FR 31961, June 8, 2007; 72 FR 70808, Dec. 13, 2007]

<Subpart effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the amendatory final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

<The final rule at 82 FR 44118-01, eff. Sept. 21, 2017, states in the summary information that "by operation of the Congressional Review Act, the rule submitted by the FCC shall be treated as if it had never taken effect. However, because the Congressional Review Act does not direct the Office of the Federal Register to remove the voided regulatory text and reissue the pre-existing regulatory text, the FCC issues this document to effect the removal of any amendments, deletions, or other modifications made by the nullified rule, and the reversion to the text of the regulations in effect immediately prior to the effect date of the Report and Order relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.' ">

SOURCE: 56 FR 18523, April 23, 1991; 56 FR 25372, June 4, 1991; 56 FR 36731, Aug. 1, 1991; 57 FR 4740, Feb. 7, 1992; 57 FR 21040, May 18, 1992; 57 FR 48335, Oct. 23, 1992; 57 FR 54331, Nov. 18, 1992; 58 FR 44773, Aug. 25, 1993; 61 FR 24903, May 17, 1996; 61 FR 50246, Sept. 25, 1996; 61 FR 52323, Oct. 7, 1996; 61 FR 59366, Nov. 22, 1996; 62 FR 39779, July 24, 1997; 62 FR 45588, Aug. 28, 1997; 62 FR 47237, Sept. 8, 1997; 62 FR 64758, Dec. 9, 1997; 63 FR 20338, April 24, 1998; 63 FR 43041, Aug. 11, 1998; 64 FR 51469, Sept. 23, 1999; 64 FR 51718, Sept. 24, 1999; 65 FR 38435, June 21, 2000; 65 FR 48396, Aug. 8, 2000; 65 FR 54804, Sept. 11, 2000; 67 FR 9616, March 4, 2002; 67 FR 22007, May 2, 2002; 68 FR 6355, Feb. 7, 2003; 69 FR 62816, Oct. 28, 2004; 76 FR 24400, May 2, 2011; 76 FR 26647, May 9, 2011; 76 FR 43205, July 20, 2011; 76 FR 65969, Oct. 25, 2011; 76 FR 67073, Oct. 31, 2011; 76 FR 73882, Nov. 28, 2011; 77 FR 30919, May 24, 2012; 77 FR 34246, June 11, 2012; 77 FR 71137, Nov. 29, 2012; 81 FR 62825, Sept. 13, 2016; 81 FR 87343, Dec. 2, 2016; 82 FR 7707, Jan. 23, 2017; 82 FR 19325, April 27, 2017; 82 FR 44119, Sept. 21, 2017; 83 FR 1577, Jan. 12, 2018; 83 FR 21737, May 10, 2018; 83 FR 33143, July 17, 2018; 83 FR 47308, Sept. 19, 2018; 83 FR 48963, Sept. 28, 2018; 84 FR 8461, March 8, 2019; 84 FR 45678, Aug. 30, 2019; 85 FR 22043, April 21, 2020; 85 FR 67461, Oct. 23, 2020; 86 FR 40731, July 28, 2021; 87 FR 75513, Dec. 9, 2022, unless otherwise noted.

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401–1473, unless otherwise noted; Pub.L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Notes of Decisions (1)

Current through July 17, 2023, 88 FR 45372. Some sections may be more current. See credits for details.

End of Document

Code of Federal Regulations
Title 47. Telecommunication
Chapter I. Federal Communications Commission (Refs & Annos)
Subchapter B. Common Carrier Services
Part 64. Miscellaneous Rules Relating to Common Carriers (Refs & Annos)
Subpart U. Customer Proprietary Network Information (Refs & Annos)

47 C.F.R. § 64.2005

§ 64.2005 Use of customer proprietary network information without customer approval.

Effective: September 21, 2017
Currentness

<Text of section effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

(a) Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

(1) If a telecommunications carrier provides different categories of service, and a customer subscribes to more than one category of service offered by the carrier, the carrier is permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.

(2) If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI with its affiliates, except as provided in § 64.2007(b).

(b) A telecommunications carrier may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from that carrier, unless that carrier has customer approval to do so, except as described in paragraph (c) of this section.

(1) A wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s). A wireline carrier may use, disclose or permit access to CPNI derived from its provision of local exchange service or interexchange service, without customer approval, for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

(2) A telecommunications carrier may not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, a local exchange carrier may not use local service CPNI to track all customers that call local service competitors.

(c) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, as described in this paragraph (c).

(1) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(2) CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.

(3) LECs, CMRS providers, and entities that provide interconnected VoIP service as that term is defined in § 9.3 of this chapter, may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

(d) A telecommunications carrier may use, disclose, or permit access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

Credits

[64 FR 53264, Oct. 1, 1999; 66 FR 7865, Jan. 26, 2001; 67 FR 59211, Sept. 20, 2002; 72 FR 31962, June 8, 2007; 72 FR 70808, Dec. 13, 2007]

<Subpart effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the amendatory final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

<The final rule at 82 FR 44118-01, eff. Sept. 21, 2017, states in the summary information that "by operation of the Congressional Review Act, the rule submitted by the FCC shall be treated as if it had never taken effect. However, because the Congressional Review Act does not direct the Office of the Federal Register to remove the voided regulatory text and reissue the pre-existing regulatory text, the FCC issues this document to effect the removal of any amendments, deletions, or other modifications made by the nullified rule, and the reversion to the text of the regulations in effect immediately prior to the effect date of the Report and Order relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.' ">

SOURCE: 56 FR 18523, April 23, 1991; 56 FR 25372, June 4, 1991; 56 FR 36731, Aug. 1, 1991; 57 FR 4740, Feb. 7, 1992; 57 FR 21040, May 18, 1992; 57 FR 48335, Oct. 23, 1992; 57 FR 54331, Nov. 18, 1992; 58 FR 44773, Aug. 25, 1993; 61 FR 24903, May 17, 1996; 61 FR 50246, Sept. 25, 1996; 61 FR 52323, Oct. 7, 1996; 61 FR 59366, Nov. 22, 1996; 62 FR 39779, July 24, 1997; 62 FR 45588, Aug. 28, 1997; 62 FR 47237, Sept. 8, 1997; 62 FR 64758, Dec. 9, 1997; 63 FR 20338, April 24, 1998; 63 FR 43041, Aug. 11, 1998; 64 FR 51469, Sept. 23, 1999; 64 FR 51718, Sept. 24, 1999; 65 FR 38435, June 21, 2000; 65 FR 48396, Aug. 8, 2000; 65 FR 54804, Sept. 11, 2000; 67 FR 9616, March 4, 2002; 67 FR 22007, May 2, 2002; 68 FR 6355, Feb. 7, 2003; 69 FR 62816, Oct. 28, 2004; 76 FR 24400, May 2, 2011; 76 FR 26647, May 9, 2011; 76 FR 43205, July 20, 2011; 76 FR 65969, Oct. 25, 2011; 76 FR 67073, Oct. 31, 2011; 76 FR 73882, Nov. 28, 2011; 77 FR 30919, May 24, 2012; 77 FR 34246, June 11, 2012; 77 FR 71137, Nov. 29, 2012; 81 FR 62825, Sept. 13, 2016; 81 FR 87343, Dec. 2, 2016; 82 FR 7707, Jan. 23, 2017; 82 FR 19325, April 27, 2017; 82 FR 44119, Sept. 21, 2017; 83 FR 1577, Jan. 12, 2018; 83 FR 21737, May 10, 2018; 83 FR 33143, July 17, 2018; 83 FR 47308, Sept. 19, 2018; 83 FR 48963, Sept. 28, 2018; 84 FR 8461, March 8,

2019; 84 FR 45678, Aug. 30, 2019; 85 FR 22043, April 21, 2020; 85 FR 67461, Oct. 23, 2020; 86 FR 40731, July 28, 2021; 87 FR 75513, Dec. 9, 2022, unless otherwise noted.

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401–1473, unless otherwise noted; Pub.L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Notes of Decisions (10)

Current through July 17, 2023, 88 FR 45372. Some sections may be more current. See credits for details.

End of Document

Code of Federal Regulations
Title 47. Telecommunication
Chapter I. Federal Communications Commission (Refs & Annos)
Subchapter B. Common Carrier Services
Part 64. Miscellaneous Rules Relating to Common Carriers (Refs & Annos)
Subpart U. Customer Proprietary Network Information (Refs & Annos)

47 C.F.R. § 64.2007

§ 64.2007 Approval required for use of customer proprietary network information.

Effective: September 21, 2017
Currentness

<Text of section effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

(a) A telecommunications carrier may obtain approval through written, oral or electronic methods.

(1) A telecommunications carrier relying on oral approval shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part.

(2) Approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by a telecommunications carrier must remain in effect until the customer revokes or limits such approval or disapproval.

(3) A telecommunications carrier must maintain records of approval, whether oral, written or electronic, for at least one year.

(b) Use of opt–out and opt–in approval processes. A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under § 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

Credits
[64 FR 53264, Oct. 1, 1999; 66 FR 7865, Jan. 26, 2001; 67 FR 59212, Sept. 20, 2002; 72 FR 31948, June 8, 2007; 72 FR 31962, June 8, 2007; 72 FR 70808, Dec. 13, 2007]

<Subpart effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the amendatory final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

<The final rule at 82 FR 44118-01, eff. Sept. 21, 2017, states in the summary information that "by operation of the Congressional Review Act, the rule submitted by the FCC shall be treated as if it had never taken effect. However, because the Congressional Review Act does not direct the Office of the Federal Register to remove the voided regulatory text and reissue the pre-existing regulatory text, the FCC issues this document to effect the removal of any amendments, deletions, or other modifications made by the nullified rule, and the reversion to the text of the regulations in effect immediately prior to the effect date of the Report and Order relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.' ">

SOURCE: 56 FR 18523, April 23, 1991; 56 FR 25372, June 4, 1991; 56 FR 36731, Aug. 1, 1991; 57 FR 4740, Feb. 7, 1992; 57 FR 21040, May 18, 1992; 57 FR 48335, Oct. 23, 1992; 57 FR 54331, Nov. 18, 1992; 58 FR 44773, Aug. 25, 1993; 61 FR 24903, May 17, 1996; 61 FR 50246, Sept. 25, 1996; 61 FR 52323, Oct. 7, 1996; 61 FR 59366, Nov. 22, 1996; 62 FR 39779, July 24, 1997; 62 FR 45588, Aug. 28, 1997; 62 FR 47237, Sept. 8, 1997; 62 FR 64758, Dec. 9, 1997; 63 FR 20338, April 24, 1998; 63 FR 43041, Aug. 11, 1998; 64 FR 51469, Sept. 23, 1999; 64 FR 51718, Sept. 24, 1999; 65 FR 38435, June 21, 2000; 65 FR 48396, Aug. 8, 2000; 65 FR 54804, Sept. 11, 2000; 67 FR 9616, March 4, 2002; 67 FR 22007, May 2, 2002; 68 FR 6355, Feb. 7, 2003; 69 FR 62816, Oct. 28, 2004; 76 FR 24400, May 2, 2011; 76 FR 26647, May 9, 2011; 76 FR 43205, July 20, 2011; 76 FR 65969, Oct. 25, 2011; 76 FR 67073, Oct. 31, 2011; 76 FR 73882, Nov. 28, 2011; 77 FR 30919, May 24, 2012; 77 FR 34246, June 11, 2012; 77 FR 71137, Nov. 29, 2012; 81 FR 62825, Sept. 13, 2016; 81 FR 87343, Dec. 2, 2016; 82 FR 7707, Jan. 23, 2017; 82 FR 19325, April 27, 2017; 82 FR 44119, Sept. 21, 2017; 83 FR 1577, Jan. 12, 2018; 83 FR 21737, May 10, 2018; 83 FR 33143, July 17, 2018; 83 FR 47308, Sept. 19, 2018; 83 FR 48963, Sept. 28, 2018; 84 FR 8461, March 8, 2019; 84 FR 45678, Aug. 30, 2019; 85 FR 22043, April 21, 2020; 85 FR 67461, Oct. 23, 2020; 86 FR 40731, July 28, 2021; 87 FR 75513, Dec. 9, 2022, unless otherwise noted.

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401–1473, unless otherwise noted; Pub.L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Notes of Decisions (6)

Current through July 17, 2023, 88 FR 45372. Some sections may be more current. See credits for details.

End of Document

Code of Federal Regulations
Title 47. Telecommunication
Chapter I. Federal Communications Commission (Refs & Annos)
Subchapter B. Common Carrier Services
Part 64. Miscellaneous Rules Relating to Common Carriers (Refs & Annos)
Subpart U. Customer Proprietary Network Information (Refs & Annos)

47 C.F.R. § 64.2008

§ 64.2008 Notice required for use of customer proprietary network information.

Effective: September 21, 2017
Currentness

<Text of section effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

(a) Notification, Generally.

(1) Prior to any solicitation for customer approval, a telecommunications carrier must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

(2) A telecommunications carrier must maintain records of notification, whether oral, written or electronic, for at least one year.

(b) Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.

(c) Content of notice. Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI.

(1) The notification must state that the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI.

(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer

subscribes. However, carriers may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

(4) The notification must be comprehensible and must not be misleading.

(5) If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

(7) A carrier may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. A carrier also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

(8) A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

(9) The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

(10) A telecommunications carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

(d) Notice requirements specific to opt–out. A telecommunications carrier must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph (f) of this section). The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(1) Carriers must wait a 30–day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. A carrier may, in its discretion, provide for a longer period. Carriers must notify customers as to the applicable waiting period for a response before approval is assumed.

(i) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and

(ii) In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.

(2) Carriers using the opt-out mechanism must provide notices to their customers every two years.

(3) Telecommunications carriers that use e-mail to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notification:

(i) Carriers must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

(ii) Carriers must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(iii) Opt-out e-mail notices that are returned to the carrier as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice;

(iv) Carriers that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail; and

(v) Telecommunications carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Carriers may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

(e) Notice requirements specific to opt–in. A telecommunications carrier may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(f) Notice Requirements Specific to One–Time Use of CPNI.

(1) Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

(2) The contents of any such notification must comply with the requirements of paragraph (c) of this section, except that telecommunications carriers may omit any of the following notice provisions if not relevant to the limited use for which the carrier seeks CPNI:

(i) Carriers need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;

(ii) Carriers need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;

(iii) Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use; and

(iv) Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

Credits

[67 FR 59212, Sept. 20, 2002; 72 FR 31948, June 8, 2007]

<Subpart effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the amendatory final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

<The final rule at 82 FR 44118-01, eff. Sept. 21, 2017, states in the summary information that "by operation of the Congressional Review Act, the rule submitted by the FCC shall be treated as if it had never taken effect. However, because the Congressional Review Act does not direct the Office of the Federal Register to remove the voided regulatory text and reissue the pre-existing regulatory text, the FCC issues this document to effect the removal of any amendments, deletions, or other modifications made by the nullified rule, and the reversion to the text of the regulations in effect immediately prior to the effect date of the Report and Order relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.' ">

SOURCE: 56 FR 18523, April 23, 1991; 56 FR 25372, June 4, 1991; 56 FR 36731, Aug. 1, 1991; 57 FR 4740, Feb. 7, 1992; 57 FR 21040, May 18, 1992; 57 FR 48335, Oct. 23, 1992; 57 FR 54331, Nov. 18, 1992; 58 FR 44773, Aug. 25, 1993; 61 FR 24903, May 17, 1996; 61 FR 50246, Sept. 25, 1996; 61 FR 52323, Oct. 7, 1996; 61 FR 59366, Nov. 22, 1996; 62 FR 39779, July 24, 1997; 62 FR 45588, Aug. 28, 1997; 62 FR 47237, Sept. 8, 1997; 62 FR 64758, Dec. 9, 1997; 63 FR 20338, April 24, 1998; 63 FR 43041, Aug. 11, 1998; 64 FR 51469, Sept. 23, 1999; 64 FR 51718, Sept. 24, 1999; 65 FR 38435, June 21, 2000; 65 FR 48396, Aug. 8, 2000; 65 FR 54804, Sept. 11, 2000; 67 FR 9616, March 4, 2002; 67 FR 22007, May 2, 2002; 68 FR 6355, Feb. 7, 2003; 69 FR 62816, Oct. 28, 2004; 76 FR 24400, May 2, 2011; 76 FR 26647, May 9, 2011; 76 FR 43205, July 20, 2011; 76 FR 65969, Oct. 25, 2011; 76 FR 67073, Oct. 31, 2011; 76 FR 73882, Nov. 28, 2011; 77 FR 30919, May 24, 2012; 77 FR 34246, June 11, 2012; 77 FR 71137, Nov. 29, 2012; 81 FR 62825, Sept. 13, 2016; 81 FR 87343, Dec. 2, 2016; 82 FR 7707, Jan. 23, 2017; 82 FR 19325, April 27, 2017; 82 FR 44119, Sept. 21, 2017; 83 FR 1577, Jan. 12, 2018; 83 FR 21737, May 10, 2018; 83 FR 33143, July 17, 2018; 83 FR 47308, Sept. 19, 2018; 83 FR 48963, Sept. 28, 2018; 84 FR 8461, March 8, 2019; 84 FR 45678, Aug. 30, 2019; 85 FR 22043, April 21, 2020; 85 FR 67461, Oct. 23, 2020; 86 FR 40731, July 28, 2021; 87 FR 75513, Dec. 9, 2022, unless otherwise noted.

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401–1473, unless otherwise noted; Pub.L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Current through July 17, 2023, 88 FR 45372. Some sections may be more current. See credits for details.

End of Document

Code of Federal Regulations
Title 47. Telecommunication
Chapter I. Federal Communications Commission (Refs & Annos)
Subchapter B. Common Carrier Services
Part 64. Miscellaneous Rules Relating to Common Carriers (Refs & Annos)
Subpart U. Customer Proprietary Network Information (Refs & Annos)

47 C.F.R. § 64.2009

§ 64.2009 Safeguards required for use of customer proprietary network information.

Effective: September 21, 2017
Currentness

<Text of section effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

(a) Telecommunications carriers must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

(b) Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.

(c) All carriers shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Carriers shall retain the record for a minimum of one year.

(d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06–36, for data pertaining to the previous calendar year.

(f) Carriers must provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

(1) The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

Credits

[64 FR 53264, Oct. 1, 1999; 66 FR 7865, Jan. 26, 2001; 67 FR 59213, Sept. 20, 2002; 72 FR 31948, June 8, 2007; 72 FR 31962, June 8, 2007; 72 FR 70808, Dec. 13, 2007]

<Subpart effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the amendatory final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

<The final rule at 82 FR 44118-01, eff. Sept. 21, 2017, states in the summary information that "by operation of the Congressional Review Act, the rule submitted by the FCC shall be treated as if it had never taken effect. However, because the Congressional Review Act does not direct the Office of the Federal Register to remove the voided regulatory text and reissue the pre-existing regulatory text, the FCC issues this document to effect the removal of any amendments, deletions, or other modifications made by the nullified rule, and the reversion to the text of the regulations in effect immediately prior to the effect date of the Report and Order relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.' ">

SOURCE: 56 FR 18523, April 23, 1991; 56 FR 25372, June 4, 1991; 56 FR 36731, Aug. 1, 1991; 57 FR 4740, Feb. 7, 1992; 57 FR 21040, May 18, 1992; 57 FR 48335, Oct. 23, 1992; 57 FR 54331, Nov. 18, 1992; 58 FR 44773, Aug. 25, 1993; 61 FR 24903, May 17, 1996; 61 FR 50246, Sept. 25, 1996; 61 FR 52323, Oct. 7, 1996; 61 FR 59366, Nov. 22, 1996; 62 FR 39779, July 24, 1997; 62 FR 45588, Aug. 28, 1997; 62 FR 47237, Sept. 8, 1997; 62 FR 64758, Dec. 9, 1997; 63 FR 20338, April 24, 1998; 63 FR 43041, Aug. 11, 1998; 64 FR 51469, Sept. 23, 1999; 64 FR 51718, Sept. 24, 1999; 65 FR 38435, June 21, 2000; 65 FR 48396, Aug. 8, 2000; 65 FR 54804, Sept. 11, 2000; 67 FR 9616, March 4, 2002; 67 FR 22007, May 2, 2002; 68 FR 6355, Feb. 7, 2003; 69 FR 62816, Oct. 28, 2004; 76 FR 24400, May 2, 2011; 76 FR 26647, May 9, 2011; 76 FR 43205, July 20, 2011; 76 FR 65969, Oct. 25, 2011; 76 FR 67073, Oct. 31, 2011; 76 FR 73882, Nov. 28, 2011; 77 FR 30919, May 24, 2012; 77 FR 34246, June 11, 2012; 77 FR 71137, Nov. 29, 2012; 81 FR 62825, Sept. 13, 2016; 81 FR 87343, Dec. 2, 2016; 82 FR 7707, Jan. 23, 2017; 82 FR 19325, April 27, 2017; 82 FR 44119, Sept. 21, 2017; 83 FR 1577, Jan. 12, 2018; 83 FR 21737, May 10, 2018; 83 FR 33143, July 17, 2018; 83 FR 47308, Sept. 19, 2018; 83 FR 48963, Sept. 28, 2018; 84 FR 8461, March 8, 2019; 84 FR 45678, Aug. 30, 2019; 85 FR 22043, April 21, 2020; 85 FR 67461, Oct. 23, 2020; 86 FR 40731, July 28, 2021; 87 FR 75513, Dec. 9, 2022, unless otherwise noted.

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401–1473, unless otherwise noted; Pub.L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Current through July 17, 2023, 88 FR 45372. Some sections may be more current. See credits for details.

End of Document

Code of Federal Regulations
Title 47. Telecommunication
Chapter I. Federal Communications Commission (Refs & Annos)
Subchapter B. Common Carrier Services
Part 64. Miscellaneous Rules Relating to Common Carriers (Refs & Annos)
Subpart U. Customer Proprietary Network Information (Refs & Annos)

47 C.F.R. § 64.2010

§ 64.2010 Safeguards on the disclosure of customer proprietary network information.

Effective: September 21, 2017
Currentness

<Text of section effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

(a) Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

(b) Telephone access to CPNI. Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) Online access to CPNI. A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

(d) In-store access to CPNI. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.

(e) Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords. To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost

or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(f) Notification of account changes. Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

(g) Business customer exemption. Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

Credits

[72 FR 31962, June 8, 2007; 72 FR 70808, Dec. 13, 2007]

<Subpart effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the amendatory final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

<The final rule at 82 FR 44118-01, eff. Sept. 21, 2017, states in the summary information that "by operation of the Congressional Review Act, the rule submitted by the FCC shall be treated as if it had never taken effect. However, because the Congressional Review Act does not direct the Office of the Federal Register to remove the voided regulatory text and reissue the pre-existing regulatory text, the FCC issues this document to effect the removal of any amendments, deletions, or other modifications made by the nullified rule, and the reversion to the text of the regulations in effect immediately prior to the effect date of the Report and Order relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.' ">

SOURCE: 56 FR 18523, April 23, 1991; 56 FR 25372, June 4, 1991; 56 FR 36731, Aug. 1, 1991; 57 FR 4740, Feb. 7, 1992; 57 FR 21040, May 18, 1992; 57 FR 48335, Oct. 23, 1992; 57 FR 54331, Nov. 18, 1992; 58 FR 44773, Aug. 25, 1993; 61 FR 24903, May 17, 1996; 61 FR 50246, Sept. 25, 1996; 61 FR 52323, Oct. 7, 1996; 61 FR 59366, Nov. 22, 1996; 62 FR 39779, July 24, 1997; 62 FR 45588, Aug. 28, 1997; 62 FR 47237, Sept. 8, 1997; 62 FR 64758, Dec. 9, 1997; 63 FR 20338, April 24, 1998; 63 FR 43041, Aug. 11, 1998; 64 FR 51469, Sept. 23, 1999; 64 FR 51718, Sept. 24, 1999; 65 FR 38435, June 21, 2000; 65 FR 48396, Aug. 8, 2000; 65 FR 54804, Sept. 11, 2000; 67 FR 9616, March 4, 2002; 67 FR 22007, May 2, 2002; 68 FR 6355, Feb. 7, 2003; 69 FR 62816, Oct. 28, 2004; 76 FR 24400, May 2, 2011; 76 FR 26647, May 9, 2011; 76 FR 43205, July 20, 2011; 76 FR 65969, Oct. 25, 2011; 76 FR 67073, Oct. 31, 2011; 76 FR 73882, Nov. 28, 2011; 77 FR 30919, May 24, 2012; 77 FR 34246, June 11, 2012; 77 FR 71137, Nov. 29, 2012; 81 FR 62825, Sept. 13, 2016; 81 FR 87343, Dec. 2, 2016; 82 FR 7707, Jan. 23, 2017; 82 FR 19325, April 27, 2017; 82 FR 44119, Sept. 21, 2017; 83 FR 1577, Jan. 12, 2018; 83 FR 21737, May 10, 2018; 83 FR 33143, July 17, 2018; 83 FR 47308, Sept. 19, 2018; 83 FR 48963, Sept. 28, 2018; 84 FR 8461, March 8, 2019; 84 FR 45678, Aug. 30, 2019; 85 FR 22043, April 21, 2020; 85 FR 67461, Oct. 23, 2020; 86 FR 40731, July 28, 2021; 87 FR 75513, Dec. 9, 2022, unless otherwise noted.

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401–1473, unless otherwise noted; Pub.L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Current through July 17, 2023, 88 FR 45372. Some sections may be more current. See credits for details.

End of Document

KeyCite Yellow Flag - Negative Treatment
Proposed Regulation

Code of Federal Regulations
Title 47. Telecommunication
Chapter I. Federal Communications Commission (Refs & Annos)
Subchapter B. Common Carrier Services
Part 64. Miscellaneous Rules Relating to Common Carriers (Refs & Annos)
Subpart U. Customer Proprietary Network Information (Refs & Annos)

47 C.F.R. § 64.2011

§ 64.2011 Notification of customer proprietary network information security breaches.

Effective: September 21, 2017
Currentness

<Text of section effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

(a) A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b) of this section.

(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni.

(1) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (b)(2) and (b)(3) of this section.

(2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (b)(1) of this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears

that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

(c) Customer notification. After a telecommunications carrier has completed the process of notifying law enforcement pursuant to paragraph (b) of this section, it shall notify its customers of a breach of those customers' CPNI.

(d) Recordkeeping. All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.

(e) Definitions. As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

(f) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

Credits

[72 FR 31963, June 8, 2007; 72 FR 70808, Dec. 13, 2007]

<Subpart effective prior to revision of Subpart U by 81 FR 87274, effective Jan. 3, 2017. On April 3, 2017, Congress disapproved the amendatory final rule (81 FR 87274), stating that "such rule shall have no force or effect". See PL 115-22, April 3, 2017, 131 Stat 88.>

<The final rule at 82 FR 44118-01, eff. Sept. 21, 2017, states in the summary information that "by operation of the Congressional Review Act, the rule submitted by the FCC shall be treated as if it had never taken effect. However, because the Congressional Review Act does not direct the Office of the Federal Register to remove the voided regulatory text and reissue the pre-existing regulatory text, the FCC issues this document to effect the removal of any amendments, deletions, or other modifications made by the nullified rule, and the reversion to the text of the regulations in effect immediately prior to the effect date of the Report and Order relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.' ">

SOURCE: 56 FR 18523, April 23, 1991; 56 FR 25372, June 4, 1991; 56 FR 36731, Aug. 1, 1991; 57 FR 4740, Feb. 7, 1992; 57 FR 21040, May 18, 1992; 57 FR 48335, Oct. 23, 1992; 57 FR 54331, Nov. 18, 1992; 58 FR 44773, Aug. 25, 1993; 61 FR 24903, May 17, 1996; 61 FR 50246, Sept. 25, 1996; 61 FR 52323, Oct. 7, 1996; 61 FR 59366, Nov. 22, 1996; 62 FR 39779, July 24, 1997; 62 FR 45588, Aug. 28, 1997; 62 FR 47237, Sept. 8, 1997; 62 FR 64758, Dec. 9, 1997; 63 FR 20338, April 24, 1998; 63 FR 43041, Aug. 11, 1998; 64 FR 51469, Sept. 23, 1999; 64 FR 51718, Sept. 24, 1999; 65 FR 38435, June 21, 2000; 65 FR 48396, Aug. 8, 2000; 65 FR 54804, Sept. 11, 2000; 67 FR 9616, March 4, 2002; 67 FR 22007, May 2, 2002; 68 FR 6355, Feb. 7, 2003; 69 FR 62816, Oct. 28, 2004; 76 FR 24400, May 2, 2011; 76 FR 26647, May 9, 2011; 76 FR 43205, July 20, 2011; 76 FR 65969, Oct. 25, 2011; 76 FR 67073, Oct. 31, 2011; 76 FR 73882, Nov. 28, 2011; 77 FR 30919, May 24, 2012; 77 FR 34246, June 11, 2012; 77 FR 71137, Nov. 29, 2012; 81 FR 62825, Sept. 13, 2016; 81 FR 87343, Dec. 2, 2016; 82 FR 7707, Jan. 23, 2017; 82 FR 19325, April 27, 2017; 82 FR 44119, Sept. 21, 2017; 83 FR 1577, Jan. 12, 2018; 83 FR 21737, May 10, 2018; 83 FR 33143, July 17, 2018; 83 FR 47308, Sept. 19, 2018; 83 FR 48963, Sept. 28, 2018; 84 FR 8461, March 8,

2019; 84 FR 45678, Aug. 30, 2019; 85 FR 22043, April 21, 2020; 85 FR 67461, Oct. 23, 2020; 86 FR 40731, July 28, 2021; 87 FR 75513, Dec. 9, 2022, unless otherwise noted.

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401–1473, unless otherwise noted; Pub.L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Current through July 17, 2023, 88 FR 45372. Some sections may be more current. See credits for details.

End of Document

22 FCC Rcd. 6927 (F.C.C.), 22 F.C.C.R. 6927, 40 Communications Reg. (P&F) 1282, 2007 WL 983953

NOTE: An Erratum is attached to the end of this document

Federal Communications Commission (F.C.C.)
Report and Order and Further Notice of Proposed Rulemaking

IN THE MATTER OF IMPLEMENTATION OF THE TELECOMMUNICATIONS ACT OF 1996: TELECOMMUNICATIONS CARRIERS' USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION AND OTHER CUSTOMER INFORMATION

CC 96-115

IP-ENABLED SERVICES

WC 04-36
FCC 07-22
Adopted: March 13, 2007
Released: April 2, 2007
Comment Date: [30 days after publication in the Federal Register]
Reply Comment Date: [60 days after publication in the Federal Register]

****1 *6928** By the Commission: Chairman Martin issuing a separate statement; Commissioners Copps and Adelstein dissenting in part and issuing separate statements; Commissioner Tate concurring in part and issuing a separate statement; Commissioner McDowell issuing a separate statement.

I. INTRODUCTION

1. In this Order, the Commission responds to the practice of "pretexting"[1] by strengthening our rules to protect the privacy of customer proprietary network information (CPNI)[2] that is collected and held by providers of communications services (hereinafter, communications carriers or carriers).[3] Section 222 of the Communications Act requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure.[4] Today, we strengthen our privacy rules by adopting additional safeguards to protect customers' CPNI against unauthorized access and disclosure.

2. Our Order is directly responsive to the actions of data brokers, or pretexters, to obtain unauthorized access to CPNI. As the Electronic Privacy Information Center (EPIC) pointed out in its ***6929** petition that led to this rulemaking proceeding,[5] numerous websites advertise the sale of personal telephone records for a price. These data brokers have been able to obtain private and personal information, including what calls were made to and/or from a particular telephone number and the duration of such calls. In many cases, the data brokers claim to be able to provide this information within fairly quick time frames, ranging from a few hours to a few days. The additional privacy safeguards we adopt today will sharply limit pretexters' ability to obtain unauthorized access to this type of personal customer information from carriers we regulate. We also adopt a Further Notice of Proposed Rulemaking seeking comment on what steps the Commission should take, if any, to secure further the privacy of customer information.

II. EXECUTIVE SUMMARY

3. As discussed below, we take the following actions to secure CPNI:
• **Carrier Authentication Requirements.** We prohibit carriers from releasing call detail information to customers during

customer-initiated telephone contact except when the customer provides a password. If a customer does not provide a password, we prohibit the release of call detail information except by sending it to an address of record or by the carrier calling the customer at the telephone of record. We also require carriers to provide mandatory password protection for online account access. However, we permit carriers to provide CPNI to customers based on in-store contact with a valid photo ID.

2 • **Notice to Customer of Account Changes. We require carriers to notify the customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.

• **Notice of Unauthorized Disclosure of CPNI.** We establish a notification process for both law enforcement and customers in the event of a CPNI breach.

• **Joint Venture and Independent Contractor Use of CPNI.** We modify our rules to require carriers to obtain opt-in consent from a customer before disclosing a customer's CPNI to a carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer.

• **Annual CPNI Certification.** We amend the Commission's rules and require carriers to file with the Commission an annual certification, including an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the previous year regarding the unauthorized release of CPNI.

• **CPNI Regulations Applicable to Providers of Interconnected VoIP Service.** We extend the application of the CPNI rules to providers of interconnected VoIP service.

• **Enforcement Proceedings.** We require carriers to take reasonable measures to discover and protect against pretexting, and, in enforcement proceedings, will infer from evidence of unauthorized disclosures of CPNI that reasonable precautions were not taken.

• **Business Customers.** In limited circumstances, we permit carriers to bind themselves contractually to authentication regimes other than those adopted in this Order for services they *6930 provide to their business customers that have a dedicated account representative and contracts that specifically address the carrier's protection of CPNI.

III. BACKGROUND

A. Section 222 and the Commission's CPNI Rules

4. *Statutory Authority*. In section 222, Congress created a framework to govern telecommunications carriers' protection and use of information obtained by virtue of providing a telecommunications service.[6] The section 222 framework calibrates the protection of such information from disclosure based on the sensitivity of the information. Thus, section 222 places fewer restrictions on the dissemination of information that is not highly sensitive and on information the customer authorizes to be released, than on the dissemination of more sensitive information the carrier has gathered about particular customers.[7] Congress accorded CPNI, the category of customer information at issue in this Order, the greatest level of protection under this framework.

5. CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue *6931 of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[8] Practically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting. CPNI therefore includes some highly-sensitive personal information.

**3 6. Section 222 reflects the balance Congress sought to achieve between giving each customer ready access to his or her own CPNI, and protecting customers from unauthorized use or disclosure of CPNI. Every telecommunications carrier has a

general duty pursuant to section 222(a) to protect the confidentiality of CPNI.[9] In addition, section 222(c)(1) provides that a carrier may only use, disclose, or permit access to customers' CPNI in limited circumstances: (1) as required by law;[10] (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[11] Section 222 also guarantees that customers have a right to obtain access to, and compel disclosure of, their own CPNI.[12] Specifically, pursuant to section 222(c)(2), every telecommunications carrier must disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer."[13]

7. *Existing Safeguards*. On February 26, 1998, the Commission released the *CPNI Order* in which it adopted a set of rules implementing section 222.[14] The Commission's CPNI rules have been amended from time to time since the *CPNI Order*, primarily in respects that do not directly impact the issues raised in this Order. Here, we focus on the substance of the Commission's rules most relevant to this Order, and briefly review the history of the creation of those rules only to the extent necessary to provide appropriate context for the actions we take today.[15]

8. In the *CPNI Order* and subsequent orders, the Commission promulgated rules implementing the express statutory obligations of section 222. Included among the Commission's CPNI regulations implementing the express statutory obligations of section 222 are requirements outlining the extent to which section 222 permits carriers to use CPNI to render the telecommunications service from which the CPNI was derived.[16] Beyond such use, the Commission's rules require carriers to obtain a customer's ***6932** knowing consent before using or disclosing CPNI. As most relevant to this Order, under the Commission's existing rules, telecommunications carriers must receive opt-out consent before disclosing CPNI to joint venture partners and independent contractors for the purposes of marketing communications-related services to customers.[17] Consistent with section 222(c)(2), the Commission's rules recognize that a carrier must comply with the express desire of a customer seeking the disclosure of his or her CPNI.[18]

9. In addition to adopting restrictions on the use and disclosure of CPNI, the Commission in the *CPNI Order* also adopted a set of rules designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI.[19] Among these safeguards are rules that require carriers to design their customer service records in such a way that the status of a customer's CPNI approval can be clearly established.[20] The Commission also requires telecommunications carriers to train their personnel as to when they are and are not authorized to use CPNI, and requires carriers to have an express disciplinary process in place.[21] The Commission's safeguard rules also require carriers to maintain records that track access to customer CPNI records. Specifically, section 64.2009(c) of the Commission's rules requires carriers to "maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI," and to maintain such records for a period of at least one year.[22] The Commission's safeguard rules also require the establishment of a supervisory review process for outbound marketing campaigns.[23] Finally, the Commission requires each carrier to certify annually regarding its compliance with the carrier's CPNI requirements and to make this certification publicly available.[24]

6933 B. *IP-Enabled Services Notice

****4** 10. On March 10, 2004, the Commission initiated a proceeding to examine issues relating to Internet Protocol (IP)-enabled services -- services and applications making use of IP, including, but not limited to VoIP services.[25] In the *IP-Enabled Notice*, the Commission sought comment on, among other things, whether to extend the CPNI requirements to any provider of VoIP or other IP-enabled services.[26]

C. *EPIC CPNI Notice*

11. On August 30, 2005, EPIC filed a petition with the Commission asking the Commission to investigate telecommunications carriers' current security practices and to initiate a rulemaking proceeding to consider establishing more stringent security standards for telecommunications carriers to govern the disclosure of CPNI.[27] In particular, EPIC proposed that the Commission consider requiring the use of consumer-set passwords, creating audit trails, employing encryption, limiting data retention, and improving notice procedures.[28] On February 14, 2006, the Commission released the *EPIC CPNI Notice*, in which it sought comment on (a) the nature and scope of the problem identified by EPIC, including pretexting, and (b) what additional steps, if any, the Commission should take to protect further the privacy of CPNI.[29] Specifically, the Commission sought comment on the five EPIC proposals listed above. In addition, the Commission tentatively concluded

that it should amend its rules to require carriers annually to file their section 64.2009(e) certifications with the Commission.[30] It also sought comment on whether it should require carriers to obtain a customer's opt-in consent before the carrier shares CPNI with its joint venture partners and independent contractors; whether to impose rules relating to how carriers verify customers' identities; whether to adopt a set of security requirements that could be used as the basis for liability if a carrier failed to implement such requirements, or adopt a set of security requirements that a carrier could implement to exempt itself from liability; whether VoIP service providers or other IP-enabled service providers should be covered by any new rules the Commission adopts in the present rulemaking; and other specific proposals that might increase the protection of CPNI.

IV. DISCUSSION

12. In this Order, we adopt necessary protections put forward by EPIC to ensure the privacy of CPNI. The carriers' record on protecting CPNI demonstrates that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI.[31] The Attorneys ***6934** General of dozens of states cite numerous suits by telecommunications carriers seeking to enjoin pretexting activities -- a clear indication that pretexters have been successful at gaining unauthorized access to CPNI.[32] Cingular,[33] Sprint,[34] T-Mobile,[35] Verizon Wireless[36] and other companies have sued ***6935** dozens of people whom they accuse of fraudulently obtaining phone records.[37] In one of the cases filed by Cingular, Cingular states in a court-filed affidavit that certain defendants or their agents posed as an employee/agent of Cingular and as a customer of the carrier to induce Cingular's customer service representative to provide them with the call records of a targeted customer.[38] The Federal Trade Commission has also filed suits against several pretexters under laws barring unfair and deceptive practices.[39] Additionally, numerous states, including California,[40] Florida,[41] Illinois,[42] Missouri,[43] and Texas[44] have all sued data brokers for pretexting phone records.

*6936 A. Carrier Authentication Requirements

1. Customer-Initiated Telephone Account Access

****5** 13. We find that the release of call detail[45] over the telephone presents an immediate risk to privacy and therefore we prohibit carriers from releasing call detail information based on customer-initiated telephone contact except under three circumstances.[46] First, a carrier can release call detail information if the customer provides the carrier with a pre-established password.[47] Second, a carrier may, at the customer's request, send call detail information to the customer's address of record.[48] Third, a carrier may call the telephone number of record and disclose call detail information.[49] A carrier may disclose non-call detail CPNI to a customer after the carrier authenticates the customer.[50]

***6937** 14. The record reflects that pretexters use evolving methods to trick employees at customer service call centers into releasing call detail information.[51] This release of call detail through customer-initiated telephone contact presents heightened privacy concerns because of pretexters' abilities to circumvent carrier authentication requirements and gain immediate access to call detail.[52] By restricting the ways in which carriers release call detail in response to customer-initiated telephone calls, we place at most a minimal inconvenience on carriers and consumers.[53]

15. *Establishment of Password Protection*. For new customers, carriers may request that the customer establish a password at the time of service initiation because the carrier can easily authenticate the customer at that time.[54] For existing customers to establish a password, a carrier must first authenticate the customer without the use of readily available biographical information,[55] or account information.[56] For example, a carrier could call the customer at the telephone number of record.[57] If a ***6938** carrier already has password protection in place for a customer account, a carrier does not have to reinitialize a customer password.[58] By permitting the carrier to determine its authentication method, the carrier has the most flexibility for designing an authentication program that can continue to evolve to fight against pretexting efforts.

16. *Use of Password Protection*. For accounts that are password protected, a carrier cannot obtain the customer's password by asking for readily available biographical information, or account information, to prompt the customer for his password.[59] We understand, of course, that passwords can be lost or forgotten, and share commenters' concern that security measures should not unnecessarily inconvenience customers or impair customer service systems.[60] We therefore allow carriers to create back-up customer authentication methods for lost or forgotten passwords that are also not based on readily available biographical information, or account information.[61] For example, the Attorneys General support the use of a shared secret back-up authentication procedure for lost or forgotten passwords.[62] As further account protection, with a shared secret

back-up authentication program, the carrier may offer the opportunity for the customer to design the shared secret question.[63] We find that limiting back-up authentication methods to those that do not include readily available biographical information, or account information, will protect customers most effectively from pretexters.

**6 *6939 17. Although we recognize that carriers and customers will be subject to a one-time burden to implement password protection if a customer is interested in gaining access to call detail during a customer-initiated telephone call, we believe that the ongoing burdens of these authentication requirements will be minimal. Further, this method balances consumers' interests in ready access to their call detail, and carriers' interests in providing efficient customer service, with the public interest in maintaining the security and confidentiality of call detail information.

18. *Alternative Access to Call Detail Information*. If a customer does not want to establish a password, the customer may still access call detail information, based on a customer-initiated telephone call, by asking the carrier to send the call detail information to an address of record or by the carrier calling the telephone number of record.[64] Because we provide multiple methods for the customer to access call detail based on a customer-initiated telephone call, neither customers who dislike passwords nor carriers concerned about timely customer service should find our requirements burdensome.[65] Furthermore, by providing a variety of secure means for customers to receive call detail information from carriers, and focusing on one of the most problematic means of pretexting -- obtaining call detail information from customer service representatives without proper identity screening -- our rules are no more extensive than necessary to protect consumers' privacy with respect to telephone access to account information.[66]

19. We do not intend for the prohibition on the release of call detail over the telephone for customer-initiated telephone contact to hinder routine carrier-customer relations regarding service/billing disputes and questions.[67] If a customer is able to provide to the carrier, during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call), then the carrier is permitted to proceed with its routine customer care procedures.[68] We believe that if a customer is able to provide this information to the carrier, without carrier assistance, then the carrier does not violate our rules if it takes routine customer service actions related to such information. We additionally clarify that under these circumstances, carriers may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password. Our rule is intended to prevent pretexter phishing and other pretexter methods for gaining unauthorized access to customer account information.

***6940 2. Online Account Access**

20. We also require carriers to password protect online access to CPNI.[69] Although section 222 of the Act imposes a duty on carriers to protect the privacy of CPNI,[70] data brokers and others have been able to access CPNI online without the account holder's knowledge or consent.[71] We agree with EPIC that the apparent ease with which data brokers have been able to access CPNI online demonstrates the insufficiency of carriers' customer authentication procedures.[72] In particular, the record evidence demonstrates that some carriers permit customers to establish online accounts by providing readily available biographical information.[73] Thus, a data broker may obtain online account access easily without the customer's knowledge. Therefore, we agree with EPIC and others that use of such identifiers is an insufficient mechanism for preventing data brokers from obtaining unauthorized online access to CPNI.[74]

7 21. To close this gap, we prohibit carriers from relying on readily available biographical information, or account information to authenticate a customer's identity before a customer accesses CPNI online. In addition, because a carrier is responsible to ensure the security and privacy of online account access, a carrier must appropriately authenticate both new and existing customers seeking access ***6941 to CPNI online.[75] However, we do not require carriers to reinitialize existing passwords for online customer accounts, but a carrier cannot base online access *solely* on readily available biographical information, or account information, or prompts for such information.[76]

22. As with the password protection for the release of call detail during customer-initiated telephone contact, we understand that passwords for online access can also be lost or forgotten, and share commenters' concern that security measures should not unnecessarily inconvenience customers or impair customer service systems.[77] We therefore allow carriers to create back-up customer authentication methods for lost or forgotten passwords in line with the back-up authentication method framework established for the password protection for customer-initiated telephone contact.[78] Further, if a customer cannot

provide a password or the proper response for the back-up authentication method to access an online account, the carrier must reauthenticate the customer based on the authentication methods adopted in this Order prior to the customer gaining online access to CPNI.[79] Finally, as with the establishment of the password for the release of call detail for customer-initiated telephone contact, although we recognize that carriers and customers will be subject to a one-time burden to implement this Order, we believe the ongoing burdens of these authentication requirements will be minimal and are outweighed by the benefits to consumer privacy.

3. Carrier Retail Location Account Access

23. We continue to allow carriers to provide customers with access to CPNI at a carrier's retail location if the customer presents a valid photo ID[80] and the valid photo ID matches the name on the account.[81] We agree with the Attorneys General and find that this is a secure authentication practice because it enables the carrier to make a reasonable judgment about the customer's identity.[82]

***6942 4. Notification of Account Changes**

24. We require carriers to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication,[83] online account, or address of record is created or changed.[84] We agree with the New Jersey Ratepayer Advocate that this notification is an important tool for customers to monitor their account's security.[85] This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, as to reasonably ensure that the customer receives this notification.[86] We believe this measure is appropriate to protect customers from data brokers that might otherwise manage to circumvent the authentication protections we adopt in this Order, and to take appropriate action in the event of pretexter activity. Further, we find that this notification requirement will also empower customers to provide carriers with timely information about pretexting activity, which the carriers may not be able to identify easily.[87]

5. Business Customer Exemption

****8** 25. We do make an exception to the rules that we adopt today for certain business customers. We agree with commenters who argue that privacy concerns of telecommunications consumers are greatest when using personal telecommunications services.[88] Indeed, the fraudulent practices described by EPIC have mainly targeted individual consumers, and the record indicates that the proprietary information of wireline and wireless business account customers already is subject to stringent safeguards, which are privately negotiated by contract.[89] Therefore, if the carrier's contract with a business customer is serviced by a dedicated account representative as the primary contact, and specifically addresses the carrier's protection of CPNI, we do not extend our carrier authentication rules to cover these business customers because businesses are typically able to negotiate the appropriate ***6943** protection of CPNI in their service agreements.[90] However, nothing in this Order exempts carriers serving wireline enterprise and wireless business account customers from section 222 or the remainder of the Commission's CPNI rules.

B. Notice of Unauthorized Disclosure of CPNI

26. We agree with EPIC that carriers should be required to notify a customer whenever a security breach results in that customer's CPNI being disclosed to a third party without that customer's authorization.[91] However, we also appreciate law enforcement's concern about delaying customer notification in order to allow law enforcement to investigate crimes.[92] Therefore, we adopt a rule that we believe balances a customer's need to know with law enforcement's ability to undertake an investigation of suspected criminal activity, which itself might advance the goal of consumer protection.[93]

27. In conjunction with the general rulemaking authority under the Act,[94] section 222(a), which imposes a duty on "[e]very telecommunications carrier . . . to protect the confidentiality of proprietary information," provides ample authority for the Commission to require carriers to report CPNI breaches to law enforcement and prohibit them from disclosing breaches to their customers until after law enforcement has been notified. Notifying law enforcement of CPNI breaches is consistent with the goal of protecting CPNI. Law enforcement can investigate the breach, which could result in legal action against the perpetrators, thus ensuring that they do not continue to breach CPNI. When and if law enforcement determines how the breach occurred, moreover, it can advise the carrier and the Commission, enabling industry to take steps to prevent future

breaches of that kind. Because law enforcement will be informed of all breaches, it will be better positioned than individual carriers to develop expertise about the methods and motives associated with CPNI breaches. Again, this should enable law enforcement to advise industry, the Commission, and perhaps Congress regarding additional measures that might prevent future breaches.

**9 28. The requirement that carriers delay customer notification of breaches until after law enforcement has been notified is also consistent with these goals. Once customers have been notified, a breach may become public knowledge, thereby impeding law enforcement's ability to investigate the *6944 breach, identify the perpetrators, and determine how the breach occurred. In short, immediate customer notification may compromise all the benefits of requiring carriers to notify law enforcement of CPNI breaches. A short delay is warranted, therefore, with the proviso that carriers may notify customers if there is an urgent need to do so to avoid immediate and irreparable harm.

29. A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).[95] A telecommunications carrier may notify the customer and/or disclose the breach publicly after seven business days following notification to the USSS and the FBI, if the USSS and the FBI have not requested that the telecommunications carrier continue to postpone disclosure.[96] A telecommunications carrier, however, may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if the carrier believes that there is an extraordinarily urgent need to notify a customer or class of customers in order to avoid immediate and irreparable harm.[97] Additionally, we require carriers to maintain a record of any discovered breaches, notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two years. This record must include, if available, the date that the carrier discovered the breach, the date that the carrier notified the USSS and the FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach.

30. We reject commenters' argument that the Commission need not impose new rules about notice to customers of unauthorized disclosure because competitive market conditions will protect CPNI from unauthorized disclosure.[98] If customers and law enforcement agencies are unaware of pretexting activity, unauthorized releases of CPNI will have little impact on carriers' behavior, and thus provide little incentive for carriers to prevent further unauthorized releases.[99] By mandating the notification process adopted here, we better empower consumers to make informed decisions about service providers and assist law enforcement with its investigations. This notice will also empower carriers and consumers to take whatever "next steps" are appropriate in light of the customer's particular situation.[100]

31. We clarify, however, that nothing in today's Order is intended to alter existing law regarding customer notification of law enforcement access to customer records. Therefore, for example, when CPNI is disclosed pursuant to the "except as required by law" exception contained in section 222(c)(1), such disclosure does not trigger the carrier's obligation to notify a customer of any "unauthorized" access *6945 to CPNI.[101] We further clarify that nothing in today's Order is intended to mandate customer notice when providers of covered services are permitted by law to disclose customers' personal information, such as to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[102] Further, we do not intend to supersede any statute, regulation, order, or interpretation in any state, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

**10 32. *Content of Customer Notice*. We decline to specify the precise content of the notice that must be provided to customers in the event of a security breach of CPNI. The notice requirement we adopt in this proceeding is general, and we recognize that numerous types of circumstances -- including situations other than pretexting -- could result in the unauthorized disclosure of a customer's CPNI to a third party. Thus, we leave carriers the discretion to tailor the language and method of notification to the circumstances.[103] Finally, we expect carriers to cooperate fully in any law enforcement investigation of such unauthorized release of CPNI or attempted unauthorized access to an account consistent with statutory and Commission requirements.

C. Additional Protection Measures

33. *Guarding Against Pretexting*. We agree with commenters that techniques for fraud vary and tend to become more

sophisticated over time, and that carriers need leeway to engage emerging threats.[104] We therefore clarify that carriers are free to bolster their security measures through additional measures to meet their section 222 obligations to protect the privacy of CPNI.[105] We also codify the existing statutory requirement contained in section 222 of the Act that carriers take reasonable measures to discover and protect against activity that is indicative of pretexting.[106] As we discuss below, adoption of the rules in this Order does not relieve carriers of their fundamental duty to remain vigilant in their protection of CPNI, nor does it necessarily insulate them from enforcement action for unauthorized disclosure of CPNI.

34. Although we expect that carriers will use forms of self-monitoring to comply with this obligation, at this time we allow carriers to determine what specific measures will best enable them to ***6946** ensure compliance with this requirement.[107] By codifying a general requirement to take reasonable measures to discover and protect against activity that is indicative of pretexting, we permit carriers to weigh the benefits and burdens of particular methods of possibly detecting pretexting. This approach will allow carriers to improve the security of CPNI in the most efficient manner possible,[108] and better enable small businesses to comply with our rules.

35. We stress our expectation that carriers will take affirmative measures to discover and protect against activity that is indicative of pretexting beyond what is required by the Commission's current rules,[109] and remind carriers that the Act imposes on them the duty of instituting effective measures to protect the privacy of CPNI.[110] Moreover, as discussed in the Enforcement Section, *infra*,[111] by requiring carriers to demonstrate that they have taken adequate measures to guard against pretexting, we give carriers adequate incentive to uncover situations where they have released CPNI to a third party without authorization. We anticipate that a carrier that practices willful blindness with regard to pretexting would not be able to demonstrate that it has taken sufficient measures to guard against pretexting. Although, we do not adopt specific rules in this Order that fully encompass this affirmative duty, we seek comment in our Further Notice on whether the Commission should require carriers to utilize audit trails and comply with certain data retention requirements.[112]

****11** 36. *Network Security*. In response to EPIC's encryption proposal, we make clear that carriers' existing statutory obligations to protect their customers' CPNI include a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.[113] Although several carriers report that they have looked for, but not found, attempts by outsiders to penetrate their CPNI databases directly,[114] commenters also report that pretexters' methods for gaining access to data evolve over time.[115] As carriers take stronger measures to safeguard CPNI, data brokers may respond by escalating their techniques to access CPNI, such as through hacking. Therefore, although we decline at this time specifically to require carriers to encrypt their CPNI databases, we interpret section 222 as requiring carriers to protect CPNI when it is stored in a carrier's databases.[116]

***6947 D. Joint Venture and Independent Contractor Use of CPNI**

37. We modify our rules to require telecommunications carriers to obtain opt-in consent from a customer before disclosing that customer's CPNI to a carrier's joint venture partner or independent contractor for the purpose of marketing communications-related services to that customer.[117] While we realize that this is a change in Commission policy, we find that new circumstances force us to reassess our existing regulations. As we have found previously, the Commission has a substantial interest in protecting customer privacy.[118] Based on this and in light of new privacy concerns, we now find that an opt-in framework for the sharing of CPNI with joint venture partners and independent contractors for the purposes of marketing communications-related services to a customer both directly advances our interest in protecting customer privacy and is narrowly tailored to achieve our goal of privacy protection. Specifically, an opt-in regime will more effectively limit the circulation of a customer's CPNI by maintaining it in a carrier's possession unless a customer provides informed consent for its release. Moreover, we find that an opt-in regime will provide necessary informed customer choice concerning these information sharing relationships with other companies.

38. In the *Notice*, the Commission sought comment on whether the existing opt-out regime is sufficiently protective of the privacy of CPNI when CPNI is disclosed to telecommunications carriers' joint venture partners and independent contractors, and whether the Commission should instead adopt an opt-in policy for this type of CPNI sharing.[119] The current opt-out regime allows for carriers to share CPNI with joint venture partners and independent contractors for the purposes of marketing communications-related services after providing only a notice to a customer.[120] The burden is then placed on the customer to opt-out of such sharing arrangements. If the customer does not respond, a carrier's sharing of customer information with these entities is allowed.

**12 39. We find that there is a substantial need to limit the sharing of CPNI with others outside a customer's carrier to protect a customer's privacy. The black market for CPNI has grown exponentially with an increased market value placed on obtaining this data, and there is concrete evidence that the dissemination of this private information does inflict specific and significant harm on individuals, including harassment and the use of the data to assume a customer's identity.[121] The reality of this private information being disseminated is well-documented and has already resulted in irrevocable damage to customers.[122] While there are safeguards in our current rules for sharing CPNI with joint venture partners *6948 and independent contractors,[123] we believe that these safeguards do not adequately protect a customer's CPNI in today's environment. Specifically, we find that once the CPNI is shared with a joint venture partner or independent contractor, the carrier no longer has control over it and thus the potential for loss of this data is heightened.[124] We find that a carrier's section 222 duty to protect CPNI extends to situations where a carrier shares CPNI with its joint venture partners and independent contractors. However, because a carrier is no longer in a position to personally protect the CPNI once it is shared -- and section 222's duties may not extend to joint venture partners or independent contractors themselves in all cases -- we find that this sharing of data, while still permitted, warrants a requirement of express prior customer authorization.[125]

40. We agree with commenters that argue that the current opt-out notices allowing carriers to share information with joint venture partners and independent contractors are often vague and not comprehensible to an average customer.[126] Further, we find that many consumer studies on opt-out regimes also reflect this consumer confusion.[127] We do not believe that simply modifying our existing opt-out notice requirements will alleviate these concerns because opt-out notices do not involve a customer actually authorizing the sharing of CPNI in the first instance, but rather leave it to the carrier to decide whether to share it after sending a notice to a customer, which a customer may or may not have read.[128] While many customers accept and understand that carriers will share their information with affiliates and agents -- as provided in our existing opt-out rules -- there is less customer willingness for their information to be shared without their express authorization with others outside the carrier-customer relationship.[129]

41. We disagree with commenters that assert that an opt-in approach will not serve to remedy the concerns raised in this proceeding.[130] The Attorneys General note that since February 2005, security breaches have resulted in the personal information of over 54 million Americans being compromised.[131] With the growing interest in obtaining customer CPNI and the resulting increase in the number of security breaches, carriers must be more vigilant in protecting a customer's CPNI from unauthorized disclosure.[132] It stands to reason that placing customers' personal data in the hands of companies outside the carrier- *6949 customer relationship places customers at increased risk, not only of inappropriate handling of the information, but also of innocent mishandling or loss of control over it. Further, we find that an opt-in regime will clarify carriers' information sharing practices because it will force carriers to provide clear and comprehensible notices to their customers in order to gain their express authorization to engage in such activity.

**13 42. We also disagree with commenters that argue that the current opt-out approach is sufficient, and that in the event of a breach, a carrier can terminate its relationship with the joint venture partner or independent contractor, or that the Commission can simply deal with the situation through an enforcement proceeding.[133] We find that in the event of a breach of CPNI security, the damage is already inflicted upon the customer. We also find that the carrier cannot simply rectify the situation by terminating its agreement nor can the Commission completely alleviate a customer's concerns about the privacy invasion through an enforcement proceeding.[134]

43. This minor modification of our rules seeks to narrow the number of avenues available for an unauthorized disclosure of CPNI without eliminating a carrier's ability to share CPNI with its joint venture partners and independent contractors under certain circumstances. We disagree that an opt-in regime's costs outweigh the benefits to customers.[135] While we appreciate commenter concern that carriers may need to engage in broader marketing campaigns for their services as a result of an opt-in regime, we believe that this cost is outweighed by the carriers' duty to protect their customers' private information, and more importantly, customers' interest in maintaining control over their private information.[136] Thus, we believe that an opt-in regime is the least restrictive means to ensure that a customer has control over its private information and is not subjected to permanent harm as a result of a carrier's disclosure of CPNI to one of its joint venture partners or independent contractors.[137]

44. We disagree with commenters who assert that an opt-in regime for disclosures to joint venture partners and independent contractors fails the *Central Hudson* test[138] for the regulation of commercial speech.[139] We recognize that more than seven

years ago, in *U.S. West, Inc. v. FCC*, the United States Court of Appeals for the Tenth Circuit held that the Commission had failed, based on the record in that proceeding, to satisfy its burden of showing that an opt-in rule passed the *Central Hudson* test.[140] That decision, however, was based on a different record than the one compiled here and, in particular, on two premises that are no longer valid. First, the Tenth Circuit concluded that there was no evidence showing harm to privacy interests from unauthorized disclosure of CPNI. "While protecting ***6950** against disclosure of sensitive and potentially embarrassing personal information may be important in the abstract, we have no indication of how it may occur in reality with respect to CPNI. Indeed, we do not even have indication that the disclosure might actually occur."[141] The record in this proceeding, by contrast, is replete with specific examples of unauthorized disclosure of CPNI and the adverse effects of such disclosures on customers.[142] Indeed, in the Telephone Records and Privacy Protection Act of 2006, Congress recently found that unauthorized disclosure of telephone records is a problem that "not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, compromise the personal safety of law enforcement officers, their families, victims of crime, witnesses, or confidential informants, and undermine the integrity of law enforcement investigations."[143] Second, the Tenth Circuit in *U.S. West* concluded that the record "d[id] not adequately show that an opt-out strategy would not sufficiently protect customer privacy."[144] In this proceeding, however, substantial evidence shows that the current opt-out rules do not adequately protect customer privacy because most customers either do not read or do not understand carriers' opt-out notices.[145] For example, the National Association of Attorneys General cites to "studies [that] serve as confirmation of what common sense tells us: that in this harried country of multitaskers, most consumers are unlikely to read extra notices that arrived in today's or last week's mail and thus, will not understand that failure to act will be treated as an affirmative consent to share his or her information."[146]

****14** 45. We find, based on the record in this proceeding, that requiring carriers to obtain opt-in consent from customers before sharing CPNI with joint venture partners and independent contractors for marketing purposes satisfies the *Central Hudson* test. Specifically, we find that: (1) unauthorized disclosure of CPNI is a serious and growing problem; (2) the government has a substantial interest in preventing unauthorized disclosure of CPNI because such disclosure can have significant adverse consequences for privacy and safety;[147] (3) the more independent entities that possess CPNI, the greater the danger of unauthorized disclosure; (4) an opt-in regime directly and materially advances privacy and safety interests by giving customers direct control over the distribution of their private information outside the carrier-customer relationship; and (5) an opt-in regime is not more extensive than necessary to protect privacy and safety interests because opt-out rules, the alternative cited by the Tenth Circuit in *U.S. West, Inc. v. FCC*, do not adequately secure customers' consent for carriers to share CPNI with unaffiliated entities. In short, given the undisputed evidence demonstrating that unauthorized disclosures of CPNI constitute a serious and prevalent problem in the United States today, we believe that carriers should be required to obtain a customer's explicit consent before sending such sensitive information outside of the company for marketing purposes. In light of the serious damage that unauthorized CPNI disclosures can cause, it is important that individual consumers determine if they want to bear the increased risk associated with sharing CPNI with independent contractors and joint venture partners, and the only way to ensure that a consumer is willingly bearing that risk is to require opt-in consent. In this vein, we note that most United States privacy laws, such as the Family Educational Rights and Privacy Act, Cable Communications Policy Act, Electronic Communications Privacy Act, Video Privacy Protection Act, Driver's Privacy Protection Act, and Children's Online Privacy Protection Act, do not ***6951** employ an opt-out approach but rather require an individual's explicit consent before private information is disclosed or employed for secondary purposes.[148]

46. We disagree with commenters who contend that requiring carriers to obtain opt-in consent from customers before sharing CPNI is unnecessary because, they claim, there is no evidence that data brokers have obtained CPNI from carriers' joint venture partners and independent contractors.[149] While it is true that the record does not include specific examples of unauthorized disclosure of CPNI by a joint venture partner or independent contractor, that does not mean unauthorized disclosure has not occurred or will not occur in the future. We see no reason why joint venture partners and independent contractors would be immune from this widespread problem. While carriers argue that pretexters do not focus their efforts on independent contractors and joint venture partners, we disagree with commenters who suggest that the governmental interests at stake in this proceeding are limited to the prevention of pretexting.[150] The rules we are adopting are designed to curtail *all* forms of unauthorized disclosure of CPNI, not just pretexting. Unauthorized disclosure of CPNI by any method invades the privacy of unsuspecting consumers and increases the risk of identity theft, harassment, stalking, and other threats to personal safety.[151] In this proceeding, commenters have identified at least two other common forms of unauthorized disclosure of CPNI: computer intrusion and disclosure by insiders.[152] Indeed, evidence in the record suggests that 50-70% of cases of identity theft arise from wrongful conduct by insiders.[153] The record further demonstrates that information security breaches are on the rise in this country, and it is axiomatic that the more companies that have access to CPNI, the greater the risk of

unauthorized disclosure through disclosure by insiders or computer intrusion.[154] Thus, by sharing CPNI with joint venture partners and independent contractors, it is clear that carriers increase the odds of wrongful disclosure of this sensitive information, and before the chances of unauthorized disclosure are increased, a customer's explicit consent should be required. In any event, returning to the issue of pretexting, we also reject the argument that pretexters do not attempt to obtain CPNI from independent contractors and joint venture partners. Indeed, Sprint admits that "pretexters persist without regard to the status of any carrier representative (whether an employee, a joint venture partner, or an independent contractor)."[155] To be ***6952** sure, certain carriers claim that they do not provide the type of CPNI to joint venture partners and independent contractors that are attractive to pretexters. But even assuming this to be true for the moment, this does not appear to be the case across the entire industry.

****15** 47. Carriers also argue that there are more narrowly tailored alternatives to requiring opt-in consent for disclosures of CPNI to independent contractors and joint venture partners. First, Verizon suggests that the Commission could mandate password protection of call detail information.[156] While we agree that this is a good idea and adopt it in this Order,[157] this step is plainly insufficient by itself to address all of the legitimate privacy concerns at issue in this proceeding. Such a step, for example, would do nothing to protect the unauthorized disclosure of call detail information in the possession of independent contractors and joint venture partners by insiders or computer intrusion, let alone the unauthorized disclosure of other forms of CPNI.

48. Second, Verizon argues that it would be sufficient to adopt an opt-in regime only for call detail information shared with independent contractors and joint venture partners.[158] We likewise conclude that this alternative would be inadequate. While we recognize that unauthorized disclosure of call detail information is a significant problem, all CPNI constitutes sensitive information that is protected under the Communications Act and our rules.[159] Moreover, we note that Congress did not distinguish between call detail and non-call detail information in the Telephone Records and Privacy Protection Act of 2006.[160] Verizon's premise that non-call detail information is not sufficiently sensitive to warrant an opt-in requirement is therefore incorrect. For example, information about a customer's calling plan may be highly sensitive. T-Mobile currently offers a "myFaves" plan that allows customers to make unlimited calls to five "myFaves" contacts for a flat monthly charge, and Alltel offers a similar calling plan (the My Circle Plan) that allows for unlimited calls to ten contacts.[161] While the identity of such contacts would not constitute call detail information, such information is no doubt highly personal and would be of significant interest to those seeking to invade another's privacy. As a result, we believe that carriers should be required to obtain a customer's explicit consent before such information is shared with independent contractors or joint venture partners and thus placed at greater risk of unauthorized disclosure.

49. Finally, carriers suggest that the Commission could mandate that carriers sharing CPNI with joint venture partners and independent contractors implement additional contractual safeguards.[162] We again conclude that this alternative would not adequately vindicate our interest in protecting consumers' privacy. Further contractual safeguards would not change the fact that the risk of unauthorized CPNI disclosures increases when such information is provided by a carrier to a joint venture partner or independent contractor. Indeed, in light of the record developed in this proceeding, it is quite apparent that safeguards implemented by carriers themselves often fail to prevent unauthorized disclosures of ***6953** CPNI.[163] It is for this reason that we believe that a carrier should be required to obtain explicit consent from its customer before that customer's CPNI is sent outside of the company for marketing purposes.

****16** 50. *Grandfathering of Previously Obtained CPNI Approvals*. To the extent that carriers voluntarily obtained opt-in approval from their customers for the disclosure of customers' CPNI to a joint venture partner or independent contractor for the purposes of marketing communications-related services to a customer prior to the adoption of this Order, those carriers can continue to use those approvals.

E. Annual Certification Filing

51. We adopt the Commission's tentative conclusion and amend our rules to require carriers to file their annual CPNI certification with the Commission, including an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.[164] We find that this amendment to the Commission's rules is an appropriate measure and will ensure that carriers regularly focus their attention on their duty to safeguard CPNI. Additionally, we find that this modification to our rules will remind carriers of the Commission's oversight and high priority regarding carrier performance in this area. Further, with this filing, the Commission will be better

able to monitor the industry's response to CPNI privacy issues and to take any necessary steps to ensure that carriers are managing customer CPNI securely.[165]

52. Under the Commission's existing CPNI regulations, each telecommunications carrier must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules and to make that certification available to the public.[166] While carriers currently are required to certify annually that their operating procedures are ***6954** adequate to ensure compliance with the Commission's CPNI rules, the failure of carriers to make this annual certification in their own public file, and the evidence EPIC introduced into the record regarding the industry-wide problem of pretexting, suggests that certain carriers have been less than vigilant concerning the safeguarding of CPNI.[167]

53. We find that carriers should be required to make this filing annually with the Enforcement Bureau on, or before, March 1, in EB Docket No. 06-36, for data pertaining to the previous calendar year.[168] We believe that this deadline will provide carriers with ample opportunity to review their own CPNI protection programs and ensure the adequacy of their defenses against fraudulent attempts to access customers' private data.[169] Further, this deadline will allow carriers sufficient time to review their filings without the certification being overshadowed by other annual filing requirements.

F. Extension of CPNI Requirements to Providers of Interconnected VoIP Service

54. We extend the application of the Commission's CPNI rules to providers of interconnected VoIP service.[170] In the *IP-Enabled Services Notice* and the *EPIC CPNI Notice*, the Commission sought ***6955** comment on whether to extend the CPNI requirements to VoIP service providers.[171] Since we have not decided whether interconnected VoIP services are telecommunications services or information services as those terms are defined in the Act, nor do we do so today,[172] we analyze the issues addressed in this Order under our Title I ancillary jurisdiction to encompass both types of service.[173] If the Commission later classifies interconnected VoIP service as a telecommunications service, the providers of interconnected VoIP services would be subject to the requirements of section 222 and the Commission's CPNI rules as telecommunications carriers under Title II.[174]

****17** 55. We conclude that we have authority under Title I of the Act to impose CPNI requirements on providers of interconnected VoIP service. Ancillary jurisdiction may be employed, in the Commission's discretion, when Title I of the Act gives the Commission subject matter jurisdiction over the service to be regulated[175] and the assertion of jurisdiction is "reasonably ancillary to the effective performance of [its] various responsibilities."[176] Both predicates for ancillary jurisdiction are satisfied here. First, as we concluded in the *Interim USF Order and VoIP 911 Order*, interconnected VoIP services fall within the subject matter jurisdiction granted to us in the Act.[177] Second, our analysis requires us to evaluate ***6956** whether imposing CPNI obligations is reasonably ancillary to the effective performance of the Commission's various responsibilities. Based on the record in this matter, we find that sections 222 and 1 of the Act provide the requisite nexus, with additional support from section 706.

56. Section 222 requires telecommunications carriers to protect the confidentiality of CPNI, and the Commission has adopted detailed regulations to help clarify this duty.[178] The Commission already has determined that interconnected VoIP service "is increasingly used to replace analog voice service" -- a trend that we expect will continue.[179] It therefore seems reasonable for American consumers to expect that their telephone calls are private irrespective of whether the call is made using the services of a wireline carrier, a wireless carrier, or an interconnected VoIP provider, given that these services, from the perspective of a customer making an ordinary telephone call, are virtually indistinguishable.[180]

57. Moreover, extending section 222's protections to interconnected VoIP service customers is necessary to protect the privacy of wireline and wireless customers that place calls to or receive calls from interconnected VoIP customers. The CPNI of interconnected VoIP customers includes call detail information concerning all calling and called parties. Thus, by protecting from inadvertent disclosure the CPNI of interconnected VoIP customers, the Commission will more effectively protect the privacy of wireline and wireless service customers. We therefore find that the extension of the CPNI privacy requirements to providers of interconnected VoIP service is reasonably ancillary to the effective performance of the Commission's duty to protect the CPNI of all telecommunications customers under Title II.

58. Section 1 of the Act charges the Commission with responsibility for making available "a rapid, efficient, Nation-wide,

and world-wide wire and radio communication service . . . for the purpose of *promoting safety of life and property* through the use of wire and radio communication."[181] In light of this statutory mandate in conjunction with the recent real-life implications of the unauthorized release of CPNI, protecting a consumer's private information continues to be one of the Commission's public safety responsibilities.[182] If we failed to exercise our responsibilities under sections 222 and 1 of the Act with respect to customers of interconnected VoIP service, a significant number of American consumers might suffer a loss of privacy and/or safety resulting from unauthorized disclosure of their CPNI -- and be ***6957** harmed by this loss. Therefore, we believe that extending the CPNI obligations to interconnected VoIP service providers is "reasonably ancillary to the effective performance of [our] responsibilities"[183] under sections 222 and 1 of the Act, and "will 'further the achievement of long-established regulatory goals'"[184] to protect the confidentiality of CPNI.[185]

****18** 59. We also are guided by section 706 of the Act, which, among other things, directs the Commission to encourage the deployment of advanced telecommunications capability to all Americans by using measures that "promote competition in the local telecommunications market."[186] The protection of CPNI may spur consumer demand for interconnected VoIP services, in turn driving demand for broadband connections, and consequently encouraging more broadband investment and deployment consistent with the goals of section 706.[187] Thus, pursuant to our ancillary jurisdiction, we extend the CPNI obligations to providers of interconnected VoIP services.[188]

G. Preemption

60. We reject commenter requests to preempt all state CPNI obligations[189] because we agree with commenters that assert we should allow states to also create rules for protecting CPNI.[190] We ***6958** recognize that many states already have laws relating to safeguarding personal information such as CPNI.[191] To the extent those laws do not create a conflict with federal requirements, carriers are able to comply with federal law and state law. Should a carrier find that it is unable to comply simultaneously with the Commission's rules and with the laws of another jurisdiction, the carrier should bring the matter to our attention in an appropriate petition.[192]

H. Implementation

61. In light of the importance of this issue to the public interest,[193] we require that our rules become effective within an aggressively short amount of time because of the important consumer and public safety considerations raised by pretexting that demand near immediate action.[194] The rules we adopt in this Order, however, are subject to approval by the Office of Management and Budget (OMB). Thus, our rules become effective six months after the Order's effective date or on receipt of OMB approval, as required by the Paperwork Reduction Act,[195] whichever is later. We will issue a Public Notice when OMB approval is received. For carriers satisfying the definition of a "small entity" or a "small business concern" under the Regulatory Flexibility Act or Small Business Act,[196] we provide an ***6959** additional six months to implement the rules pertaining to the online carrier authentication requirements.[197]

62. We find that the requirements we adopt in this Order most appropriately respond to actions by wrongdoers to obtain unauthorized access to CPNI, and carriers' failures to adequately protect CPNI in violation of their section 222 duty. This order balances those actions and inactions against the privacy concerns of all Americans. By requiring carriers (including interconnected VoIP service providers) to implement CPNI protections as a top priority, we hope to minimize the likelihood of future unauthorized disclosures of consumer's CPNI.

I. Enforcement

63. We take seriously the protection of customers' private information and commit to remaining vigilant to ensure compliance with applicable privacy laws within our jurisdiction. One way in which we will help protect consumer privacy is through strong enforcement measures. When investigating compliance with the rules and statutory obligations, the Commission will consider whether the carrier has taken reasonable precautions to prevent the unauthorized disclosure of a customer's CPNI. Specifically, we hereby put carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer's CPNI that the carrier did not sufficiently protect that customer's CPNI. A carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue. If the Commission finds at the conclusion of its investigation that the carrier indeed has not taken

sufficient steps adequately to protect the privacy of CPNI, the Commission may sanction it for this oversight, including through forfeiture.

**19 64. We offer here additional guidance regarding the Commission's expectations that will inform our investigations. We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.[198] Of course, we require carriers to implement the specific minimum requirements set forth in the Commission's rules. We further expect carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier. For instance, and as discussed above, although we decline to impose audit trail obligations on carriers at this time, we expect carriers through audits or other measures to take reasonable measures to discover and protect against activity that is indicative of pretexting. Similarly, although we do not specifically require carriers to encrypt their customers' CPNI, we expect a carrier to encrypt its CPNI databases if doing so would provide significant additional protection against the unauthorized access to CPNI at a cost that is reasonable given the technology a carrier already has implemented.

65. By adopting certain specific minimum standards regarding what measures carriers must take to protect the privacy of CPNI, and by committing to taking resolute enforcement action to ensure that the *6960 goals of section 222 are achieved, we believe we appropriately balance consumer privacy interests with carriers' interests in minimizing burdens on their customers. Our two-prong approach will (1) allow carriers to implement whatever security measures are warranted in light of their technological choices, (2) create a diversity of security practices that will enable market forces to improve carriers' security measures over time, (3) avoid creating unnecessary regulatory barriers that could impede carriers from adapting to new threats as the methods used by data brokers evolve, and (4) alleviate commenters' concerns that specific safeguard rules could provide pretexters with a "roadmap" of how to obtain CPNI without authorization. We further believe that our two-pronged approach will ensure a high level of privacy protection for CPNI because carriers will have sufficient incentive and ability to adopt whatever security mechanisms work best with their existing systems and procedures.

66. *Carrier Safe Harbor*. We decline to immunize carriers from possible sanction for disclosing customers' private information without appropriate authorization. Some carriers support the adoption of a "safe harbor," which would immunize carriers from liability for improper disclosure of CPNI if the carrier followed certain security guidelines, such as those comparable to the Federal Trade Commission's (FTC's) guidelines for the financial industry.[199] We decline to adopt this proposal because such a rule would result in less protection of customers' CPNI than exists under the status quo. The guidelines the carriers propose to trigger immunity do not add meaningful protections beyond carriers' existing regulatory obligations.[200] Therefore, if we adopted the proposed safe harbor, carriers would receive immunity from liability for meeting the requirements set forth in the safe harbor, even if a carrier acted egregiously and in derogation of its general duty to protect CPNI from unauthorized release. The public interest is better served if the Commission retains the option of taking strong enforcement measures regarding carriers' duties under section 222 and the Commission's rules.

V. FURTHER NOTICE OF PROPOSED RULEMAKING

**20 67. The Commission has a duty to ensure that, as technologies evolve, the consumer protection objectives of the Act are maintained. Through this Further Notice of Proposed Rulemaking, we seek comment on whether the Commission should act to expand its CPNI rules further, and whether it should expand the consumer protections to ensure that customer information and CPNI are protected in the context of mobile communication devices.

A. Additional CPNI Protective Measures

68. *Password Protection*. In light of the rules we adopt in today's Order and the recent enactment of criminal penalties against pretexters, we seek comment on whether the Commission should adopt any further carrier requirements to protect CPNI. Specifically, while we limited our rules to password protecting call detail information for customer-initiated telephone contact, we seek comment on whether to extend these rules to include optional or mandatory password protection for non-call detail CPNI. Should this password protection be for all non-call detail CPNI or should it only include certain account changes? Further, if the Commission were to adopt password protection for certain account changes, what should that include (*e.g.*, changes in the address of record, account plans, or billing methods)? Would requiring these forms of password protection place an undue burden on carriers, *6961 customers, or others, including any burdens placed on small carriers? We solicit further comment on any other modifications to our rules that we should adopt in light of pretexting activity, and a

carrier's duty to protect CPNI.

69. *Audit Trails*. While we did not adopt rules requiring audit trails at this time, in light of our new rules and the recent enactment of criminal penalties against pretexters, we seek comment on whether the Commission should adopt rules pertinent to audit trails. Are audit trails generally used by carriers to track customer contact? We ask carriers to assess the benefits and burdens, including the burdens on small carriers, of recording the disclosure of CPNI and customer contact. Our current record indicates that the broad use of audit trails likely would be of limited value in ending pretexting because such a log would record enormous amounts of data, the vast majority of it being legitimate customer inquiry.[201] Commenters also report that implementing and maintaining audit trails would be costly with little to no corresponding benefit to the consumer.[202] However, would an audit trail assist law enforcement with its criminal investigations against pretexters? Further, in the interim period since we sought comment on this issue, have carriers' reactions to audit trails changed or has the technology changed such that audit trails are now an economically feasible option?

70. *Physical Safeguards*. We also seek comment on whether the Commission, in light of the rules we adopt in this Order and the recent enactment of criminal penalties against pretexters, should adopt rules that govern the physical transfer of CPNI among companies, such as between a carrier and its affiliates, or the transfer of CPNI to any other third party authorized to access or maintain CPNI, including a carrier's joint venture partners and independent contractors. Specifically, we seek comment on what physical safeguards carriers currently are using when they transfer, or allow access to, CPNI to ensure that they maintain the security and confidentiality of CPNI?[203] We also seek comment on whether these safeguards for the physical transfer of, or for access to, CPNI are sufficient? Further, we seek comment on what steps the Commission should require of a carrier to protect CPNI when CPNI is being transferred or accessed by the carrier, its affiliates, or its third parties (*e.g.*, encryption, audit trails, logs, etc.). Additionally, we seek comment on the benefits and burdens, including the burdens on small carriers, of requiring carriers to physically safeguard the security and confidentiality of CPNI.

****21** 71. *Limiting Data Retention*. We also seek comment on whether the Commission, in light of the rules we adopt in this Order and the recent enactment of criminal penalties against pretexters, should adopt rules that require carriers to limit data retention. If the Commission did adopt such a rule, what should be the maximum amount of time that a carrier should be able to retain customer records? Additionally, should all customer records be eliminated or is there a subset of customer records that are more susceptible to abuse and should be destroyed? Also, should the Commission define exceptions where a carrier is permitted to retain certain records (*e.g.*, for the length of carrier-carrier or carrier-customer disputes)? The Department of Justice argues that destruction of CPNI after a specified period would hamper law enforcement efforts by destroying data sometimes needed for criminal and other lawful investigations.[204] We also seek comment on whether there are any state or Commission data ***6962** retention requirements that might conflict with a carrier's data limitation.[205] Additionally, does a limitation on data retention enhance protection of CPNI?[206] Alternatively, should the Commission require carriers to de-identify customer records after a certain period?[207] We seek comment on the benefits and burdens, including the burdens on small carriers, of requiring carriers to limit their data retention or to de-identify customer records.

B. Protection of Information Stored in Mobile Communications Devices

72. We seek comment on what steps the Commission should take, if any, to secure the privacy of customer information stored in mobile communications devices.[208] Specifically, we seek comment on what methods carriers currently use, if any, for erasing customer information on mobile equipment prior to refurbishing the equipment,[209] and the extent to which carriers enable customers to permanently erase their personal information prior to discarding the device. We also seek comment on whether the Commission should require carriers to permanently erase, or allow customers to permanently erase, customer information in such circumstances. Should the Commission require manufacturers to configure wireless devices so consumers can easily and permanently delete personal information from those devices? Further, we seek comment on the burdens, including those placed on small carriers, associated with a Commission rule requiring carriers and manufacturers to fully expunge existing customer data from a mobile device at the customer's request.

VI. PROCEDURAL MATTERS

A. *Ex Parte* Presentations

73. The rulemaking this Notice initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the

Commission's *ex parte* rules.[210] Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentations must contain summaries of the substance of the presentations and not merely a listing of the subjects discussed. More than a one or two sentence description of the views and arguments presented generally is required.[211] Other requirements pertaining to oral and written presentations are set forth in section 1.1206(b) of the Commission's rules.[212]

***6963 B. Comment Filing Procedures**

****22** 74. Pursuant to sections 1.415 and 1.419 of the Commission's rules,[213] interested parties may file comments and reply comments regarding the Notice on or before the dates indicated on the first page of this document. **All filings related to this Further Notice of Proposed Rulemaking should refer to CC Docket No. 96-115 and WC Docket No. 04-36**. Comments may be filed using: (1) the Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies. See Electronic Filing of Documents in Rulemaking Proceedings, 63 FR 24121 (1998).

• Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://www.fcc.gov/cgb/ecfs/ or the Federal eRulemaking Portal: http://www.regulations.gov. Filers should follow the instructions provided on the website for submitting comments.

• ECFS filers must transmit one electronic copy of the comments for CC Docket No. 96-115 and WC Docket No. 04-36. In completing the transmittal screen, filers should include their full name, U.S. Postal Service mailing address, and the applicable docket number. Parties may also submit an electronic comment by Internet e-mail. To get filing instructions, filers should send an e-mail to ecfs@fcc.gov, and include the following words in the body of the message, "get form." A sample form and directions will be sent in response.

• Paper Filers: Parties who choose to file by paper must file an original and four copies of each filing. Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail (although we continue to experience delays in receiving U.S. Postal Service mail). All filings must be addressed to the Commission's Secretary, Marlene H. Dortch, Office of the Secretary, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554.

• The Commission's contractor will receive hand-delivered or messenger-delivered paper filings for the Commission's Secretary at 236 Massachusetts Avenue, N.E., Suite 110, Washington, D.C. 20002. The filing hours at this location are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes must be disposed of before entering the building.

• Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

• U.S. Postal Service first-class, Express, and Priority mail should be addressed to 445 12th Street, S.W., Washington D.C. 20554.

75. Parties should send a copy of their filings to Janice Myles, Competition Policy Division, Wireline Competition Bureau, Federal Communications Commission, Room 5-C140, 445 12th Street, S.W., Washington, D.C. 20554, or by e-mail to janice.myles@fcc.gov. Parties shall also serve one copy with the Commission's copy contractor, Best Copy and Printing, Inc. (BCPI), Portals II, 445 12th Street, S.W., Room CY-B402, Washington, D.C. 20554, (202) 488-5300, or via e-mail to fcc@bcpiweb.com.

****23** 76. Documents in CC Docket No. 96-115 and WC Docket No. 04-36 will be available for public inspection and copying during business hours at the FCC Reference Information Center, Portals II, 445 12th Street S.W., Room CY-A257, Washington, D.C. 20554. The documents may also be purchased ***6964** from BCPI, telephone (202) 488-5300, facsimile (202) 488-5563, TTY (202) 488-5562, e-mail fcc@bcpiweb.com.

C. Final Regulatory Flexibility Analysis

77. As required by the Regulatory Flexibility Act of 1980, see 5 U.S.C. § 604, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this document. The FRFA is set forth in Appendix C.

D. Initial Regulatory Flexibility Analysis

78. As required by the Regulatory Flexibility Act of 1980, see 5 U.S.C. § 603, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this document. The IRFA is set forth in Appendix D. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the Notice provided below in Appendix D.

E. Paperwork Reduction Act

79. This Order contains modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies are invited to comment on the new information collection requirements contained in this proceeding. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. § 3506(c)(4), we previously sought specific comment on how we might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

80. In the Order, we have assessed the burdens placed on small businesses to notify customers of account changes, to notify law enforcement and customers of unauthorized CPNI disclosure; to obtain opt-in consent prior to sharing CPNI with joint venture partners and independent contractors; to file annually a CPNI certification with the Commission, including an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the past year concerning the unauthorized release of CPNI, and to extend the CPNI rules to providers of interconnected VoIP services, and find that these requirements do not place a significant burden on small businesses.

****24** 81. This Further Notice contains proposed information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invited the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this Further Notice, as required by the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. Public and agency comments are due **60 days after publication in the Federal Register**. Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; and (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. § 3506(c)(4), we seek comment on how we might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

***6965 F. Congressional Review Act**

82. The Commission will send a copy of this Report and Order and Further Notice of Proposed Rulemaking in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act (CRA), *see* 5 U.S.C. § 801(a)(1)(A).

G. Accessible Formats

83. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice) or 202-418-0432 (TTY). Contact the FCC to request reasonable accommodations for filing comments (accessible format documents, sign language interpreters, CART, etc.) by e-mail: FCC504@fcc.gov; phone: 202-418-0530 or TTY: 202-418-0432.

VII. ORDERING CLAUSES

84. Accordingly, IT IS ORDERED that pursuant to sections 1, 4(i), 4(j), 222, and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i)-(j), 222, 303(r), this Report and Order and Further Notice of Proposed Rulemaking in CC Docket No. 96-115 and WC Docket No. 04-36 IS ADOPTED, and that Part 64 of the Commission's rules, 47 C.F.R. Part 64, is amended as set forth in Appendix B. The Order shall become effective upon publication in the Federal Register subject to OMB approval for new information collection requirements or six months after the Order's effective date, whichever is later.

**25 85. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order and Further Notice of Proposed Rulemaking, including the Final Regulatory Flexibility Analysis and the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

ERRATUM

Erratum Released: May 9, 2007

By the Chief, Wireline Competition Bureau:

On April 2, 2007, the Commission released a *Report and Order and Further Notice of Proposed Rulemaking*, FCC 07-22, in the above-captioned proceeding. This Erratum corrects Appendix B, Final Rules in the *Report and Order and Further Notice of Proposed Rulemaking* as follows:
1. In section 64.2003(k), the text is amended to read as follows:
(k) *Telecommunications carrier or carrier*. The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3(44) of the Communications Act of 1934, as amended, 47 U.S.C. 153(44). For the purposes of this subpart, the term "telecommunications carrier" or "carrier" shall include an entity that provides interconnected VoIP service, as that term is defined in section 9.3 of these rules.

2. In section 64.2003, paragraphs (l), (p), and (q) are redesignated as paragraphs (m), (q), and (r), respectively.

3. In section 64.2005(c)(3), the text is amended to read as follows:
(3) LECs, CMRS providers, and entities that provide interconnected VoIP service as that term is defined in section 9.3 of these rules, may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

4. In section 64.2011, paragraphs (c)-(e) are redesignated as (d)-(f), respectively, and a new paragraph (c) is added to read as follows:
(c) *Customer Notification*. After a telecommunications carrier has completed the process of notifying law enforcement pursuant to paragraph (b), it shall notify its customers of a breach of those customers' CPNI.

FEDERAL COMMUNICATIONS COMMISSION

Thomas J. Navin
Chief
Wireline Competition Bureau

***6966 Appendix A**

Commenters in CC Docket No. 96-115

Comments	Abbreviation
Alexicon Telecommunications Consulting	Alexicon
Alltel Corporation	Alltel
American Association of Paging Carriers	AAPC
American Cable Association	ACA
AT&T Inc.	AT&T
Attorneys General of the Undersigned States	Attorneys General
BellSouth Corporation	BellSouth
Centennial Communications Corp.	Centennial
Charter Communications, Inc.	Charter
Cingular Wireless LLC	Cingular
COMPTEL	COMPTEL
Cross Telephone Company, Cimmaron Telephone Company, Pottawatomie Telephone Company, Chickaswa	Oklahoma Carriers

Telephone, and Salina-Spavinaw Telephone Company	
Crown Castle International Corp.	Crown Castle
CTIA-The Wireless Association®	CTIA
Dobson Communications Corporation	Dobson
Electronic Privacy Information Center, Consumer Action, Privacy Rights Now Coalition, Center for Digital Democracy, Consumer Federation of America, Privacy Journal, Center for Financial Privacy and Human Rights, and National Consumers League	EPIC *et al*.
Enterprise Wireless Alliance and the USMSS, Inc.	Enterprise Wireless
Eschelon Telecom, Inc., SNIP Link Inc., and XO Communications, Inc.	Joint Commenters
Global Crossing North America, Inc.	Global Crossing
Infonxx, Inc.	Infonxx
Independent Carrier Group	ICG
Kim Phan	Phan
Leap Wireless International, Inc. and Cricket	Leap

Communications, Inc.	
McManis & Monsaive Association	MMA
MetroPCS Communications, Inc.	MetroPCS
Microsoft Corporation, Skype Inc. and Yahoo! Inc.	Internet Companies
Myung Kim	Kim
National Association of State Utility Consumer Advocates	NASUCA
National Cable & Telecommunications Association	NCTA
National Telecommunications Cooperative Association	NTCA
New Jersey Division of the Ratepayer Advocate	New Jersey Ratepayer Advocate
NextG Networks, Inc.	NextG
Nicholas Leggett	Leggett
Organization for the Promotion and Advancement of Small Telecommunications Companies	OPASTCO
Pennsylvania Public Utility Commission	PaPUC
Princeton University Students	Princeton Students
Privacy Rights Clearinghouse	Privacy Rights
Public Service Commission of the State of Missouri	MoPSC

Public Utilities Commission of Ohio	Ohio PUC
Qwest Communications International Inc.	Qwest
RNK Inc. d/b/a RNK Telecom	RNK
Rural Cellular Association	RCA
Sprint Nextel Corporation	Sprint Nextel
TCA, Inc. -- Telecom Consulting Associations	TCA
Texas Office of Public Utility Counsel	TX OPUC
Texas Statewide Telephone Cooperative, Inc.	TSTCI
The People of the State of California and the California Public Utilities Commission	CaPUC
Time Warner Inc.	Time Warner
Time Warner Telecom Inc.	TWTC
T-Mobile USA, Inc.	T-Mobile
United States Departments of Justice and Homeland Security	DOJ/DHS
United States Internet Service Provider Association	USISPA
United States Telecom Association	USTelecom

USA Mobility, Inc.	USA Mobility
US LEC Corp.	US LEC
Verizon	Verizon
Verizon Wireless	Verizon Wireless

***6967 Reply Commenters in CC Docket No. 96-115**

Reply Comments	**Abbreviation**
AT&T Inc.	AT&T
BellSouth Corporation	BellSouth
Centennial Communications Corp. d/b/a Centennial Wireless	Centennial
Charter Communications, Inc.	Charter
Cingular Wireless LLC	Cingular
CTIA-The Wireless Association®	CTIA
Direct Marketing Association, Inc.	DMA
Dobson Communications Corporation	Dobson
Electronic Privacy Information Center	EPIC
Embarq Corporation	Embarq
Enterprise Wireless Alliance, together with USMSS, Inc.	EWA

Eschelon Telecom, Inc., SNiP LiNK Inc., and XO Communications, Inc.	Joint Commenters
Insite Wireless LLC	Insite
MetroPCS Communications Inc.	MetroPCS
National Association of State Utility Consumer Advocates	NASUCA
Pennsylvania Public Utility Commission	PA PUC
Rock Hill Telephone Company d/b/a Comporium Communications, Fort Mill Telephone Company d/b/a Comporium Communications, and Lancaster Telephone Company d/b/a Comporium Communications	Comporium
Sprint Nextel Corporation	Sprint Nextel
T-Mobile USA, Inc.	T-Mobile
United States Cellular Corporation	US Cellular
Verizon	Verizon
Verizon Wireless	Verizon Wireless
Virgin Mobile USA, LLC	Virgin Mobile

***6968 Commenters in WC Docket No. 04-36**

Comments	Abbreviation
8X8, Inc.	8X8
AARP	AARP
ACN Communications Services, Inc.	ACN
Ad Hoc Telecommunications Users Committee	Ad Hoc
Alcatel North America	Alcatel
Alliance for Public Technology	APT
America's Rural Consortium	ARC
American Foundation for the Blind	AFB
American Public Communications Council	APCC
Amherst, Massachusetts Cable Advisory Committee	Amherst CAC
Arizona Corporation Commission	Arizona Commission
Artic Slope Telephone Association Cooperative, Inc. Cellular Mobile Systems of St. Cloud, LLC d/b/a Cellular 2000 Comanche County Telephone, Inc. DeKalb Telephone Cooperative, Inc. d/b/a DTC Communications	Artic Slope *et al*.

Grand River Mutual Telephone Corporation	
Interstate 35 Telephone Company	
KanOkla Telephone Association, Inc.	
Siskiyou Telephone Company	
Uintah Basin Telecommunications Association, Inc.	
Vermont Telephone Company, Inc.	
Wheat State Telephone, Inc.	
Association for Communications Technology Professionals in Higher Education	ACUTA
Association for Local Telecommunications Services	ALTS
Association of Public-Safety Communications Officials-International, Inc.	APCO
AT&T Corporation	AT&T
Attorney General of the State of New York	New York Attorney General
Avaya, Inc.	Avaya
BellSouth Corporation	BellSouth
Bend Broadband	Bend Broadband *et al*.

Cebridge Connections, Inc. Insight Communications Company, Inc. Susquehanna Communication	
Boulder Regional Emergency Telephone Service Authority	BRETSA
BT Americas Inc.	BTA
Cablevision Systems Corp.	Cablevision
Callipso Corporation	Callipso
Cbeyond Communications, LLC GlobalCom, Inc. MPower Communications, Corp.	Cbeyond *et al*.
CenturyTel, Inc.	CenturyTel
Charter Communications	Charter
Cheyenne River Sioux Tribe Telephone Authority	Cheyenne Telephone Authority
Cisco Systems, Inc.	Cisco
Citizens Utility Board	CUB
City and County of San Francisco	San Francisco
City of New York	New York City

Comcast Corporation	Comcast
Communication Service for the Deaf, Inc.	CSD
Communications Workers of America	CWA
CompTel/ASCENT	CompTel
Computer & Communications Industry Association	CCIA
Computing Technology Industry Association	CompTIA
Consumer Electronics Association	CEA
Covad Communications	Covad
Cox Communications, Inc.	Cox
CTIA-The Wireless Association	CTIA
Department of Homeland Security	DHS
DialPad Communication, Inc. ICG Communications, Inc. Qovia, Inc. VoicePulse, Inc.	Dialpad *et al*.
DJE Teleconsulting, LLC	DJE
Donald Clark Jackson	Jackson
EarthLink, Inc.	EarthLink

EDUCAUSE	EDUCAUSE
Electronic Frontier Foundation	EFF
Enterprise Communications Association	ECA
Federation for Economically Rational Utility Policy	FERUP
Francois D. Menard	Menard
Frontier and Citizens Telephone Companies	Frontier/Citizens
General Communications, Inc.	GCI
Global Crossing North America, Inc.	Global Crossing
GVNW Consulting, Inc.	GVNW
ICORE, Inc.	ICORE
IEEE-USA	IEEE-USA
Illinois Commerce Commission	Illinois Commerce Commission
Inclusive Technologies	Inclusive Technologies
Independent Telephone & Telecommunications Alliance	ITTA
Information Technology Association of America	ITAA
Information Technology Industry Council	ITIC
Interstate Telcom Consulting, Inc.	ITCI

Ionary Consulting	Ionary
Iowa Utilities Board	Iowa Commission
King County E911 Program	King County
Level 3 Communications LLC	Level 3
Lucent Technologies Inc.	Lucent Technologies
Maine Public Utilities Commissioners	Maine Commissioners
MCI	MCI
Microsoft Corporation	Microsoft
Minnesota Public Utilities Commission	Minnesota Commission
Montana Public Service Commission	Montana Commission
Motorola, Inc.	Motorola
National Association of Regulatory Utility Commission	NARUC
National Association of State Utility Consumer Advocates	NASUCA
National Association of Telecommunications Officers and Advisors National League of Cities National Association of Counties	NATOA *et al*.

U.S. Conference of Mayors

National Association of Towns and Townships

Texas Coalition of Cities for Utility Issues

Washington Association of Telecommunications

Officers and Advisors

Greater Metro Telecommunications Consortium

Mr. Hood Cable Regulatory Commission

Metropolitan Washington Council of Governments

Rainier Communications Commission

City of Philadelphia

City of Tacoma, Washington

Montgomery County, Maryland

National Cable & Telecommunications Association	NCTA
National Consumers League	NCL
National Emergency Number Association	NENA
National Exchange Carrier Association, Inc.	NECA
National Governors Association	NGA
National Grange	National Grange

National Telecommunications Cooperative Association	NTCA
Nebraska Public Service Commission	Nebraska Commission
Nebraska Rural Independent Companies	Nebraska Rural Independent Companies
Net2Phone, Inc.	Net2Phone
New Jersey Board of Public Utilities	New Jersey Commission
New Jersey Division of the Ratepayer Advocate	New Jersey Ratepayer Advocate
New York State Department of Public Service	New York Commission
NexVortex, Inc.	nexVortex
Nortel Networks	Nortel
Nuvio Corporation	Nuvio
Office of Advocacy, U.S. Small Business Administration	SBA
Office of the Attorney General of Texas	Texas Attorney General
Office of the People's Counsel for the District of Columbia	D.C. Counsel
Ohio Public Utilities Commission	Ohio Commission
Omnitor	Omnitor
Organization for the Promotion and Advancement of	OPASTCO

Small Telecommunications Companies	
Pac-West Telecomm, Inc.	Pac-West
People of the State of California and the California Public Utilities Commission	California Commission
Public Service Commission of the State of Missouri	Missouri Commission
Pulver.com	pulver.com
Qwest Communications International Inc.	Qwest
Rehabilitation Engineering Research Center on Telecommunications Access	RERCTA
Rural Independent Competitive Alliance	RICA
SBC Communications, Inc.	SBC
Self Help for Hard of Hearing People	SHHHP
Skype, Inc.	Skype
Sonic.net, Inc.	Sonic.net
SPI Solutions, Inc.	SPI Solutions
Spokane County 911 Communications	Spokane County 911
Sprint Corporation	Sprint

TCA, Inc. -- Telecom Consulting Associates	TCA
Telecommunications for the Deaf, Inc	TDI
Telecommunications Industry Association	TIA
Tellme Networks, Inc	Tellme Networks
Tennessee Regulatory Authority	TRA
Texas Coalition of Cities for Utility Issues	TCCFUI
Texas Commission on State Emergency Communications.	TCSEC
Texas Department of Information Resources	Texas DIR
Time Warner Inc.	Time Warner
Time Warner Telecom	TWTC
TracFone Wireless, Inc.	TracFone
UniPoint Enhanced Services Inc. d/b/a PointOne	PointOne
United States Conference of Catholic Bishops	USCCB *et al.*
Alliance for Community Media	
Appalachian People's Actions Coalition	
Center for Digital Democracy	
Consumer Action	

Edgemont Neighborhood Coalition	
Migrant Legal Action Program	
United States Department of Justice	DOJ
United States Telecom Association	USTA
United Telecom Council	UTC *et al*.
The United Power Line Council	
USA Datanet Corporation	USAD Datanet
Utah Division of Public Utilities	Utah Commission
Valor Telecommunications of Texas, L.P. and Iowa	Valor *et al*.
Telecommunications Services, Inc.	
VeriSign, Inc.	VeriSign
Verizon Telephone Company	Verizon
Vermont Public Service Board	Vermont
Virgin Mobile USA, LLC	Virgin Mobile
Virginia State Corporation Commission	Virginia Commission
Voice on the Net Coalition	VON Coalition
Vonage Holdings Corp	Vonage
Western Telecommunications Alliance	WTA

WilTel Communications, LLC	WilTel
Wisconsin Electric Power Company Wisconsin Gas	Wisconsin Electric *et al.*
Yellow Pages Integrated Media Association	YPIMA
Z-Tel Communications, Inc.	Z-Tel

***6971 Reply Commenters in WC Docket No. 04-36**

Reply Comments	**Abbreviation**
8X8, Inc.	8X8
Ad Hoc Telecom Manufacturer Coalition	Ad Hoc Telecom Manufacturers Coalition
Ad Hoc Telecommunications Users Committee	Ad Hoc
Adam D. Thierer, Director of Telecommunications Studies, Cato Institute	Thierer
Alcatel North America	Alcatel
Alliance for Public Technology et al.	APT *et al.*
American Cable Association	ACA
American Electric Power Service Corporation Duke Energy Corporation	American Electric Power *et al.*

Xcel Energy Inc.	
Association for Local Telecommunications Services	ALTS
AT&T Corp.	AT&T
Avaya Inc.	Avaya
BellSouth Corporation	BellSouth
Broadband Service Providers Association	BSPA
Cablevision Systems Corp.	Cablevision
Callipso Corporation	Callipso
Central Station Alarm Association	CSAA
Cingular Wireless LLC	Cingular
Cisco Systems, Inc.	Cisco
City and County of San Francisco	San Francisco
Comcast Corporation	Comcast
CompTel/Ascent	CompTel
Consumer Electronics Association	CEA
Consumer Federation of America Consumers Union	CFA *et al.*
Covad Communications	Covad

CTC Communications Corp.	CTS
CTIA-The Wireless Association	CTIA
Department of Defense	DoD
Donald Clark Jackson	Jackson
EarthLink, Inc.	EarthLink
Educause	Educause
Enterprise Communications Association	ECA
Ericsson Inc.	Ericsson
Florida Public Service Commission	Florida Commission
Francois D. Menard	Menard
General Communication (GCI)	GCI
Global Crossing North America, Inc.	Global Crossing
Independent Telephone & Telecommunications Alliance	ITTA
Information Technology Association of America	Information Technology Association of America
Intergovernmental Advisory Committee	IAC
Intrado Inc.	Intrado

Knology, Inc.	Knology
Level 3 Communications LLC	Level 3
Massachusetts Office of the Attorney General	Massachusetts Attorney General
MCI	MCI
Montana Public Service Commission	Montana Commission
Motorola, Inc.	Motorola
National Association of State Utility Consumer Advocates	NASUCA
National Association of Telecommunications Officers and Advisors National League of Cities National Association of Counties U.S. Conference of Mayors National Association of Towns and Townships Texas Coalition of Cities for Utility Issues Washington Association of Telecommunications Officers and Advisors Greater Metro Telecommunications Consortium Mr. Hood Cable Regulatory Commission	NATOA *et al*.

Metropolitan Washington Council of Governments	
Rainier Communications Commission	
City of Philadelphia	
City of Tacoma, Washington	
Montgomery County, Maryland	
National Cable & Telecommunications Association	NCTA
National Emergency Number Association	NENA
National Exchange Carrier Association, Inc.	NECA
Nebraska Public Service Commission	Nebraska Commission
Nebraska Rural Independent Companies	Nebraska Rural Independent Companies
Net2Phone, Inc.	Net2Phone
New Jersey Division of the Ratepayer Advocate	New Jersey Ratepayer Advocate
New York State Department of Public Service	New York Commission
Nextel Communications, Inc.	Nextel
Nuvio Corporation	Nuvio
Office of the People's Counsel for the District of Columbia	D.C. Counsel

Organization for the Promotion and Advancement of Small Telecommunications Companies	OPASTCO
Pac-West Telecomm, Inc.	Pac-West
Pennsylvania Public Utility Commission	Pennsylvania Commission
Public Service Commission of Wisconsin	Wisconsin Commission
Qwest Communications International Inc.	Qwest
Regulatory Studies Program (RSP) of the Mercatus Center at George Mason University	Mercatus Center
Rehabilitation Engineering Research Center on Telecommunications Access	RERCTA
RNKL, Inc. d/b/a RNK Telecom	RNK
Rural Independent Competitive Alliance	RICA
SBC Communications Inc.	SBC
Skype, Inc.	Skype
Southern Communications Services, Inc. d/b/a Southern LINC	Southern LINC
Sprint Corporation	Sprint

Telecommunications Industry Association	TIA
Tellme Networks, Inc	Tellme Networks
Texas Statewide Telephone Cooperative, Inc.	Texas Statewide Telephone Cooperative
Time Warner Telecom, Inc.	Time Warner Telecom
T-Mobile USA, Inc.	T-Mobile
TracFone Wireless, Inc.	TracFone
United States Conference of Catholic Bishops Alliance for Community Media Appalachian Peoples' Action Coalition Center for Digital Democracy Consumer Action Edgemont Neighborhood Coalition Migrant Legal Action Program	USCCB *et al*.
United States Department of Justice	DOJ
United States Telecom Association	USTA
USA Datanet Corporation	USA Datanet
Utah Division of Public Utilities	Utah Commission
VeriSign, Inc.	VeriSign

Verizon Telephone Companies	Verizon
Voice on the Net Coalition	VON Coalition
Wisconsin Department of Public Instruction	Wisconsin Department of Public Instruction

***6975 Appendix B**

Final Rules
Subpart U of Part 64, of Title 47 of the Code of Federal Regulations is amended to read as follows:

SUBPART U -- CUSTOMER PROPRIETARY NETWORK INFORMATION
1. Section 64.2003(k) is amended to read as follows:
(k) *Telecommunications carrier or carrier*. The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3(44) of the Communications Act of 1934, as amended, 47 U.S.C. 153(44). For the purposes of this Subpart, the term "telecommunications carrier" or "carrier" shall include "interconnected VoIP provider" as that term is defined in section 9.3 of these rules.

2. Section 64.2003 is amended by redesignating paragraphs (a)-(l) and by adding the following paragraphs:
(a) *Account information*. "Account information" is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

(b) *Address of record*. An "address of record," whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

(d) *Call detail information*. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

(l) *Readily available biographical information*. "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

(p) *Telephone number of record*. The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

(q) *Valid photo ID*. A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

3. Section 64.2005(c)(3) is amended to read as follows:
(3) LECs, CMRS providers, and interconnected VoIP providers may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory

assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

***6976** 4. Section 64.2007 is amended by deleting paragraphs (b)(2) and (b)(3), and revising paragraph (b)(1) to read as follows:
(b) *Use of Opt-Out and Opt-In Approval Processes*. A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section § 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

5. Section 64.2009 is amended by revising paragraph (e) to read as follows:
(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

6. Section 64.2010 is added to read as follows:

§ 64.2010 Safeguards on the disclosure of customer proprietary network information
(a) *Safeguarding CPNI*. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

(b) *Telephone access to CPNI*. Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or, by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) *Online access to CPNI*. A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service ***6977** account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

(d) *In-store access to CPNI*. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.

(e) *Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords*. To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(f) *Notification of account changes*. Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

(g) *Business Customer Exemption*. Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

7. Section 64.2011 is added to read as follows:

§ 64.2011 Notification of customer proprietary network information security breaches
(a) A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b).

(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni.
(1) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (2) and (3).

***6978** (2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (1), in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

(c) *Recordkeeping*. All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b), and notifications made to customers. The record must

include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.

(d) *Definitions*. As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

**26 (e) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

***6979 Appendix C**

Final Regulatory Flexibility Analysis

86. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[214] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *EPIC CPNI Notice* in CC Docket No. 96-115 and the *IP-Enabled Services Notice* in WC Docket 04-36.[215] The Commission sought written public comment on the proposals in both notices, including comment on the IRFA.[216] We received comments specifically directed toward the IRFA from three commenters in CC Docket No. 96-115 and from three commenters in WC Docket No. 04-36. These comments are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[217]

A. Need for, and Objectives of, the Rules

87. Today's Order strengthens the Commission's rules to protect the privacy of CPNI that is collected and held by providers of communications services. Section 222 of the Communications Act requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure. This Order adopts additional safeguards to protect customers' CPNI against unauthorized access and disclosure.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

88. *Comments Received in Response to the EPIC CPNI Notice*. In this section, we respond to comments filed in response to the IRFA.[218] To the extent we received comments raising general small business concerns during this proceeding, those comments are discussed throughout the Order.

89. We disagree with Alexicon that small carriers are less vulnerable to unauthorized attempts to access CPNI.[219] In fact, Alexicon itself points out that one of its client companies actually experienced an unauthorized access attempt, and thus we find the steps the Commission takes in this Order are applicable to all carriers.[220] We do, however, agree with commenters that argue the Commission should not adopt many of EPIC's suggested requirements.[221] We also agree with commenters that argue for flexible rules to allow carriers to determine proper authentication methods for its customers.[222] Therefore, we do not adopt specific authentication methods, or back-up authentication methods for lost or forgotten passwords and instead adopt rules that provide limits on the types of authentication methods that meet section 222's mandate to protect CPNI.[223] Further, we agree with commenters that small carriers should be provided ***6980** additional time to implement the requirements that we do adopt in this Order.[224] Thus, we provide small carriers with an additional six month implementation period for the online carrier authentication requirements adopted in this Order.[225]

**27 90. *Comments Received in Response to the IP-Enabled Services Notice*. In this section, we respond to comments filed in response to the IRFA.[226] To the extent we received comments raising general small business concerns during this proceeding, those comments are discussed throughout the Order.

91. We disagree with the SBA and Menard that the Commission should postpone acting in this proceeding -- thereby postponing extending the application of the CPNI rules to interconnected VoIP service providers -- and instead should reevaluate the economic impact and the compliance burdens on small entities and issue a further notice of proposed rulemaking in conjunction with a supplemental IRFA identifying and analyzing the economic impacts on small entities and

less burdensome alternatives.[227] We believe the additional steps suggested by SBA and Menard are unnecessary because small entities already have received sufficient notice of the issues addressed in today's Order[228] and because the Commission has considered the economic impact on small entities and what ways are feasible to minimize the burdens imposed on those entities, and, to the extent feasible, has implemented those less burdensome alternatives.[229]

C. Description and Estimate of the Number of Small Entities to Which Rules Will Apply

92. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein.[230] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[231] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[232] A small business concern is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[233]

***6981** 93. *Small Businesses*. Nationwide, there are a total of approximately 22.4 million small businesses, according to SBA data.[234]

94. *Small Organizations*. Nationwide, there are approximately 1.6 million small organizations.[235]

95. *Small Governmental Jurisdictions*. The term "small governmental jurisdiction" is defined generally as "governments of cities, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[236] Census Bureau data for 2002 indicate that there were 87,525 local governmental jurisdictions in the United States.[237] We estimate that, of this total, 84,377 entities were "small governmental jurisdictions."[238] Thus, we estimate that most governmental jurisdictions are small.

1. Telecommunications Service Entities

a. Wireline Carriers and Service Providers

96. We have included small incumbent local exchange carriers in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small business size standard (*e.g.*, a telephone communications business having 1,500 or fewer employees), and "is not dominant in its field of operation."[239] The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent local exchange carriers are not dominant in their field of operation because any such dominance is not "national" in scope.[240] We have therefore included small incumbent local exchange carriers in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

****28** 97. *Incumbent Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[241] According to Commission data,[242] 1,303 carriers have reported that they are engaged in the provision of incumbent local exchange services. Of these 1,303 carriers, an estimated 1,020 have 1,500 or fewer employees and 283 have more than 1,500 employees. Consequently, the Commission estimates that most providers of incumbent ***6982** local exchange service are small businesses that may be affected by our action.

98. *Competitive Local Exchange Carriers, Competitive Access Providers (CAPs), "Shared-Tenant Service Providers," and "Other Local Service Providers."* Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[243] According to Commission data,[244] 769 carriers have reported that they are engaged in the provision of either competitive access provider services or competitive local exchange carrier services. Of these 769 carriers, an estimated 676 have 1,500 or fewer employees and 93 have more than 1,500 employees. In addition, 12 carriers have reported that they are "Shared-Tenant Service Providers," and all 12 are estimated to have 1,500 or fewer employees. In addition, 39 carriers have reported that they are "Other Local Service Providers." Of the 39, an estimated 38 have 1,500 or fewer employees and one has more than 1,500 employees. Consequently, the Commission estimates that most providers of competitive local exchange service, competitive

access providers, "Shared-Tenant Service Providers," and "Other Local Service Providers" are small entities that may be affected by our action.

99. *Local Resellers*. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[245] According to Commission data,[246] 143 carriers have reported that they are engaged in the provision of local resale services. Of these, an estimated 141 have 1,500 or fewer employees and two have more than 1,500 employees. Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by our action.

100. *Toll Resellers*. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[247] According to Commission data,[248] 770 carriers have reported that they are engaged in the provision of toll resale services. Of these, an estimated 747 have 1,500 or fewer employees and 23 have more than 1,500 employees. Consequently, the Commission estimates that the majority of toll resellers are small entities that may be affected by our action.

****29** 101. *Payphone Service Providers (PSPs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for payphone services providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[249] According to Commission data,[250] 613 carriers have reported that they are engaged in the provision of payphone services. Of these, an estimated 609 have 1,500 or fewer employees and four have more than 1,500 employees. Consequently, the Commission estimates that the majority of payphone service providers are small entities that may be affected by our action.

***6983** 102. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for providers of interexchange services. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[251] According to Commission data,[252] 316 carriers have reported that they are engaged in the provision of interexchange service. Of these, an estimated 292 have 1,500 or fewer employees and 24 have more than 1,500 employees. Consequently, the Commission estimates that the majority of IXCs are small entities that may be affected by our action.

103. *Operator Service Providers (OSPs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for operator service providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[253] According to Commission data,[254] 23 carriers have reported that they are engaged in the provision of operator services. Of these, an estimated 20 have 1,500 or fewer employees and three have more than 1,500 employees. Consequently, the Commission estimates that the majority of OSPs are small entities that may be affected by our action.

104. *Prepaid Calling Card Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. The appropriate size standard under SBA rules is for the category Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[255] According to Commission data,[256] 89 carriers have reported that they are engaged in the provision of prepaid calling cards. Of these, 88 are estimated to have 1,500 or fewer employees and one has more than 1,500 employees. Consequently, the Commission estimates that all or the majority of prepaid calling card providers are small entities that may be affected by our action.

105. *800 and 800-Like Service Subscribers*.[257] Neither the Commission nor the SBA has developed a small business size standard specifically for 800 and 800-like service ("toll free") subscribers. The appropriate size standard under SBA rules is for the category Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[258] The most reliable source of information regarding the number of these service subscribers appears to be data the Commission collects on the 800, 888, and 877 numbers in use.[259] According to our data, at the end of January, 1999, the number of 800 numbers assigned was 7,692,955; the number of 888 numbers assigned was 7,706,393; and the number of 877 numbers assigned was 1,946,538. We do not have data specifying the number of these subscribers that are not independently owned and operated or have more than 1,500 employees, and thus are unable at this time to estimate with greater precision the number of toll free subscribers that would qualify as small businesses under the SBA size standard. Consequently, we ***6984** estimate that there are 7,692,955 or fewer small entity 800 subscribers; 7,706,393 or fewer small entity 888

subscribers; and 1,946,538 or fewer small entity 877 subscribers.

b. International Service Providers

****30** 106. The Commission has not developed a small business size standard specifically for providers of international service. The appropriate size standards under SBA rules are for the two broad census categories of "Satellite Telecommunications" and "Other Telecommunications." Under both categories, such a business is small if it has $12.5 million or less in average annual receipts.[260]

107. The first category of Satellite Telecommunications "comprises establishments primarily engaged in providing point-to-point telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[261] For this category, Census Bureau data for 2002 show that there were a total of 371 firms that operated for the entire year.[262] Of this total, 307 firms had annual receipts of under $10 million, and 26 firms had receipts of $10 million to $24,999,999.[263] Consequently, we estimate that the majority of Satellite Telecommunications firms are small entities that might be affected by our action.

108. The second category of Other Telecommunications "comprises establishments primarily engaged in (1) providing specialized telecommunications applications, such as satellite tracking, communications telemetry, and radar station operations; or (2) providing satellite terminal stations and associated facilities operationally connected with one or more terrestrial communications systems and capable of transmitting telecommunications to or receiving telecommunications from satellite systems."[264] For this category, Census Bureau data for 2002 show that there were a total of 332 firms that operated for the entire year.[265] Of this total, 259 firms had annual receipts of under $10 million and 15 firms had annual receipts of $10 million to $24,999,999.[266] Consequently, we estimate that the majority of Other Telecommunications firms are small entities that might be affected by our action.

c. Wireless Telecommunications Service Providers

109. Below, for those services subject to auctions, we note that, as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Also, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated.

***6985** 110. *Wireless Service Providers*. The SBA has developed a small business size standard for wireless firms within the two broad economic census categories of "Paging"[267] and "Cellular and Other Wireless Telecommunications."[268] Under both SBA categories, a wireless business is small if it has 1,500 or fewer employees. For the census category of Paging, Census Bureau data for 2002 show that there were 807 firms in this category that operated for the entire year.[269] Of this total, 804 firms had employment of 999 or fewer employees, and three firms had employment of 1,000 employees or more.[270] Thus, under this category and associated small business size standard, the majority of firms can be considered small. For the census category of Cellular and Other Wireless Telecommunications, Census Bureau data for 2002 show that there were 1,397 firms in this category that operated for the entire year.[271] Of this total, 1,378 firms had employment of 999 or fewer employees, and 19 firms had employment of 1,000 employees or more.[272] Thus, under this second category and size standard, the majority of firms can, again, be considered small.

****31** 111. *Cellular Licensees*. The SBA has developed a small business size standard for wireless firms within the broad economic census category "Cellular and Other Wireless Telecommunications."[273] Under this SBA category, a wireless business is small if it has 1,500 or fewer employees. For the census category of Cellular and Other Wireless Telecommunications, Census Bureau data for 2002 show that there were 1,397 firms in this category that operated for the entire year.[274] Of this total, 1,378 firms had employment of 999 or fewer employees, and 19 firms had employment of 1,000 employees or more.[275] Thus, under this category and size standard, the great majority of firms can be considered small. Also, according to Commission data, 437 carriers reported that they were engaged in the provision of cellular service, Personal Communications Service (PCS), or Specialized Mobile Radio (SMR) Telephony services, which are placed together in the data.[276] We have estimated that 260 of these are small, under the SBA small business size standard.[277]

112. *Common Carrier Paging*. The SBA has developed a small business size standard for wireless firms within the broad

economic census category, "Cellular and Other Wireless Telecommunications."[278] Under this SBA category, a wireless business is small if it has 1,500 or fewer employees. For the census category of Paging, Census Bureau data for 2002 show that there were 807 ***6986** firms in this category that operated for the entire year.[279] Of this total, 804 firms had employment of 999 or fewer employees, and three firms had employment of 1,000 employees or more.[280] Thus, under this category and associated small business size standard, the majority of firms can be considered small. In the Paging *Third Report and Order*, we developed a small business size standard for "small businesses" and "very small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments.[281] A "small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $15 million for the preceding three years. Additionally, a "very small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years.[282] The SBA has approved these small business size standards.[283] An auction of Metropolitan Economic Area licenses commenced on February 24, 2000, and closed on March 2, 2000.[284] Of the 985 licenses auctioned, 440 were sold. Fifty-seven companies claiming small business status won. Also, according to Commission data, 375 carriers reported that they were engaged in the provision of paging and messaging services.[285] Of those, we estimate that 370 are small, under the SBA-approved small business size standard.[286]

113. *Wireless Communications Services*. This service can be used for fixed, mobile, radiolocation, and digital audio broadcasting satellite uses. The Commission established small business size standards for the wireless communications services (WCS) auction. A "small business" is an entity with average gross revenues of $40 million for each of the three preceding years, and a "very small business" is an entity with average gross revenues of $15 million for each of the three preceding years. The SBA has approved these small business size standards.[287] The Commission auctioned geographic area licenses in the WCS service. In the auction, there were seven winning bidders that qualified as "very small business" entities, and one that qualified as a "small business" entity.

****32** 114. *Wireless Telephony*. Wireless telephony includes cellular, personal communications services (PCS), and specialized mobile radio (SMR) telephony carriers. As noted earlier, the SBA has developed a small business size standard for "Cellular and Other Wireless Telecommunications" services.[288] Under that SBA small business size standard, a business is small if it has 1,500 or fewer employees.[289] According to Commission data, 445 carriers reported that they were engaged in the ***6987** provision of wireless telephony.[290] We have estimated that 245 of these are small under the SBA small business size standard.

115. *Broadband Personal Communications Service*. The broadband Personal Communications Service (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission defined "small entity" for Blocks C and F as an entity that has average gross revenues of $40 million or less in the three previous calendar years.[291] For Block F, an additional classification for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years."[292] These standards defining "small entity" in the context of broadband PCS auctions have been approved by the SBA.[293] No small businesses, within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that qualified as small entities in the Block C auctions. A total of 93 small and very small business bidders won approximately 40 percent of the 1,479 licenses for Blocks D, E, and F.[294] On March 23, 1999, the Commission re-auctioned 347 C, D, E, and F Block licenses. There were 48 small business winning bidders. On January 26, 2001, the Commission completed the auction of 422 C and F Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in this auction, 29 qualified as "small" or "very small" businesses. Subsequent events, concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant.

116. *Narrowband Personal Communications Services*. To date, two auctions of narrowband personal communications services (PCS) licenses have been conducted. For purposes of the two auctions that have already been held, "small businesses" were entities with average gross revenues for the prior three calendar years of $40 million or less. Through these auctions, the Commission has awarded a total of 41 licenses, out of which 11 were obtained by small businesses. To ensure meaningful participation of small business entities in future auctions, the Commission has adopted a two-tiered small business size standard in the *Narrowband PCS Second Report and Order*.[295] A "small business" is an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $40 million. A "very small business" is an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $15 million. The SBA has approved these small business size standards.[296] In the

future, the Commission will auction 459 licenses to serve Metropolitan Trading Areas (MTAs) and 408 response channel licenses. There is also one megahertz of narrowband PCS spectrum that has been held in reserve and that the Commission has not yet decided to release for licensing. The Commission cannot predict accurately the number of licenses that will be awarded to small entities in future auctions. However, four of the 16 ***6988** winning bidders in the two previous narrowband PCS auctions were small businesses, as that term was defined. The Commission assumes, for purposes of this analysis that a large portion of the remaining narrowband PCS licenses will be awarded to small entities. The Commission also assumes that at least some small businesses will acquire narrowband PCS licenses by means of the Commission's partitioning and disaggregation rules.

****33** 117. *220 MHz Radio Service -- Phase I Licensees*. The 220 MHz service has both Phase I and Phase II licenses. Phase I licensing was conducted by lotteries in 1992 and 1993. There are approximately 1,515 such non-nationwide licensees and four nationwide licensees currently authorized to operate in the 220 MHz band. The Commission has not developed a small business size standard for small entities specifically applicable to such incumbent 220 MHz Phase I licensees. To estimate the number of such licensees that are small businesses, we apply the small business size standard under the SBA rules applicable to "Cellular and Other Wireless Telecommunications" companies. This category provides that a small business is a wireless company employing no more than 1,500 persons.[297] For the census category Cellular and Other Wireless Telecommunications, Census Bureau data for 1997 show that there were 977 firms in this category, total, that operated for the entire year.[298] Of this total, 965 firms had employment of 999 or fewer employees, and an additional 12 firms had employment of 1,000 employees or more.[299] Thus, under this second category and size standard, the majority of firms can, again, be considered small. Assuming this general ratio continues in the context of Phase I 220 MHz licensees, the Commission estimates that nearly all such licensees are small businesses under the SBA's small business size standard. In addition, limited preliminary census data for 2002 indicate that the total number of cellular and other wireless telecommunications carriers increased approximately 321 percent from 1997 to 2002.[300]

118. *220 MHz Radio Service -- Phase II Licensees*. The 220 MHz service has both Phase I and Phase II licenses. The Phase II 220 MHz service is a new service, and is subject to spectrum auctions. In the *220 MHz Third Report and Order*, we adopted a small business size standard for "small" and "very small" businesses for purposes of determining their eligibility for special provisions such as bidding credits and installment payments.[301] This small business size standard indicates that a "small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $15 million for the preceding three years.[302] A "very small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues that do not exceed $3 million for the preceding three years. The SBA has approved these small business size standards.[303] Auctions of Phase II licenses commenced on September 15, 1998, and closed on October 22, 1998.[304] In the first ***6989** auction, 908 licenses were auctioned in three different-sized geographic areas: three nationwide licenses, 30 Regional Economic Area Group (EAG) Licenses, and 875 Economic Area (EA) Licenses. Of the 908 licenses auctioned, 693 were sold.[305] Thirty-nine small businesses won licenses in the first 220 MHz auction. The second auction included 225 licenses: 216 EA licenses and 9 EAG licenses. Fourteen companies claiming small business status won 158 licenses.[306]

****34** 119. *800 MHz and 900 MHz Specialized Mobile Radio Licenses*. The Commission awards "small entity" and "very small entity" bidding credits in auctions for Specialized Mobile Radio (SMR) geographic area licenses in the 800 MHz and 900 MHz bands to firms that had revenues of no more than $15 million in each of the three previous calendar years, or that had revenues of no more than $3 million in each of the previous calendar years, respectively.[307] These bidding credits apply to SMR providers in the 800 MHz and 900 MHz bands that either hold geographic area licenses or have obtained extended implementation authorizations. The Commission does not know how many firms provide 800 MHz or 900 MHz geographic area SMR service pursuant to extended implementation authorizations, nor how many of these providers have annual revenues of no more than $15 million. One firm has over $15 million in revenues. The Commission assumes, for purposes here, that all of the remaining existing extended implementation authorizations are held by small entities, as that term is defined by the SBA. The Commission has held auctions for geographic area licenses in the 800 MHz and 900 MHz SMR bands. There were 60 winning bidders that qualified as small or very small entities in the 900 MHz SMR auctions. Of the 1,020 licenses won in the 900 MHz auction, bidders qualifying as small or very small entities won 263 licenses. In the 800 MHz auction, 38 of the 524 licenses won were won by small and very small entities.

120. *700 MHz Guard Band Licensees*. In the *700 MHz Guard Band Order*, we adopted a small business size standard for "small businesses" and "very small businesses" for purposes of determining their eligibility for special provisions such as

bidding credits and installment payments.[308] A "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $15 million for the preceding three years. Additionally, a "very small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years. An auction of 52 Major Economic Area (MEA) licenses commenced on September 6, 2000, and closed on September 21, 2000.[309] Of the 104 licenses auctioned, 96 licenses were sold to nine bidders. Five of these bidders were small businesses that won a total of 26 licenses. A second auction of 700 MHz Guard Band licenses commenced on February 13, 2001 and closed on February 21, 2001. All eight of the licenses auctioned were sold to three bidders. One of these bidders was a small business that won a total of two licenses.[310]

121. *Rural Radiotelephone Service*. The Commission has not adopted a size standard for small businesses specific to the Rural Radiotelephone Service.[311] A significant subset of the Rural Radiotelephone Service is the Basic Exchange Telephone Radio System (BETRS).[312] The Commission ***6990** uses the SBA's small business size standard applicable to "Cellular and Other Wireless Telecommunications," *i.e.*, an entity employing no more than 1,500 persons.[313] There are approximately 1,000 licensees in the Rural Radiotelephone Service, and the Commission estimates that there are 1,000 or fewer small entity licensees in the Rural Radiotelephone Service that may be affected by the rules and policies adopted herein.

****35** 122. *Air-Ground Radiotelephone Service*. The Commission has not adopted a small business size standard specific to the Air-Ground Radiotelephone Service.[314] We will use SBA's small business size standard applicable to "Cellular and Other Wireless Telecommunications," *i.e.*, an entity employing no more than 1,500 persons.[315] There are approximately 100 licensees in the Air-Ground Radiotelephone Service, and we estimate that almost all of them qualify as small under the SBA small business size standard.

123. *Aviation and Marine Radio Services*. Small businesses in the aviation and marine radio services use a very high frequency (VHF) marine or aircraft radio and, as appropriate, an emergency position-indicating radio beacon (and/or radar) or an emergency locator transmitter. The Commission has not developed a small business size standard specifically applicable to these small businesses. For purposes of this analysis, the Commission uses the SBA small business size standard for the category "Cellular and Other Telecommunications," which is 1,500 or fewer employees.[316] Most applicants for recreational licenses are individuals. Approximately 581,000 ship station licensees and 131,000 aircraft station licensees operate domestically and are not subject to the radio carriage requirements of any statute or treaty. For purposes of our evaluations in this analysis, we estimate that there are up to approximately 712,000 licensees that are small businesses (or individuals) under the SBA standard. In addition, between December 3, 1998 and December 14, 1998, the Commission held an auction of 42 VHF Public Coast licenses in the 157.1875-157.4500 MHz (ship transmit) and 161.775-162.0125 MHz (coast transmit) bands. For purposes of the auction, the Commission defined a "small" business as an entity that, together with controlling interests and affiliates, has average gross revenues for the preceding three years not to exceed $15 million dollars. In addition, a "very small" business is one that, together with controlling interests and affiliates, has average gross revenues for the preceding three years not to exceed $3 million dollars.[317] There are approximately 10,672 licensees in the Marine Coast Service, and the Commission estimates that almost all of them qualify as "small" businesses under the above special small business size standards.

124. *Offshore Radiotelephone Service*. This service operates on several UHF television broadcast channels that are not used for television broadcasting in the coastal areas of states bordering the Gulf of Mexico.[318] There are presently approximately 55 licensees in this service. We are unable to estimate at this time the number of licensees that would qualify as small under the SBA's small business size standard for "Cellular and Other Wireless Telecommunications" services.[319] Under that SBA small business size standard, a business is small if it has 1,500 or fewer employees.[320]

****36 *6991** 125. *39 GHz Service*. The Commission created a special small business size standard for 39 GHz licenses -- an entity that has average gross revenues of $40 million or less in the three previous calendar years.[321] An additional size standard for "very small business" is: an entity that, together with affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years.[322] The SBA has approved these small business size standards.[323] The auction of the 2,173 39 GHz licenses began on April 12, 2000 and closed on May 8, 2000. The 18 bidders who claimed small business status won 849 licenses. Consequently, the Commission estimates that 18 or fewer 39 GHz licensees are small entities that may be affected by the rules and polices adopted herein.

126. *Multipoint Distribution Service, Multichannel Multipoint Distribution Service, and ITFS*. Multichannel Multipoint

Distribution Service (MMDS) systems, often referred to as "wireless cable," transmit video programming to subscribers using the microwave frequencies of the Multipoint Distribution Service (MDS) and Instructional Television Fixed Service (ITFS).[324] In connection with the 1996 MDS auction, the Commission established a small business size standard as an entity that had annual average gross revenues of less than $40 million in the previous three calendar years.[325] The MDS auctions resulted in 67 successful bidders obtaining licensing opportunities for 493 Basic Trading Areas (BTAs). Of the 67 auction winners, 61 met the definition of a small business. MDS also includes licensees of stations authorized prior to the auction. In addition, the SBA has developed a small business size standard for Cable and Other Program Distribution, which includes all such companies generating $12.5 million or less in annual receipts.[326] According to Census Bureau data for 1997, there were a total of 1,311 firms in this category, total, that had operated for the entire year.[327] Of this total, 1,180 firms had annual receipts of under $10 million and an additional 52 firms had receipts of $10 million or more but less than $25 million. Consequently, we estimate that the majority of providers in this service category are small businesses that may be affected by the rules and policies adopted herein. This SBA small business size standard also appears applicable to ITFS. There are presently 2,032 ITFS licensees. All but 100 of these licenses are held by educational institutions. Educational institutions are included in this analysis as small entities.[328] Thus, we tentatively conclude that at least 1,932 licensees are small businesses.

127. *Local Multipoint Distribution Service*. Local Multipoint Distribution Service (LMDS) is a fixed broadband point-to-multipoint microwave service that provides for two-way video telecommunications.[329] The auction of the 1,030 Local Multipoint Distribution Service (LMDS) licenses ***6992** began on February 18, 1998 and closed on March 25, 1998. The Commission established a small business size standard for LMDS licenses as an entity that has average gross revenues of less than $40 million in the three previous calendar years.[330] An additional small business size standard for "very small business" was added as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years.[331] The SBA has approved these small business size standards in the context of LMDS auctions.[332] There were 93 winning bidders that qualified as small entities in the LMDS auctions. A total of 93 small and very small business bidders won approximately 277 A Block licenses and 387 B Block licenses. On March 27, 1999, the Commission re-auctioned 161 licenses; there were 40 winning bidders. Based on this information, we conclude that the number of small LMDS licenses consists of the 93 winning bidders in the first auction and the 40 winning bidders in the re-auction, for a total of 133 small entity LMDS providers.

****37** 128. *218-219 MHz Service*. The first auction of 218-219 MHz spectrum resulted in 170 entities winning licenses for 594 Metropolitan Statistical Area (MSA) licenses. Of the 594 licenses, 557 were won by entities qualifying as a small business. For that auction, the small business size standard was an entity that, together with its affiliates, has no more than a $6 million net worth and, after federal income taxes (excluding any carry over losses), has no more than $2 million in annual profits each year for the previous two years.[333] In the *218-219 MHz Report and Order and Memorandum Opinion and Order*, we established a small business size standard for a "small business" as an entity that, together with its affiliates and persons or entities that hold interests in such an entity and their affiliates, has average annual gross revenues not to exceed $15 million for the preceding three years.[334] A "very small business" is defined as an entity that, together with its affiliates and persons or entities that hold interests in such an entity and its affiliates, has average annual gross revenues not to exceed $3 million for the preceding three years.[335] We cannot estimate, however, the number of licenses that will be won by entities qualifying as small or very small businesses under our rules in future auctions of 218-219 MHz spectrum.

129. *24 GHz -- Incumbent Licensees*. This analysis may affect incumbent licensees who were relocated to the 24 GHz band from the 18 GHz band, and applicants who wish to provide services in the 24 GHz band. The applicable SBA small business size standard is that of "Cellular and Other Wireless Telecommunications" companies. This category provides that such a company is small if it employs no more than 1,500 persons.[336] According to Census Bureau data for 1997, there were 977 firms in this category, total, that operated for the entire year.[337] Of this total, 965 firms had employment of 999 or ***6993** fewer employees, and an additional 12 firms had employment of 1,000 employees or more.[338] Thus, under this size standard, the great majority of firms can be considered small. These broader census data notwithstanding, we believe that there are only two licensees in the 24 GHz band that were relocated from the 18 GHz band, Teligent[339] and TRW, Inc. It is our understanding that Teligent and its related companies have less than 1,500 employees, though this may change in the future. TRW is not a small entity. Thus, only one incumbent licensee in the 24 GHz band is a small business entity.

130. *24 GHz -- Future Licensees*. With respect to new applicants in the 24 GHz band, the small business size standard for "small business" is an entity that, together with controlling interests and affiliates, has average annual gross revenues for the three preceding years not in excess of $15 million.[340] "Very small business" in the 24 GHz band is an entity that, together

with controlling interests and affiliates, has average gross revenues not exceeding $3 million for the preceding three years.[341] The SBA has approved these small business size standards.[342] These size standards will apply to the future auction, if held.

2. Cable and OVS Operators

**38 131. *Cable and Other Program Distribution*. This category includes cable systems operators, closed circuit television services, direct broadcast satellite services, multipoint distribution systems, satellite master antenna systems, and subscription television services. The SBA has developed small business size standard for this census category, which includes all such companies generating $12.5 million or less in revenue annually.[343] According to Census Bureau data for 2002, there were a total of 1,191 firms in this category that operated for the entire year.[344] Of this total, 1,087 firms had annual receipts of under $10 million, and 43 firms had receipts of $10 million or more but less than $25 million.[345] Consequently, the Commission estimates that the majority of providers in this service category are small businesses that may be affected by the rules and policies adopted herein.

132. *Cable System Operators*. The Commission has developed its own small business size standards for cable system operators, for purposes of rate regulation. Under the Commission's rules, a **6994 "small cable company" is one serving fewer than 400,000 subscribers nationwide.[346] In addition, a "small system" is a system serving 15,000 or fewer subscribers.[347]

133. *Cable System Operators (Telecom Act Standard)*. The Communications Act of 1934, as amended, also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1 percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000."[348] The Commission has determined that there are approximately 67,700,000 subscribers in the United States.[349] Therefore, an operator serving fewer than 677,000 subscribers shall be deemed a small operator, if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate.[350] Based on available data, the Commission estimates that the number of cable operators serving 677,000 subscribers or fewer, totals 1,450. The Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million,[351] and therefore is unable, at this time, to estimate more accurately the number of cable system operators that would qualify as small cable operators under the size standard contained in the Communications Act of 1934.

134. *Open Video Services*. Open Video Service (OVS) systems provide subscription services.[352] The SBA has created a small business size standard for Cable and Other Program Distribution.[353] This standard provides that a small entity is one with $12.5 million or less in annual receipts. The Commission has certified approximately 25 OVS operators to serve 75 areas, and some of these are currently providing service.[354] Affiliates of Residential Communications Network, Inc. (RCN) received approval to operate OVS systems in New York City, Boston, Washington, D.C., and other areas. RCN has sufficient revenues to assure that they do not qualify as a small business entity. Little financial information is available for the other entities that are authorized to provide OVS and are not yet operational. Given that some entities authorized to provide OVS service have not yet begun to generate revenues, the Commission concludes that up to 24 OVS operators (those remaining) might qualify as small businesses that may be affected by the rules and policies adopted herein.

3. Internet Service Providers

**39 135. *Internet Service Providers*. The SBA has developed a small business size standard for Internet Service Providers (ISPs). ISPs "provide clients access to the Internet and generally provide related services such as web hosting, web page designing, and hardware or software consulting related to **6995 Internet connectivity."[355] Under the SBA size standard, such a business is small if it has average annual receipts of $21 million or less.[356] According to Census Bureau data for 2002, there were 2,529 firms in this category that operated for the entire year.[357] Of these, 2,437 firms had annual receipts of under $10 million, and 47 firms had receipts of $10 million or more but less then $25 million.[358] Consequently, we estimate that the majority of these firms are small entities that may be affected by our action.

4. Other Internet-Related Entities

136. *Web Search Portals*. Our action pertains to interconnected VoIP services, which could be provided by entities that provide other services such as email, online gaming, web browsing, video conferencing, instant messaging, and other, similar IP-enabled services. The Commission has not adopted a size standard for entities that create or provide these types of services

or applications. However, the census bureau has identified firms that "operate web sites that use a search engine to generate and maintain extensive databases of Internet addresses and content in an easily searchable format. Web search portals often provide additional Internet services, such as e-mail, connections to other web sites, auctions, news, and other limited content, and serve as a home base for Internet users."[359] The SBA has developed a small business size standard for this category; that size standard is $6 million or less in average annual receipts.[360] According to Census Bureau data for 1997, there were 195 firms in this category that operated for the entire year.[361] Of these, 172 had annual receipts of under $5 million, and an additional nine firms had receipts of between $5 million and $9,999,999. Consequently, we estimate that the majority of these firms are small entities that may be affected by our action.

137. *Data Processing, Hosting, and Related Services*. Entities in this category "primarily ... provid[e] infrastructure for hosting or data processing services."[362] The SBA has developed a small business size standard for this category; that size standard is $21 million or less in average annual receipts.[363] According to Census Bureau data for 1997, there were 3,700 firms in this category that operated for the entire year.[364] Of these, 3,477 had annual receipts of under $10 million, and an additional 108 firms had receipts of between $10 million and $24,999,999. Consequently, we estimate that the majority of these firms are small entities that may be affected by our action.

***6996** 138. *All Other Information Services*. "This industry comprises establishments primarily engaged in providing other information services (except new syndicates and libraries and archives)."[365] Our action pertains to interconnected VoIP services, which could be provided by entities that provide other services such as email, online gaming, web browsing, video conferencing, instant messaging, and other, similar IP-enabled services. The SBA has developed a small business size standard for this category; that size standard is $6 million or less in average annual receipts.[366] According to Census Bureau data for 1997, there were 195 firms in this category that operated for the entire year.[367] Of these, 172 had annual receipts of under $5 million, and an additional nine firms had receipts of between $5 million and $9,999,999. Consequently, we estimate that the majority of these firms are small entities that may be affected by our action.

****40** 139. *Internet Publishing and Broadcasting*. "This industry comprises establishments engaged in publishing and/or broadcasting content on the Internet exclusively. These establishments do not provide traditional (non-Internet) versions of the content that they publish or broadcast."[368] The SBA has developed a small business size standard for this new (2002) census category; that size standard is 500 or fewer employees.[369] To assess the prevalence of small entities in this category, we will use 1997 Census Bureau data for a relevant, now-superseded census category, "All Other Information Services." The SBA small business size standard for that prior category was $6 million or less in average annual receipts. According to Census Bureau data for 1997, there were 195 firms in the prior category that operated for the entire year.[370] Of these, 172 had annual receipts of under $5 million, and an additional nine firms had receipts of between $5 million and $9,999,999. Consequently, we estimate that the majority of the firms in this current category are small entities that may be affected by our action.

140. *Software Publishers*. These companies may design, develop or publish software and may provide other support services to software purchasers, such as providing documentation or assisting in installation. The companies may also design software to meet the needs of specific users. The SBA has developed a small business size standard of $21 million or less in average annual receipts for all of the following pertinent categories: Software Publishers, Custom Computer Programming Services, and Other Computer Related Services.[371] For Software Publishers, Census Bureau data for 1997 indicate that there were 8,188 firms in the category that operated for the entire year.[372] Of these, 7,633 had annual receipts under $10 million, and an additional 289 firms had receipts of between $10 million and $24, 999,999. For providers of Custom Computer Programming Services, the Census Bureau data indicate that there ***6997** were 19,334 firms that operated for the entire year.[373] Of these, 18,786 had annual receipts of under $10 million, and an additional 352 firms had receipts of between $10 million and $24,999,999. For providers of Other Computer Related Services, the Census Bureau data indicate that there were 5,524 firms that operated for the entire year.[374] Of these, 5,484 had annual receipts of under $10 million, and an additional 28 firms had receipts of between $10 million and $24,999,999. Consequently, we estimate that the majority of the firms in each of these three categories are small entities that may be affected by our action.

5. Equipment Manufacturers

141. The equipment manufacturers described in this section are merely indirectly affected by our current action, and therefore are not formally a part of this RFA analysis. We have included them, however, to broaden the record in this proceeding and to alert them to our decisions.

**41 142. *Wireless Communications Equipment Manufacturers*. The SBA has established a small business size standard for Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. Examples of products in this category include "transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment"[375] and may include other devices that transmit and receive IP-enabled services, such as personal digital assistants (PDAs). Under the SBA size standard, firms are considered small if they have 750 or fewer employees.[376] According to Census Bureau data for 1997, there were 1,215 establishments[377] in this category that operated for the entire year.[378] Of those, there were 1,150 that had employment of under 500, and an additional 37 that had employment of 500 to 999. The percentage of wireless equipment manufacturers in this category was approximately 61.35%,[379] so we estimate that the number of wireless equipment manufacturers with employment of under 500 was actually closer to 706, with an additional 23 establishments having employment of between 500 and 999. Consequently, we estimate that the majority of wireless communications equipment manufacturers are small entities that may be affected by our action.

143. *Telephone Apparatus Manufacturing*. This category "comprises establishments primarily engaged primarily in manufacturing wire telephone and data communications equipment."[380] Examples *6998 of pertinent products are "central office switching equipment, cordless telephones (except cellular), PBX equipment, telephones, telephone answering machines, and data communications equipment, such as bridges, routers, and gateways."[381] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[382] According to Census Bureau data for 1997, there were 598 establishments in this category that operated for the entire year.[383] Of these, 574 had employment of under 1,000, and an additional 17 establishments had employment of 1,000 to 2,499. Consequently, we estimate that the majority of these establishments are small entities that may be affected by our action.

144. *Electronic Computer Manufacturing*. This category "comprises establishments primarily engaged in manufacturing and/or assembling electronic computers, such as mainframes, personal computers, workstations, laptops, and computer servers."[384] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[385] According to Census Bureau data for 1997, there were 563 establishments in this category that operated for the entire year.[386] Of these, 544 had employment of under 1,000, and an additional 11 establishments had employment of 1,000 to 2,499. Consequently, we estimate that the majority of these establishments are small entities that may be affected by our action.

**42 145. *Computer Terminal Manufacturing*. "Computer terminals are input/output devices that connect with a central computer for processing."[387] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[388] According to Census Bureau data for 1997, there were 142 establishments in this category that operated for the entire year, and all of the establishments had employment of under 1,000.[389] Consequently, we estimate that the majority or all of these establishments are small entities that may be affected by our action.

146. *Other Computer Peripheral Equipment Manufacturing*. Examples of peripheral equipment in this category include keyboards, mouse devices, monitors, and scanners.[390] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[391] According to Census Bureau data for 1997, there were 1061 establishments in this *6999 category that operated for the entire year.[392] Of these, 1,046 had employment of under 1,000, and an additional six establishments had employment of 1,000 to 2,499. Consequently, we estimate that the majority of these establishments are small entities that may be affected by our action.

147. *Fiber Optic Cable Manufacturing*. These establishments manufacture "insulated fiber-optic cable from purchased fiber-optic strand."[393] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[394] According to Census Bureau data for 1997, there were 38 establishments in this category that operated for the entire year.[395] Of these, 37 had employment of under 1,000, and one establishment had employment of 1,000 to 2,499. Consequently, we estimate that the majority of these establishments are small entities that may be affected by our action.

148. *Other Communication and Energy Wire Manufacturing*. These establishments manufacture "insulated wire and cable of nonferrous metals from purchased wire."[396] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[397] According to Census Bureau data for 1997, there were 275

establishments in this category that operated for the entire year.[398] Of these, 271 had employment of under 1,000, and four establishments had employment of 1,000 to 2,499. Consequently, we estimate that the majority or all of these establishments are small entities that may be affected by our action.

149. *Audio and Video Equipment Manufacturing*. These establishments manufacture "electronic audio and video equipment for home entertainment, motor vehicle, public address and musical instrument amplifications."[399] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 750 or fewer employees.[400] According to Census Bureau data for 1997, there were 554 establishments in this category that operated for the entire year.[401] Of these, 542 had employment of under 500, and nine establishments had employment of 500 to 999. Consequently, we estimate that the majority of these establishments are small entities that may be affected by our action.

****43** 150. *Electron Tube Manufacturing*. These establishments are "primarily engaged in manufacturing electron tubes and parts (except glass blanks)."[402] The SBA has developed a small ***7000** business size standard for this category of manufacturing; that size standard is 750 or fewer employees.[403] According to Census Bureau data for 1997, there were 158 establishments in this category that operated for the entire year.[404] Of these, 148 had employment of under 500, and three establishments had employment of 500 to 999. Consequently, we estimate that the majority of these establishments are small entities that may be affected by our action.

151. *Bare Printed Circuit Board Manufacturing*. These establishments are "primarily engaged in manufacturing bare (i.e., rigid or flexible) printed circuit boards without mounted electronic components."[405] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[406] According to Census Bureau data for 1997, there were 1,389 establishments in this category that operated for the entire year.[407] Of these, 1,369 had employment of under 500, and 16 establishments had employment of 500 to 999. Consequently, we estimate that the majority of these establishments are small entities that may be affected by our action.

152. *Semiconductor and Related Device Manufacturing*. These establishments manufacture "computer storage devices that allow the storage and retrieval of data from a phase change, magnetic, optical, or magnetic/optical media."[408] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[409] According to Census Bureau data for 1997, there were 1,082 establishments in this category that operated for the entire year.[410] Of these, 987 had employment of under 500, and 52 establishments had employment of 500 to 999.

153. *Electronic Capacitor Manufacturing*. These establishments manufacture "electronic fixed and variable capacitors and condensers."[411] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[412] According to Census Bureau data for 1997, there were 128 establishments in this category that operated for the entire year.[413] Of these, 121 had employment of under 500, and four establishments had employment of 500 to 999.

***7001** 154. *Electronic Resistor Manufacturing*. These establishments manufacture "electronic resistors, such as fixed and variable resistors, resistor networks, thermistors, and varistors."[414] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[415] According to Census Bureau data for 1997, there were 118 establishments in this category that operated for the entire year.[416] Of these, 113 had employment of under 500, and 5 establishments had employment of 500 to 999.

****44** 155. *Electronic Coil, Transformer, and Other Inductor Manufacturing*. These establishments manufacture "electronic inductors, such as coils and transformers."[417] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[418] According to Census Bureau data for 1997, there were 448 establishments in this category that operated for the entire year.[419] Of these, 446 had employment of under 500, and two establishments had employment of 500 to 999.

156. *Electronic Connector Manufacturing*. These establishments manufacture "electronic connectors, such as coaxial, cylindrical, rack and panel, pin and sleeve, printed circuit and fiber optic."[420] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[421] According to Census Bureau data for 1997, there were 347 establishments in this category that operated for the entire year.[422] Of these, 332 had employment of under 500, and 12 establishments had employment of 500 to 999.

157. *Printed Circuit Assembly (Electronic Assembly) Manufacturing*. These are establishments "primarily engaged in loading components onto printed circuit boards or who manufacture and ship loaded printed circuit boards."[423] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[424] According to Census Bureau data for 1997, there were 714 establishments in this category that operated for the entire year.[425] Of these, 673 had employment of under 500, and 24 establishments had employment of 500 to 999.

***7002** 158. *Other Electronic Component Manufacturing*. These are establishments "primarily engaged in loading components onto printed circuit boards or who manufacture and ship loaded printed circuit boards."[426] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[427] According to Census Bureau data for 1997, there were 1,835 establishments in this category that operated for the entire year.[428] Of these, 1,814 had employment of under 500, and 18 establishments had employment of 500 to 999.

159. *Computer Storage Device Manufacturing*. These establishments manufacture "computer storage devices that allow the storage and retrieval of data from a phase change, magnetic, optical, or magnetic/optical media."[429] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[430] According to Census Bureau data for 1997, there were 209 establishments in this category that operated for the entire year.[431] Of these, 197 had employment of under 500, and eight establishments had employment of 500 to 999.

D. Description of Projected Reporting, Recordkeeping and Other Compliance Requirements

****45** 160. We are requiring telecommunications carriers and providers of interconnected VoIP service to collect certain information and take other actions to comply with our rules regarding the use of CPNI. For example, carriers must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis stating that the officer has personal knowledge that the carrier has established procedures that are adequate to ensure compliance with the CPNI rules.[432] The carrier must also provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the CPNI rules.[433] Further, the carrier must include an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the past year concerning the unauthorized release of CPNI.[434] Additionally, carriers must obtain opt-in approval before sharing CPNI with their joint venture partners or independent contractors for the purposes of marketing communications-related services to customers.[435] Also, carriers are required to maintain a record of any discovered breaches, notifications to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) regarding those breaches, as well as the USSS and FBI response to those notifications for a period of at least two years.[436]

***7003** 161. We also impose other requirements on telecommunications carriers and providers of interconnected VoIP service. Specifically, the Order prohibits carriers from releasing call detail information over the phone during customer-initiated telephone calls except by those methods provided for in the Order.[437] The Order also requires, with the exception of carriers that are small businesses, that a carrier not permit customers to gain access to an online account without first properly authenticating the customer and, for subsequent access, without a customer password or response to a back-up authentication method for lost or forgotten passwords, neither of which may be based on a carrier prompt for readily available biographical information, or account information.[438] For the rules pertaining to online carrier authentication, we provide carriers that satisfy the definition of a "small entity" or a "small business concern" under the RFA or SBA an additional six months to implement these rules.[439]

162. The Order also requires that carriers notify customers through a carrier-originated voicemail or text message to the telephone number of record, or by mail or email to the address of record whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.[440] Further, the Order requires that carriers notify the USSS and the FBI no later than seven days after a reasonable determination of a CPNI breach.[441]

E. Steps Taken to Minimize Significant Economic Impact on Small Entities, and Significant Alternatives Considered

****46** 163. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include (among others) the following four alternatives: (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification,

consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.[442]

164. The notices invited comment on a number of issues related to small entities. For example, the Commission sought comment on the effect the various proposals described in the *EPIC CPNI Notice* will have on small entities, and on what effect alternative rules would have on those entities.[443] Additionally, the Commission invited comment on ways in which the Commission can achieve its goal of protecting consumers while at the same time impose minimal burdens on small telecommunications service providers.[444] With respect to any of the Commission consumer protection regulations already in place, the Commission sought comment on whether it has adopted any provisions for small entities that the Commission should similarly consider in this proceeding? Specifically, it invited comment on whether the problems identified by EPIC were better or worse at smaller carriers.[445] The Commission invited comment on whether small carriers should be exempt from password-related ***7004** security procedures to protect CPNI.[446] The Commission invited comment on the benefits and burdens of recording audit trails for the disclosure of CPNI on small carriers.[447] The Commission invited comment on whether requiring a small carrier to encrypt its stored data would be unduly burdensome.[448] The Commission solicited comment on the cost to a small carrier of notifying a customer upon release of CPNI.[449] The Commission sought comment on whether the Commission should amend its rules to require carriers to file annual certifications concerning CPNI and whether this requirement should extend to only telecommunications carriers that are not small telephone companies as defined by the Small Business Administration, and whether small carriers should be subject to different CPNI-related obligations.[450]

165. The Commission has considered each of the alternatives described above, and in today's Order, imposes minimal regulation on small entities to the extent consistent with its goal of ensuring that carriers and providers of interconnected VoIP service protect against the unauthorized release of CPNI. Specifically, the Commission extended the implementation date for the rules pertaining to online authentication by six months so that small businesses will have additional time to come into compliance with the Order's rules.[451]

****47** 166. However, as stated above, we must assess the interests of small businesses in light of the overriding public interest of protecting against the unlawful release of CPNI. The Order discusses that CPNI is made up of very personal data.[452] Therefore, the Commission concluded that it was important for *all* telecommunications carriers and providers of interconnected VoIP service, including small businesses, to comply with the rules the Commission adopts in this Order six months after the Order's effective date or on receipt of OMB approval, as required by the Paperwork Reduction Act, whichever is later. For example, the Commission concluded that carriers and providers of interconnected VoIP service must stop releasing call detail information based on customer-initiated telephone calls except by those methods provided for in the Order. Additionally, the Commission concluded that it was important for *all* telecommunications carriers and providers of interconnected VoIP service to report breaches of CPNI data to law enforcement. The Commission therefore rejected solutions that would exempt small businesses. The record indicated that exempting small carriers from these regulations would compromise the Commission's goal of protecting all Americans from the unauthorized release of CPNI.

167. **Report to Congress:** The Commission will send a copy of the Order, including this FRFA, in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act.[453] In addition, the Commission will send a copy of the Order, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the Order and FRFA (or summaries thereof) will also be published in the Federal Register.[454]

***7005 Appendix D**

Initial Regulatory Flexibility Analysis

168. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[455] the Commission has prepared the present Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities that might result from this Further Notice. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the Further Notice provided above. The Commission will send a copy of the Further Notice, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration.[456] In addition, the Further Notice and the IRFA (or summaries thereof) will be published in the Federal Register.[457]

A. Need for, and Objectives of, the Proposed Rules

169. In the Further Notice, we seek comment on what steps the Commission should take, if any, to expand its CPNI rules further, and whether it should expand the consumer protections to ensure that customer information and CPNI are protected in the context of mobile communications devices. In particular, we seek comment on whether the Commission should adopt any further carrier requirements to protect CPNI, including password protection, audit trails, physical security, and limits on data retention.[458] Further, we seek comment on what methods carriers currently use, if any, for erasing customer information on mobile equipment prior to refurbishing the equipment, and the extent to which carriers enable customers to permanently erase their personal information prior to discarding the device.[459] We also seek comment on whether the Commission should require carriers or manufacturers to permanently erase, or allow customers to permanently erase, customer information in such circumstances.[460] For each of these issues, we seek comment on the burdens, including those placed on small carriers, associated with corresponding Commission rules related to each issue.[461]

B. Legal Basis

170. The legal basis for any action that may be taken pursuant to this Further Notice is contained in sections 1, 4(i), 4(j), and 222 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i)-(j), 222.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules May Apply

171. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules.[462] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and ***7006** "small governmental jurisdiction."[463] In addition, the term " small business" has the same meaning as the term "small business concern" under the Small Business Act.[464] A small business concern is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[465]

172. *Small Businesses*. Nationwide, there are a total of approximately 22.4 million small businesses, according to SBA data.[466]

173. *Small Organizations*. Nationwide, there are approximately 1.6 million small organizations.[467]

174. *Small Governmental Jurisdictions*. The term "small governmental jurisdiction" is defined generally as "governments of cities, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[468] Census Bureau data for 2002 indicate that there were 87,525 local governmental jurisdictions in the United States.[469] We estimate that, of this total, 84,377 entities were "small governmental jurisdictions."[470] Thus, we estimate that most governmental jurisdictions are small.

1. Telecommunications Service Entities

a. Wireline Carriers and Service Providers

175. We have included small incumbent local exchange carriers in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small business size standard (*e.g.*, a telephone communications business having 1,500 or fewer employees), and "is not dominant in its field of operation."[471] The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent local exchange carriers are not dominant in their field of operation because any such dominance is not "national" in scope.[472] We have therefore included small incumbent local ***7007** exchange carriers in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

176. *Incumbent Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[473] According to Commission data,[474] 1,303 carriers have reported that they are engaged in the provision of incumbent local exchange services. Of these 1,303 carriers, an estimated 1,020 have 1,500 or fewer employees and 283 have more than 1,500 employees. Consequently, the Commission estimates that most providers of incumbent local exchange

service are small businesses that may be affected by our action.

177. *Competitive Local Exchange Carriers, Competitive Access Providers (CAPs), "Shared-Tenant Service Providers," and "Other Local Service Providers."* Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[475] According to Commission data,[476] 769 carriers have reported that they are engaged in the provision of either competitive access provider services or competitive local exchange carrier services. Of these 769 carriers, an estimated 676 have 1,500 or fewer employees and 93 have more than 1,500 employees. In addition, 12 carriers have reported that they are "Shared-Tenant Service Providers," and all 12 are estimated to have 1,500 or fewer employees. In addition, 39 carriers have reported that they are "Other Local Service Providers." Of the 39, an estimated 38 have 1,500 or fewer employees and one has more than 1,500 employees. Consequently, the Commission estimates that most providers of competitive local exchange service, competitive access providers, "Shared-Tenant Service Providers," and "Other Local Service Providers" are small entities that may be affected by our action.

178. *Local Resellers*. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[477] According to Commission data,[478] 143 carriers have reported that they are engaged in the provision of local resale services. Of these, an estimated 141 have 1,500 or fewer employees and two have more than 1,500 employees. Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by our action.

179. *Toll Resellers*. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[479] According to Commission data,[480] 770 carriers have reported that they are engaged in the provision of toll resale services. Of these, an estimated 747 have 1,500 or fewer employees and 23 have ***7008** more than 1,500 employees. Consequently, the Commission estimates that the majority of toll resellers are small entities that may be affected by our action.

180. *Payphone Service Providers (PSPs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for payphone services providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[481] According to Commission data,[482] 613 carriers have reported that they are engaged in the provision of payphone services. Of these, an estimated 609 have 1,500 or fewer employees and four have more than 1,500 employees. Consequently, the Commission estimates that the majority of payphone service providers are small entities that may be affected by our action.

181. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for providers of interexchange services. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[483] According to Commission data,[484] 316 carriers have reported that they are engaged in the provision of interexchange service. Of these, an estimated 292 have 1,500 or fewer employees and 24 have more than 1,500 employees. Consequently, the Commission estimates that the majority of IXCs are small entities that may be affected by our action.

182. *Operator Service Providers (OSPs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for operator service providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[485] According to Commission data,[486] 23 carriers have reported that they are engaged in the provision of operator services. Of these, an estimated 20 have 1,500 or fewer employees and three have more than 1,500 employees. Consequently, the Commission estimates that the majority of OSPs are small entities that may be affected by our action.

183. *Prepaid Calling Card Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. The appropriate size standard under SBA rules is for the category Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[487] According to Commission data,[488] 89 carriers have reported that they are engaged in the provision of prepaid calling cards. Of these, 88 are estimated to have 1,500 or fewer employees and one has more than 1,500 employees. Consequently, the Commission estimates that all or the majority of prepaid calling card providers are small entities that may be affected by our

action.

***7009** 184. *800 and 800-Like Service Subscribers*.[489] Neither the Commission nor the SBA has developed a small business size standard specifically for 800 and 800-like service ("toll free") subscribers. The appropriate size standard under SBA rules is for the category Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[490] The most reliable source of information regarding the number of these service subscribers appears to be data the Commission collects on the 800, 888, and 877 numbers in use.[491] According to our data, at the end of January, 1999, the number of 800 numbers assigned was 7,692,955; the number of 888 numbers assigned was 7,706,393; and the number of 877 numbers assigned was 1,946,538. We do not have data specifying the number of these subscribers that are not independently owned and operated or have more than 1,500 employees, and thus are unable at this time to estimate with greater precision the number of toll free subscribers that would qualify as small businesses under the SBA size standard. Consequently, we estimate that there are 7,692,955 or fewer small entity 800 subscribers; 7,706,393 or fewer small entity 888 subscribers; and 1,946,538 or fewer small entity 877 subscribers.

b. International Service Providers

185. The Commission has not developed a small business size standard specifically for providers of international service. The appropriate size standards under SBA rules are for the two broad census categories of "Satellite Telecommunications" and "Other Telecommunications." Under both categories, such a business is small if it has $12.5 million or less in average annual receipts.[492]

186. The first category of Satellite Telecommunications "comprises establishments primarily engaged in providing point-to-point telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[493] For this category, Census Bureau data for 2002 show that there were a total of 371 firms that operated for the entire year.[494] Of this total, 307 firms had annual receipts of under $10 million, and 26 firms had receipts of $10 million to $24,999,999.[495] Consequently, we estimate that the majority of Satellite Telecommunications firms are small entities that might be affected by our action.

187. The second category of Other Telecommunications "comprises establishments primarily engaged in (1) providing specialized telecommunications applications, such as satellite tracking, communications telemetry, and radar station operations; or (2) providing satellite terminal stations and associated facilities operationally connected with one or more terrestrial communications systems and capable of transmitting telecommunications to or receiving telecommunications from satellite systems."[496] For this category, Census Bureau data for 2002 show that there were a total of 332 firms that operated for ***7010** the entire year.[497] Of this total, 259 firms had annual receipts of under $10 million and 15 firms had annual receipts of $10 million to $24,999,999.[498] Consequently, we estimate that the majority of Other Telecommunications firms are small entities that might be affected by our action.

c. Wireless Telecommunications Service Providers

188. Below, for those services subject to auctions, we note that, as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Also, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated.

189. *Wireless Service Providers*. The SBA has developed a small business size standard for wireless firms within the two broad economic census categories of "Paging"[499] and "Cellular and Other Wireless Telecommunications."[500] Under both SBA categories, a wireless business is small if it has 1,500 or fewer employees. For the census category of Paging, Census Bureau data for 2002 show that there were 807 firms in this category that operated for the entire year.[501] Of this total, 804 firms had employment of 999 or fewer employees, and three firms had employment of 1,000 employees or more.[502] Thus, under this category and associated small business size standard, the majority of firms can be considered small. For the census category of Cellular and Other Wireless Telecommunications, Census Bureau data for 2002 show that there were 1,397 firms in this category that operated for the entire year.[503] Of this total, 1,378 firms had employment of 999 or fewer employees, and 19 firms had employment of 1,000 employees or more.[504] Thus, under this second category and size standard, the majority of firms can, again, be considered small.

190. *Cellular Licensees*. The SBA has developed a small business size standard for wireless firms within the broad economic census category "Cellular and Other Wireless Telecommunications."[505] Under this SBA category, a wireless business is small if it has 1,500 or fewer employees. For the census category of Cellular and Other Wireless Telecommunications, Census Bureau data for 2002 show that there were 1,397 firms in this category that operated for the entire year.[506] Of this total, 1,378 firms had employment of 999 or fewer employees, and 19 firms had employment of 1,000 employees or more.[507] ***7011** Thus, under this category and size standard, the great majority of firms can be considered small. Also, according to Commission data, 437 carriers reported that they were engaged in the provision of cellular service, Personal Communications Service (PCS), or Specialized Mobile Radio (SMR) Telephony services, which are placed together in the data.[508] We have estimated that 260 of these are small, under the SBA small business size standard.[509]

191. *Common Carrier Paging*. The SBA has developed a small business size standard for wireless firms within the broad economic census category, "Cellular and Other Wireless Telecommunications."[510] Under this SBA category, a wireless business is small if it has 1,500 or fewer employees. For the census category of Paging, Census Bureau data for 2002 show that there were 807 firms in this category that operated for the entire year.[511] Of this total, 804 firms had employment of 999 or fewer employees, and three firms had employment of 1,000 employees or more.[512] Thus, under this category and associated small business size standard, the majority of firms can be considered small. In the Paging *Third Report and Order*, we developed a small business size standard for "small businesses" and "very small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments.[513] A "small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $15 million for the preceding three years. Additionally, a "very small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years.[514] The SBA has approved these small business size standards.[515] An auction of Metropolitan Economic Area licenses commenced on February 24, 2000, and closed on March 2, 2000.[516] Of the 985 licenses auctioned, 440 were sold. Fifty-seven companies claiming small business status won. Also, according to Commission data, 375 carriers reported that they were engaged in the provision of paging and messaging services.[517] Of those, we estimate that 370 are small, under the SBA-approved small business size standard.[518]

192. *Wireless Telephony*. Wireless telephony includes cellular, personal communications services (PCS), and specialized mobile radio (SMR) telephony carriers. As noted earlier, the SBA has developed a small business size standard for "Cellular and Other Wireless Telecommunications" ***7012** services.[519] Under that SBA small business size standard, a business is small if it has 1,500 or fewer employees.[520] According to Commission data, 445 carriers reported that they were engaged in the provision of wireless telephony.[521] We have estimated that 245 of these are small under the SBA small business size standard.

193. *Broadband Personal Communications Service*. The broadband Personal Communications Service (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission defined "small entity" for Blocks C and F as an entity that has average gross revenues of $40 million or less in the three previous calendar years.[522] For Block F, an additional classification for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years."[523] These standards defining "small entity" in the context of broadband PCS auctions have been approved by the SBA.[524] No small businesses, within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that qualified as small entities in the Block C auctions. A total of 93 small and very small business bidders won approximately 40 percent of the 1,479 licenses for Blocks D, E, and F.[525] On March 23, 1999, the Commission re-auctioned 347 C, D, E, and F Block licenses. There were 48 small business winning bidders. On January 26, 2001, the Commission completed the auction of 422 C and F Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in this auction, 29 qualified as "small" or "very small" businesses. Subsequent events, concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant.

194. *Narrowband Personal Communications Services*. To date, two auctions of narrowband personal communications services (PCS) licenses have been conducted. For purposes of the two auctions that have already been held, "small businesses" were entities with average gross revenues for the prior three calendar years of $40 million or less. Through these auctions, the Commission has awarded a total of 41 licenses, out of which 11 were obtained by small businesses. To ensure meaningful participation of small business entities in future auctions, the Commission has adopted a two-tiered small business size standard in the *Narrowband PCS Second Report and Order*.[526] A "small business" is an entity that, together with

affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $40 million. A "very small business" is an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $15 ***7013** million. The SBA has approved these small business size standards.[527] In the future, the Commission will auction 459 licenses to serve Metropolitan Trading Areas (MTAs) and 408 response channel licenses. There is also one megahertz of narrowband PCS spectrum that has been held in reserve and that the Commission has not yet decided to release for licensing. The Commission cannot predict accurately the number of licenses that will be awarded to small entities in future auctions. However, four of the 16 winning bidders in the two previous narrowband PCS auctions were small businesses, as that term was defined. The Commission assumes, for purposes of this analysis that a large portion of the remaining narrowband PCS licenses will be awarded to small entities. The Commission also assumes that at least some small businesses will acquire narrowband PCS licenses by means of the Commission's partitioning and disaggregation rules.

195. *Rural Radiotelephone Service*. The Commission has not adopted a size standard for small businesses specific to the Rural Radiotelephone Service.[528] A significant subset of the Rural Radiotelephone Service is the Basic Exchange Telephone Radio System (BETRS).[529] The Commission uses the SBA's small business size standard applicable to "Cellular and Other Wireless Telecommunications," *i.e.*, an entity employing no more than 1,500 persons.[530] There are approximately 1,000 licensees in the Rural Radiotelephone Service, and the Commission estimates that there are 1,000 or fewer small entity licensees in the Rural Radiotelephone Service that may be affected by the rules and policies adopted herein.

196. *Air-Ground Radiotelephone Service*. The Commission has not adopted a small business size standard specific to the Air-Ground Radiotelephone Service.[531] We will use SBA's small business size standard applicable to "Cellular and Other Wireless Telecommunications," *i.e.*, an entity employing no more than 1,500 persons.[532] There are approximately 100 licensees in the Air-Ground Radiotelephone Service, and we estimate that almost all of them qualify as small under the SBA small business size standard.

197. *Offshore Radiotelephone Service*. This service operates on several UHF television broadcast channels that are not used for television broadcasting in the coastal areas of states bordering the Gulf of Mexico.[533] There are presently approximately 55 licensees in this service. We are unable to estimate at this time the number of licensees that would qualify as small under the SBA's small business size standard for "Cellular and Other Wireless Telecommunications" services.[534] Under that SBA small business size standard, a business is small if it has 1,500 or fewer employees.[535]

2. Cable and OVS Operators

198. *Cable and Other Program Distribution*. This category includes cable systems operators, closed circuit television services, direct broadcast satellite services, multipoint distribution systems, satellite master antenna systems, and subscription television services. The SBA has developed small ***7014** business size standard for this census category, which includes all such companies generating $12.5 million or less in revenue annually.[536] According to Census Bureau data for 2002, there were a total of 1,191 firms in this category that operated for the entire year.[537] Of this total, 1,087 firms had annual receipts of under $10 million, and 43 firms had receipts of $10 million or more but less than $25 million.[538] Consequently, the Commission estimates that the majority of providers in this service category are small businesses that may be affected by the rules and policies adopted herein.

199. *Cable System Operators*. The Commission has developed its own small business size standards for cable system operators, for purposes of rate regulation. Under the Commission's rules, a "small cable company" is one serving fewer than 400,000 subscribers nationwide.[539] In addition, a "small system" is a system serving 15,000 or fewer subscribers.[540]

200. *Cable System Operators (Telecom Act Standard)*. The Communications Act of 1934, as amended, also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1 percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000."[541] The Commission has determined that there are approximately 67,700,000 subscribers in the United States.[542] Therefore, an operator serving fewer than 677,000 subscribers shall be deemed a small operator, if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate.[543] Based on available data, the Commission estimates that the number of cable operators serving 677,000 subscribers or fewer, totals 1,450. The Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million,[544] and therefore

is unable, at this time, to estimate more accurately the number of cable system operators that would qualify as small cable operators under the size standard contained in the Communications Act of 1934.

**48 201. *Open Video Services*. Open Video Service (OVS) systems provide subscription services.[545] The SBA has created a small business size standard for Cable and Other Program Distribution.[546] This standard provides that a small entity is one with $12.5 million or less in annual receipts. The Commission has certified approximately 25 OVS operators to serve 75 areas, and some of *7015 these are currently providing service.[547] Affiliates of Residential Communications Network, Inc. (RCN) received approval to operate OVS systems in New York City, Boston, Washington, D.C., and other areas. RCN has sufficient revenues to assure that they do not qualify as a small business entity. Little financial information is available for the other entities that are authorized to provide OVS and are not yet operational. Given that some entities authorized to provide OVS service have not yet begun to generate revenues, the Commission concludes that up to 24 OVS operators (those remaining) might qualify as small businesses that may be affected by the rules and policies adopted herein.

3. Internet Service Providers

202. *Internet Service Providers*. The SBA has developed a small business size standard for Internet Service Providers (ISPs). ISPs "provide clients access to the Internet and generally provide related services such as web hosting, web page designing, and hardware or software consulting related to Internet connectivity."[548] Under the SBA size standard, such a business is small if it has average annual receipts of $21 million or less.[549] According to Census Bureau data for 2002, there were 2,529 firms in this category that operated for the entire year.[550] Of these, 2,437 firms had annual receipts of under $10 million, and 47 firms had receipts of $10 million or more but less then $25 million.[551] Consequently, we estimate that the majority of these firms are small entities that may be affected by our action.

203. *All Other Information Services*. "This industry comprises establishments primarily engaged in providing other information services (except new syndicates and libraries and archives)."[552] The SBA has developed a small business size standard for this category; that size standard is $6 million or less in average annual receipts.[553] According to Census Bureau data for 1997, there were 195 firms in this category that operated for the entire year.[554] Of these, 172 had annual receipts of under $5 million, and an additional nine firms had receipts of between $5 million and $9,999,999. Consequently, we estimate that the majority of these firms are small entities that may be affected by our action.

4. Equipment Manufacturers

204. *Wireless Communications Equipment Manufacturers*. The SBA has established a small business size standard for Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. Examples of products in this category include "transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, *7016 and radio and television studio and broadcasting equipment"[555] and may include other devices that transmit and receive IP-enabled services, such as personal digital assistants (PDAs). Under the SBA size standard, firms are considered small if they have 750 or fewer employees.[556] According to Census Bureau data for 1997, there were 1,215 establishments[557] in this category that operated for the entire year.[558] Of those, there were 1,150 that had employment of under 500, and an additional 37 that had employment of 500 to 999. The percentage of wireless equipment manufacturers in this category was approximately 61.35%,[559] so we estimate that the number of wireless equipment manufacturers with employment of under 500 was actually closer to 706, with and additional 23 establishments having employment of between 500 and 999. Consequently, we estimate that the majority of wireless communications equipment manufacturers are small entities that may be affected by our action.

**49 205. *Telephone Apparatus Manufacturing*. This category "comprises establishments primarily engaged primarily in manufacturing wire telephone and data communications equipment."[560] Examples of pertinent products are "central office switching equipment, cordless telephones (except cellular), PBX equipment, telephones, telephone answering machines, and data communications equipment, such as bridges, routers, and gateways."[561] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[562] According to Census Bureau data for 1997, there were 598 establishments in this category that operated for the entire year.[563] Of these, 574 had employment of under 1,000, and an additional 17 establishments had employment of 1,000 to 2,499. Consequently, we estimate that the majority of these establishments are small entities that may be affected by our action.

206. *Semiconductor and Related Device Manufacturing*. These establishments manufacture "computer storage devices that

allow the storage and retrieval of data from a phase change, magnetic, optical, or magnetic/optical media."[564] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 500 or fewer employees.[565] According to Census Bureau ***7017** data for 1997, there were 1,082 establishments in this category that operated for the entire year.[566] Of these, 987 had employment of under 500, and 52 establishments had employment of 500 to 999.

207. *Computer Storage Device Manufacturing*. These establishments manufacture "computer storage devices that allow the storage and retrieval of data from a phase change, magnetic, optical, or magnetic/optical media."[567] The SBA has developed a small business size standard for this category of manufacturing; that size standard is 1,000 or fewer employees.[568] According to Census Bureau data for 1997, there were 209 establishments in this category that operated for the entire year.[569] Of these, 197 had employment of under 500, and eight establishments had employment of 500 to 999.

D. Description of Projected Reporting, Recordkeeping and Other Compliance Requirements

208. Should the Commission decide to adopt any further regulations to ensure that all providers of telecommunication services meet consumer protection needs in regard to CPNI, including the security of the privacy of customer information stored in mobile communications devices, the associated rules potentially could modify the reporting and recordkeeping requirements of certain telecommunications providers. We could, for instance, require that telecommunications providers require further customer password-related security procedures to access CPNI data.[570] We could also require telecommunications providers to track customer contact through the use of audit trails or to limit their retention of data related to CPNI.[571] Additionally, we could require additional physical safeguards be implemented to protect the transfer of CPNI.[572] Further, we could require telecommunications providers and/or manufacturers to configure wireless devices so consumers can easily and permanently delete personal information from mobile communications devices.[573] These proposals may impose additional reporting and recordkeeping requirements on entities. Also, we seek comment on whether any of these proposals places burdens on small entities.[574] Entities, especially small businesses, are encouraged to quantify the costs and benefits or any reporting requirement that may be established in this proceeding.

E. Steps Taken to Minimize Significant Economic Impact on Small Entities, and Significant Alternatives Considered

****50** 209. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include (among others) the following four alternatives: (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather ***7018** than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.[575]

210. The Commission's primary objective is to secure the privacy of customer information collected by telecommunications carriers and stored in mobile communications devices. We seek comment on the burdens, including those placed on small carriers, associated with related Commission rules and whether the Commission should adopt different requirements for small businesses.[576]

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

211. None.

***7019 STATEMENT OF CHAIRMAN KEVIN J. MARTIN**

****51** Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36

The unauthorized disclosure of consumers' private calling records is a significant privacy invasion. Today, the Commission significantly strengthens the Commission's existing safeguards and takes a strong approach to protecting consumer privacy.

The Commission has taken numerous steps to combat these alarming breaches of the privacy of consumers' telephone records. We investigated so-called "data brokers" to determine how they are obtaining this information, and levied forfeitures

against companies that failed to respond to our subpoenas and requests for information. We also investigated telecommunications carriers to determine whether they had implemented appropriate safeguards, and issued Notices of Apparent Liability against carriers that failed to comply with the Commission's rules.

The Order we adopt prohibits carriers from releasing over the phone sensitive personal data, call detail records, unless the customer provides a password, requires providers to notify customers immediately when changes are made to a customer's account and requires providers to notify their customers in the event of a breach of confidentiality. Service providers also must annually certify their compliance with these regulations, inform the Commission of any actions they have taken against data brokers, and provide a summary of the complaints they receive regarding the unauthorized release of CPNI. Today's action also ensures that law enforcement will have necessary tools to investigate and enforce illegal access to customer records.

While we work to create an environment in which market forces can thrive, the Commission must also act to protect consumers. With its strong approach to safeguarding consumer privacy, this item does just that. In particular, this item requires *express* consumer consent before a carrier may disclose a customer's phone records to joint venture partners or independent contractors for the purposes of marketing communications services. The former "opt-out" approach to customer consent, whereby a carrier may disclose a customer's phone records provided that a customer does not *expressly* withhold consent to such use, shifted too much of the burden to consumers, and has resulted in a much broader dissemination of consumer phone records. The "opt-in" approach adopted in this Order clearly is supported by the record, is consistent with applicable law, and directly advances our interest in protecting customer privacy.

Compliance with our consumer protection regulations is not optional for any telephone service provider. We need to take whatever actions are necessary to enforce these requirements to secure the privacy of personal and confidential information of American customers.

***7020 STATEMENT OF COMMISSIONER MICHAEL J. COPPS APPROVING IN PART, DISSENTING IN PART**

****52** Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36

Few rights are as fundamental as the right to privacy in our daily lives, but this cherished right seems under almost constant attack. As recent abuses by unscrupulous data brokers and others illustrate, the Commission's existing customer proprietary network information (CPNI) rules have not adequately protected individual privacy. Recognizing the seriousness of the threat, Congress recently made pretexting a federal crime. Now it is time for the Commission to step up to the plate and update its rules to protect consumers from the dangers that portend when personal information is turned over to telephone carriers.

Today we take action to protect the privacy of American consumers by imposing additional safeguards on how telephone carriers handle the vast amount of customers' personal information that they collect and hold. We require passwords before call detail information is released over the phone. We require carriers to provide notice to customers when changes occur to their accounts. Very importantly, we require carriers to obtain prior consent from their customers before providing personal information to their joint venture partners and independent contractors. My personal preference remains that a customer's private information should never be shared by a carrier with any entity for marketing purposes without a customer opting-in to the use of his or her personal information. But today's order strikes an acceptable balance -- a balance that will give consumers more confidence that their personal data will not be shared with certain third parties with whom the carriers have attenuated oversight. In 2002 I disagreed with the Commission's decision not to implement opt-in requirements for the use of consumers' personal information. In light of recent and well-documented abuses of consumer privacy, this recalibration of our rules is the least that we should do, and I very much appreciate the Chairman's willingness to take these important steps.

There is one aspect of this order, however, from which I must respectfully dissent. The Commission adopts a process by which customers could be left totally uninformed of unauthorized access to their CPNI for 14 days after a carrier reasonably determines there has been a records breach. Worse, the FBI and the U.S. Secret Service would have the ability to keep victims of these unauthorized disclosures in the dark even longer, perhaps indefinitely. As some have described it, it is akin to not telling victims of a burglary that their home has been broken into because law enforcement needs to continue dusting

for fingerprints.

**53 While I have always recognized the legitimate interests of law enforcement to be notified when there has been unauthorized access to a customer's CPNI, I also believe that consumers need to know when their private information has been accessed. There may be circumstances in which a delayed notification regime would be reasonable, for example, when an investigation of a large-scale breach of a database might be compromised because mass notification via the media is required. The Commission, however, adopts a rule that, in my opinion, is needlessly overbroad. It fails to distinguish those exigent circumstances in which delayed notification is necessary from what I believe to be the majority of cases in which immediate notification to a victim is appropriate. I continue to believe that notification to the victim of unauthorized access to their personal information will often actually aid law enforcement because the violator is frequently someone well known to the victim. If an unauthorized individual has gained access to personal telephone records involving victims of stalking or spousal violence, it won't be the carrier or the law enforcement agency -- but the victims -- who are in the best position to know when and how harm may be heading toward them.

*7021 Given the scope of the procedures adopted here -- procedures which pre-empt state consumer privacy protections to the extent that they require immediate notification to consumers when their privacy has been violated -- the delayed notification proposal would have benefited from greater scrutiny and analysis, particularly with respect to law enforcement's apparent unfettered ability to extend the period of non-notification. This seems especially important given the recent and troubling report by the Justice Department's own Inspector General raising serious questions as to whether the FBI properly followed the law in obtaining access to the telephone records of thousands of consumers. Our approach here requires more balance than the instant item provides.

Finally, while we make positive strides today, I look forward to taking prompt action on the proposals in the Further Notice regarding additional passwords, audit trails and data retention limits. When the stakes for misuse of our personal information are so high, the Commission must continue to be extraordinarily vigilant to ensure that the privacy of consumers is protected.

***7022 STATEMENT OF COMMISSIONER JONATHAN S. ADELSTEIN APPROVING IN PART, DISSENTING IN PART**

Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36

Through this proceeding, we address an issue of immediate personal importance to American consumers, the protection of sensitive information that telephone companies collect about their customers. This information can include some of the most private personal information about an individual, and failure to safeguard it can result in highly invasive intrusions into both the personal and professional lives of consumers. When someone gets hold of who you are calling, and for how long, it is like letting strangers pick your brain about your friends, plans or business dealings. So, I am pleased to support much of this Order, which takes meaningful steps to shut off the information drain that has left so many customers exasperated.

**54 Congress recognized the sensitivity of this information in the Telecommunications Act of 1996 when it prohibited phone companies from using or disclosing customer proprietary network information without the customer's approval. It charged the Commission with enforcing this privacy protection and the Commission previously adopted a set of rules designed to ensure that telephone companies have effective safeguards in place.

Today's action comes in response to the chorus of evidence detailing the need for greater privacy measures. Indeed, this proceeding flows from a petition filed by a watchful public interest group, the Electronic Privacy Information Center (EPIC), which alerted the FCC during the summer of 2005 to the troubling trend of telephone call records being made available on the Internet without customers' knowledge or consent. As EPIC then made clear to the Commission and as the record to this proceeding has borne out, disclosure of these records is far more than a mere annoyance; indeed, it can lead to tragic consequences.

So, our efforts here to strengthen our rules are critical and time sensitive. This Order takes several important steps tighten our rules and provide greater security for sensitive consumer records. Requiring more rigorous customer authentication, giving customers notice of account changes, and applying a more consumer-friendly approach to sharing of customer data should all

serve to improve customers control over their private data. As documented by EPIC, the sheer volume of customer information illegally available for public consumption made clear just how porous the existing firewalls and safeguards have been. At the same time, the Commission strikes a balanced approach in this Order, giving consumers greater ability to control their own information while also giving companies a degree of flexibility in how they implement safeguards. In this regard, I would like to thank Chairman Martin and the Wireline Competition Bureau for their attention to this item. Their extra work to fine tune the rules we adopt here will surely improve their functioning for consumers and providers alike.

Although much of this Order does exactly what Congress contemplated -- putting the customer in control -- there is one critical aspect where this Order falls short. Despite the Order's conclusion that customers should have notice of unauthorized disclosure of customer information, this Order set up a process which can result in the unnecessary and even indefinite delay of consumer notification without any accountability. Under these rules, the Commission gives the Federal Bureau of Investigation a potentially open-ended ability to delay customer notification of security breaches. While I expect that the FBI will work as quickly as possible to identify any investigative issues, I find no statutory basis in the Act for granting the FBI a blank check to delay notice to customers. I can understand the need for delay in extraordinary circumstances identified by law enforcement, but automatic delays coupled with ***7023** unlimited and unchecked extensions are not appropriate. Particularly given that timely notice to consumers may be essential for those customers to take protective action, I must dissent from this portion of the Order.

****55** Finally, even as we work here to improve our rules and as Congress considers additional safeguards, we must also re-double our efforts to address abuses of this private information. Swift enforcement action against companies that are violating our rules will be essential if we are to live up to our duty under the Act to protect customers' sensitive and private information.

***7024 STATEMENT OF COMMISSIONER DEBORAH TAYLOR TATE**
Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36

I have said time and again that the brokerage of personal information -- whether it be personal identity, financial records, or a list of phone calls -- is intolerable. "Pretexting" is nothing more than stealing; robbing consumers in a variety of slick ways of their most personal information. Indeed the law places a duty on telecommunications providers to protect this information and today, we take important steps to better secure private customer telephone records.

While I generally prefer market-based solutions to government intervention, I agree with my colleagues that the widespread actions of pretexters to obtain this type of personal customer information from carriers, required this action on our part.

I fully support strict requirements governing treatment of this sensitive data. However, I hope that the broad scope of our actions will not impact the ability of both companies and consumers to benefit from marketing information which may lead to lower prices or competitive bundled packages. An approach limiting the very strict "opt-in" obligations only to call detail records may have cured the problem at hand in a less burdensome manner.

In the end, however, customer privacy must take precedence. I am pleased that the rules we adopt today will go a long way towards closing off the avenues that information snatchers have repeatedly used to violate the privacy of consumer phone records.

***7025 STATEMENT OF COMMISSIONER ROBERT M. McDOWELL**
Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36

Pretexting has become the biggest threat to consumer security in the Information Age. Today's action further enhances the Commission's ability to protect consumers from these advanced fraudulent practices by strengthening our existing rules. Among the new requirements imposed on carriers, the decision prohibits carriers from releasing call detail information

during customer-initiated telephone calls except when the customer provides a password. It also precludes carriers from disclosing CPNI to independent contractors and joint venture partners without the customer's specific consent, and requires carriers to notify customers of all account changes and unauthorized disclosures of CPNI.

**56 We must take all necessary steps to protect unauthorized disclosure of this sensitive data, keeping in mind that pretexters are constantly trying new techniques to defraud consumers. In view of the pretexters' malevolent intent, the Commission will vigilantly pressure carriers to take precautions to stay ahead of the pretexters. However, our rules should strike a careful balance and should also guard against imposing over-reaching and unnecessary requirements that could cause unjustified burdens and costs on carriers. In the spirit of finding that balance, the *Further Notice* seeks comment on possible additional protections against unauthorized disclosure of CPNI. I look forward to reviewing the comments on those proposals.

Footnotes

1 As used in this Order, "pretexting" is the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records. Indeed, Congress has responded to the problem by making pretexting a criminal offense subject to fines and imprisonment. Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039).

2 CPNI includes personally identifiable information derived from a customer's relationship with a provider of communications services. Section 222 of the Communications Act of 1934, as amended (Communications Act, or Act), establishes a duty of every telecommunications carrier to protect the confidentiality of its customers' CPNI. 47 U.S.C. § 222. Section 222 was added to the Communications Act by the Telecommunications Act of 1996. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 151 *et seq*.).

3 This Order also extends the CPNI requirements to interconnected VoIP service providers. *See infra* Section IV.F. As used in this Order, the terms "communications carriers" and "carriers" refer to telecommunications carriers and providers of interconnected VoIP service.

4 Prior to the 1996 Act, the Commission had established CPNI requirements applicable to the enhanced services operations of AT&T, the Bell Operating Companies (BOCs), and GTE, and the customer premises equipment (CPE) operations of AT&T and the BOCs, in the Computer II, Computer III, GTE Open Network Architecture (ONA), and BOC CPE Relief proceedings. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8068-70, para. 7 (1998) (*CPNI Order*) (describing the Commission's privacy protections for confidential customer information in place prior to the 1996 Act).

5 Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) (EPIC Petition).

6 Section 222(a) imposes a general duty on telecommunications carriers to protect the confidentiality of proprietary information -- a duty owed to other carriers, equipment manufacturers, and customers. 47 U.S.C. § 222(a). Section 222(b) states that a carrier that receives or obtains proprietary information from other carriers in order to provide a telecommunications service may only use such information for that purpose and may not use that information for its own marketing efforts. 47 U.S.C. § 222(b). Section 222(c) outlines the confidentiality protections applicable to customer information. 47 U.S.C. § 222(c). Section 222(d) delineates certain exceptions to the general principle of confidentiality. 47 U.S.C. § 222(d). The Commission addressed the scope of section 222(e) in the *Subscriber List Information Order and Order on Reconsideration. Implementation of the Telecommunications Act of 1996:*

Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, Provision of Directory Listing Information Under the Telecommunications Act of 1934, as amended, CC Docket Nos. 96-115, 96-98, and 99-273, Third Report and Order, Second Order on Reconsideration, and Notice of Proposed Rulemaking, 14 FCC Rcd 15550 (1999) (*Subscriber List Information Order), on reconsideration*, CC Docket No. 96-115, Memorandum Opinion and Order on Reconsideration, 19 FCC Rcd 18439 (2004) (*Order on Reconsideration*).

7 The Commission's previous orders in this proceeding have addressed three general categories of customer information to which different privacy protections and carrier obligations apply pursuant to section 222: (1) individually identifiable CPNI, (2) aggregate customer information, and (3) subscriber list information. *See, e.g., CPNI Order*, 13 FCC Rcd 8061; *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, Provision of Directory Listing Information Under the Telecommunications Act of 1934, as amended*, CC Docket Nos. 96-115, 96-98, and 99-273, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409 (1999) (*CPNI Reconsideration Order*); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, Provision of Directory Listing Information Under the Telecommunications Act of 1934, as amended*, CC Docket Nos. 96-115, 96-98, and 99-273, Clarification Order and Second Further Notice of Proposed Rulemaking, 16 FCC Rcd 16506 (2001); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended; 2000 Biennial Regulatory Review -- Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, Third Report and Order and Third Further Notice of Proposed Rulemaking, CC Docket Nos. 96-115, 96-149, and 00-257, 17 FCC Rcd 14860 (2002) (*Third Report and Order*).

8 47 U.S.C. § 222(h)(1).

9 47 U.S.C. § 222(a).

10 *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 21 FCC Rcd 9990 (2006) (clarifying that section 222 does not prevent a telecommunications carrier from complying with the obligation in 42 U.S.C. § 13032 to report violations of specific federal statutes relating to child pornography).

11 47 U.S.C. § 222(c)(1). Subsequent to the adoption of section 222(c)(1), Congress added section 222(f). Section 222(f) provides that for purposes of section 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location information concerning the user of a commercial mobile service or (2) automatic crash notification information of any person other than for use in the operation of an automatic crash notification system. 47 U.S.C. § 222(f).

12 *See CPNI Order*, 13 FCC Rcd at 8101-02, para. 53.

13 47 U.S.C. § 222(c)(2).

14 *See CPNI Order*, 13 FCC Rcd 8061.

15 The Commission summarized the history of the CPNI proceeding in the *Third Report and Order*. *See Third Report and Order*, 17 FCC Rcd at 14863-72, paras. 5-25.

16 As the Commission discussed in the *CPNI Order*, "the language of section 222(c)(1)(A) and (B) reflects Congress' judgment that customer approval for carriers to use, disclose, and permit access to CPNI can be inferred in the context of an existing customer-carrier relationship. This is so because the customer is aware that its carrier has access to CPNI, and, through subscription to the carrier's service, has implicitly approved the carrier's use of CPNI within that existing relationship." *CPNI Order*, 13 FCC Rcd at 8080, para. 23 (introducing the "total service approach" to define the boundaries of a customer's implied consent concerning use of CPNI); *see also* 47 C.F.R. § 64.2005(a).

17 47 C.F.R. § 64.2007(b); *but see infra* Section IV.D. (modifying this disclosure requirement to require customer opt-in consent). A customer is deemed to have provided "opt-out approval" if that customer has been given appropriate notification of the carrier's request for consent consistent with the Commission's rules and the customer has failed to object to such use or disclosure within the waiting period described in section 64.2008(d)(1) of the Commission's rules, a minimum of 30 days. 47 C.F.R. § 64.2003(i); *see also* 47 C.F.R. § 64.2008(d)(1). Under the Commission's rules, carriers must also receive a customer's opt-out approval before intra-company use of CPNI beyond the total service approach. 47 U.S.C. § 64.2005(a), (b). Except as required by law, carriers may not disclose CPNI to third parties, or to their own affiliates that do not provide communications-related services, unless the consumer has given opt-in consent, which is express written, oral, or electronic consent. 47 C.F.R. §§ 64.2005(b), 64.2007(b)(3), 64.2008(e); *see also* 47 C.F.R. § 64.2003(h) (defining "opt-in approval").

18 47 U.S.C. § 222(c)(2); *see also, e.g., CPNI Order*, 13 FCC Rcd at 8101-02, para. 53; 47 C.F.R. § 2005(b)(3) (prohibiting the disclosure of CPNI without opt-in consent except as permitted by section 222 of the Act or the Commission's rules).

19 *See CPNI Order*, 13 FCC Rcd at 8195, para. 193.

20 47 C.F.R. § 64.2009(a); *see also CPNI Order*, 13 FCC Rcd at 8198, para. 198.

21 47 C.F.R. § 64.2009(b); *see also CPNI Order*, 13 FCC Rcd at 8198, para. 198.

22 47 C.F.R. § 64.2009(c); *see also CPNI Order*, 13 FCC Rcd at 8198-99, para. 199.

23 47 C.F.R. § 64.2009(d); *see also CPNI Order*, 13 FCC Rcd at 8199, para. 200.

24 47 C.F.R. § 64.2009(e); *see also CPNI Reconsideration Order*, 14 FCC Rcd at 14468 n.331 (clarifying that carriers must "make these certifications available for public inspection, copying and/or printing at any time during regular business hours at a centrally located business office of the carrier"). The Commission's rules also require carriers to notify the Commission in writing within five business days of any instance in which the opt-out mechanisms did not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly. 47 C.F.R. § 64.2009(f); *see Third Report and Order*, 17 FCC Rcd at 14910-11, paras. 114-15 (adopting such requirement).

25 *See IP-Enabled Services*, WC Docket No. 04-36, Notice of Proposed Rulemaking, 19 FCC Rcd 4863 (2004) (*IP-Enabled Services Notice*).

26 *IP-Enabled Services Notice*, 19 FCC Rcd at 4910, para. 71.

27 *See* EPIC Petition.

28 *See id*.

29 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, 21 FCC Rcd 1782 (2006) (*EPIC CPNI Notice or Notice*).

30 *See id*. at 1793, para. 29.

31 For example, the Enforcement Bureau issued Notices of Apparent Liability against Cbeyond Communications, LLC, Alltel Corporation, and AT&T for each failing to certify that they had established operating procedures adequate to ensure compliance with the Commission's rules governing the protection and use of CPNI. *Cbeyond Communications, LLC*, Notice of Apparent Liability for Forfeiture, 21 FCC Rcd 4316 (2006); *Alltel Corporation*, Notice of Apparent Liability for Forfeiture, 21 FCC Rcd 746 (2006); *AT&T, Inc.*, Notice of Apparent Liability for Forfeiture, 21 FCC Rcd 751 (2006). Additionally, AT&T recently notified the Commission that it failed to send its CPNI "opt-out" notice to 1.2 million customers resulting in the marketing to customers who may have otherwise opted out. *See* Letter from Davida M. Grant, Senior Counsel, AT&T Inc., to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 (filed Nov. 3, 2006) (AT&T CPNI Notification). Recent investigations by law enforcement authorities, including the Chicago Police Department and Federal Bureau of Investigation (FBI), have documented the ease with which a party, without proper authorization, may obtain the confidential calling records of consumers. *See* Law Enforcement and Phone Privacy Protection Act of 2006, H.R. Rep. No. 109-395, 109th Cong. 2d Sess. 2 (2006) (citing Frank Main, *Anyone Can Buy Cell Phone Records: Online Services Raise Security Concerns for Law Enforcement*, Chi. Sun-Times, January 5, 2006, at A3). For instance, a Chicago police official obtained call records of an undercover narcotics officer's telephone number, and received accurate call records within four hours of the request. *See* Prevention of Fraudulent Access to Phone Records Act, H.R. Rep. No. 109-398, 109th Cong. 2d Sess. 2 (2006); Frank Main, *Anyone Can Buy Cell Phone Records: Online Services Raise Security Concerns for Law Enforcement*, Chi. Sun Times, Jan. 5, 2006, at A3. In 1999, law enforcement authorities discovered that an information broker sold a Los Angeles detective's pager number to an Israeli mafia member who was trying to determine the identity of the detective's confidential information. *See* Frank Main, *Cell Call Lists Reveal Your Location: Anybody Can Pay to Track Where You Used Phone*, Chi. Sun Times, Jan. 19, 2006, at A3. Citizens themselves have also testified to the ease with which a pretexter can navigate easily around the carriers' authentication systems. For example, a political Internet blogger purchased the cell phone records of former presidential candidate General Wesley Clark. *See* Frank Main, *Blogger Buys Presidential Candidate's Call List: "Nobody's Records Are Untouchable," as $90 Purchase Online Shows*, Chi. Sun-Times, January 13, 2006, at A10. Journalist Christopher Byron also testified before Congress about his own battle with pretexters, stating that pretexters repeatedly called AT&T pretending to be him or his wife and asking for his phone records, which the pretexter was able to obtain. *See Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?: Hearings Before the Subcommittee on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. (Sept. 29, 2006) (testimony of Christopher Byron).

32 *See* Attorneys General Comments at 3 (identifying multiple filed lawsuits). All comments and reply comments cited in this Order

refer to comments and reply comments cited in CC Docket No. 96-115 unless otherwise stated.

33 *See, e.g., Cingular Wireless LLC v. Data Find Solutions, Inc.; James Kester; 1st Source Information Specialists Inc.; Kenneth W. Gorman; Steven Schwartz; John Does 1-100; and XYZ Corps. 1-100*, Case No. 1:05-CV-3269-CC (N.D. Ga. filed Dec. 23, 2005); *Cingular Wireless LLC v. Efindoutthetruth.com, Inc.; Lisa Loftus; Tiffany Wey; North American Services, LLC d/b/a North American Information; Tom Doyle; John Does 1-100; and XYZ Corps. 1-100*, Case No. 1:05-CV-3268-ODE (N.D. Ga. filed Dec. 23, 2005); *Cingular Wireless LLC v. Global Information Group, Inc.; GIG Liquidation, Inc. f/k/a Global Information Group; Bureau of Heirs, Inc.; Edward Herzog; Laurie Misner; Robin Goodwin; John Does 1-100; and XYZ Corps. 1-100*, Case No. 1:06-CV-0413-TWT (N.D. Ga. filed Feb. 23, 2006); *Cingular Wireless LLC v. Get A Grip Consulting, Inc.; Paraben Corporation d/b/a Get A Grip Software Publishing; Robert Schroeder; John Does 1-100; and XYZ Corps. 1-100*, Case No. 1:06-CV-0498 (N.D. Ga. filed Mar. 2, 2006).

34 *See, e.g., Sprint Nextel Corp. d/b/a Sprint Nextel v. I" Source Information Specialists, Inc., et al.*,Case No. 06001083 (02) (Broward County, Florida Cir. Ct. filed Jan. 26, 2006); *Sprint Nextel Corp. d/b/a Sprint Nextel v. All Star Investigations, Inc., et al.*, Case No. 06 01736 (Miami-Dade County, Florida Cir. Ct. filed Jan. 27, 2006); *Sprint Nextel Corp. d/b/a Sprint Nextel v. San Marco & Associates Private Investigation, Inc., et al.*, Case No. 8:06-CV-00484-T-17TGW (MD. Fla. filed March 17, 2006).

35 *See, e.g., T-Mobile USA, Inc. v. C.F. Anderson et al.*, Cause No. 06-2-04163 (King County Super. Ct. Feb. 2, 2006) (Stipulated Order and Permanent Injunction); *T-Mobile USA, Inc. v. 1st Source Information Services, et al.*, Case No. 06-2-03113-0 SEA (King County Super. Ct. May 22, 2006) (Final Order and Judgment); *T-Mobile USA, Inc. v. AccuSearch, et al.*, Case No. 06-2-06933-1 SEA (King County Super. Ct. filed May 18, 2006) (Stipulated Order of Injunction).

36 *See, e.g., Cellco Partnership d/b/a Verizon Wireless v. Source Resources*, Permanent Injunction on Consent, Docket No. SOM-L-I013-05 (Sup. Ct. of N.J.; Law Div.: Somerset County Sept. 13, 2005); *Cellco Partnership d/b/a Verizon Wireless v. Global Information Group, Inc., et al.*, Order, No. 05-09757 (Fla. Cir. Ct., 13th Judicial Circuit, Hillsborough County, Nov. 2, 2005); *Cellco Partnership d/b/a Verizon Wireless v. Data Find Solutions, Inc., et al.*, Order, No. 06-CV-326 (SRC) (D.N.J., Jan. 31, 2006).

37 *See* Matt Richtel and Miguel Helft, *An Industry Is Based on a Simple Masquerade*, N.Y. Times, Sept. 11, 2006, at C1; *see also* Charles Toutant, *Verizon Wireless Suing 'Pretexters' Who Gain Access to Customer Data*, 186 N.J.L.J. 976 (2006); Marguerite E. Patrick, *Lessons Learned: Issues Exposed in the Aftermath of the Hewlett-Packard Debacle*, 1 Privacy & Data Protection Leg. Rep. 1 (October 2006); *Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?: Hearings Before the Subcommittee on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. (Sept. 26, 2006) (testimony of Michael Holden).

38 *See* H.R. Rep. 109-398 at 2.

39 *See Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?: Hearings Before the Subcommittee on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 1 (Sept. 29, 2006) (testimony of the Joel Winston, Federal Trade Commission) (citing *FTC v. Info Search, Inc.*, No. 1:06-CV-01099-AMD (D. Md. filed May 1, 2006); *FTC v. Accusearch, Inc. d/b/a Abika.com*, No. 06-CV-0105 (D. Wyo. filed May 1, 2006); *FTC v. CEO Group, Inc. d/b/a Check Em Out*, No. 06-60602 (S.D. Fla. filed May 1, 2006); *FTC v. 77 Investigations, Inc.*, No. EDCV06-0439 VAP (C.D. Cal. filed May 1, 2006); *FTC v. Integrity Sec. & Investigation Servs., Inc.*, No. 2:06-CV-241-RGD-JEB (E.D. Va. filed May 1, 2006)).

40 *See, e.g., California v. Data Trace USA Inc.*, No. GIC862672 (Cal. Super. Ct. filed Mar. 14, 2006).

41 *See, e.g., Florida v. 1st Source Information Specialists, Inc.*, No. 37-2006-CA-00234 (Fla. Cir. Ct. filed Jan. 24, 2006); *Florida v. Global Information Group, Inc., et al.*, No. 06-1570 (Fla. Cir. Ct. filed Feb. 24, 2006).

42 *See, e.g., Illinois v. 1st Source Information Specialists, et al.*, No. 2006-CH-29 (Ill. Cir. Ct. filed Jan. 20, 2006); *see also* Press Release, *Office of the Attorney General, Madigan Sues Second Company that Sells Cell Phone Records* (Mar. 15, 2006), *available at* www.ag.state.il.us/pressroom/2006_03/20060315c.html (announcing the filing of a law suit against a Florida company that allegedly obtained and sold phone records without customer consent).

43 *See, e.g., Missouri v. Data Trace USA, Inc., et al.*, No. 06AC-CC-00158 (Mo. Cir. Ct. filed Mar. 3, 2006; *see also* Press Release, Missouri Attorney General's Office, *Locatecell.com must stop selling cell phone records of Missourians, under court order obtained by Nixon* (Feb. 15, 2006), *available at* www.ago.mo.gov/newsreleases/2006/021506.htm (announcing the issuance of a court order to stop the sale of Missourians' cell phone records by several people currently or formerly associated with the website Locatecell.com).

44 *See, e.g., Texas v. John Strange d/b/a USA Skiptrace.com*, No. 06-1666 (Tex. Dist. Ct. Travis County filed Feb. 9, 2006); *see also* Press Release, Attorney General of Texas, *Attorney General Abbott Files First Suit Against Sellers of Private Phone Records* (Feb. 9, 2006), *available at* http:// www.oag.state.tx.us/oagnews/release.php?id=1449.

45 "Call detail" or "call records" includes any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. *See, e.g., Third Report and Order*, 17 FCC Rcd at 14864, para. 7. Remaining minutes of use is an example of CPNI that is not call detail information. We disagree with commenters that argue we should adopt a more narrow definition of call detail; a narrower definition that included only inbound or outbound telephone numbers would make it too easy for unauthorized persons with partial information to confirm and expand on that information. *See, e.g.*, Letter from Jim Halpert, Counsel to the Anti-Pretexting Working Group, DLA Piper, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 Attach. at 2 (filed Oct. 31, 2006); Letter from William F. Maher, Jr., Counsel for T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Nov. 30, 2006); Letter from Charon Phillips, Verizon Wireless, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Dec. 1, 2006).

46 *See, e.g.*, Letter form Donna Epps, Vice President Federal Regulatory, Verizon, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 (filed Nov. 20, 2006) (arguing that any password requirement should only apply to accessing call detail information). By limiting our rules to the disclosure of call detail information, we believe that we have narrowly tailored our requirements to address the problem of pretexting. *See, e.g.*, AT&T Reply at 2 (arguing that the Commission should ensure that any measures taken are "narrowly tailored to address a demonstrated problem"); Letter from Donna Epps, Vice President, Federal Regulatory, Verizon, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at Attach. (filed Jan. 29, 2007) (Verizon Jan. 29, 2007 *Ex Parte Letter*) (stating that password protecting call detail records "is a narrowly tailored solution" that "directly targets the means and methods used by pretexters"). We also limit the requirements we impose in this section to customer-initiated contact with the carrier. We find that there is not the same need for authentication when the carrier initiates contact with a customer via the telephone number of record or via the address of record. By "telephone number of record," we mean the telephone number associated with the underlying service, rather than some other telephone number supplied as a customer's "contact information." By "address of record," whether postal or electronic, we mean an address that the carrier has associated with the customer's account for at least 30 days. Requiring that the address be on file for 30 days will foreclose a pretexter's ability to change an address of record for the purpose of being sent call detail information immediately.

47 We understand that many consumers may not like passwords and thus we only extend the use of password protection of call detail

information during customer-initiated telephone calls. *See, e.g.*, AT&T Comments at 8-11 (noting studies that demonstrate customers are opposed to mandatory passwords; Centennial Comments at 3-4 (arguing that customers find passwords burdensome). Further, for those customers not interested in password protection, we provide other alternatives for carrier disclosure of call detail information that directly advance our goal of protecting against pretexter activity and will not unduly burden carrier-customer relations.

48 This exception to the disclosure of call detail information in no way alters a carrier's usual practice of sending monthly billing statements to the customer.

49 *See supra* note 46 (defining "telephone number of record"). We find that it is necessary for the carrier to call the customer at the telephone number of record, rather than rely on caller ID as an authentication method, because pretexters can easily replicate caller ID numbers. *See, e.g.*, Alltel Comments at 5.

50 Although we do not enact password protection for non-call detail CPNI in this Order, carriers are still subject to section 222's duties to protect CPNI, and thus a carrier must authenticate a customer prior to disclosing non-call detail CPNI. *See* 47 U.S.C. § 222; *see also* Verizon Wireless Comments at 9 (arguing that "passcodes" can lead to a frustrating experience for customers seeking answers to simple billing questions). We rely on carriers to determine the authentication method for the release of non-call detail CPNI that is appropriate for the information sought and which adheres to section 222's duty. However, we seek comment on whether the Commission should impose password protection on non-call detail CPNI in today's Further Notice. *See infra* Section V.A.

51 *See, e.g.*, Alltel Comments at 5; Cingular Comments at 13; Dobson Comments at 2; Sprint Nextel Comments at 4-5; *see also* Testimony of James Rapp, House Energy and Commerce Committee, Subcommittee on Oversight and Investigations Hearing: "Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?" Attach. A (June 21, 2006) (setting forth an outline of a training manual on how to obtain call detail and other personal information), *available at* http://energycommerce.house.gov/108/Hearings/06212006hearing1916/Rapp.pdf; Brad Stone, *A 'Pretexter' and His Tricks: Phone Records Are a Snap to Snag. Just Ask David Gandal*, Newsweek, Sept. 10, 2006, at 43 (interviewing a pretexter who explains how pretexting is accomplished); *supra* para. 12 and accompanying notes (identifying lawsuits alleging pretexting activity).

52 Specifically, the Attorneys General state that data brokers consistently demonstrate that they can obtain almost any type of personal information, including social security numbers and mother's maiden name, which carriers currently use to authenticate a customer. *See, e.g.*, Attorneys General Comments at 15; *see also* EPIC *et al*. Comments at 12.

53 Customers requiring instant access to call detail information also have the option of accessing such data online in the protected manner described in Section IV.A.2, or by visiting a carrier's retail location with a valid photo ID as described in Section IV.A.3.

54 *See, e.g.*, Virgin Mobile Reply at 4 (mandating that customers select a password at the time of the service activation process). By "new customers," we include only those customers that establish service after the effective date of our rules.

55 "Readily available biographical information" includes such things as the customer's social security number, or the last four digits of that number; the customer's mother's maiden name; a home address; or a date of birth. *See, e.g.*, EPIC Petition at 8; *see also* AT&T Comments at 3 (noting that authenticating customers by relying "solely on a customer's name, address and/or phone number may be insufficient" and that the Commission could reasonably conclude "that all carriers should authenticate a customer's identity using non-public information prior to releasing CPNI"); *id*. at 7 (finding that authenticating the customer based on

non-public information would impose "little additional cost").

56 *See, e.g.*, EPIC Reply at 2. "Account information" includes such things as account number or any component thereof, the telephone number associated with the account, or amount of last bill.

57 A carrier could also use a Personal Identification Number (PIN) method to authenticate the customer. A PIN authentication method could entail a carrier supplying the customer with a randomly-generated PIN, not based on readily available biographical information, or account information, which the customer would then provide to the carrier prior to establishing a password. Carriers could supply the PIN to the customer by a carrier-originated voicemail or text message to the telephone number of record, or by sending it to an address of record so as to reasonably ensure that it is delivered to the intended party. *See, e.g.*, Letter from William F. Maher, Jr., Counsel for T-Mobile USA, Inc., Morrison & Foerster, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 2 (filed Nov. 20, 2006) (providing customers with a temporary password by sending it to the customer's mobile phone number). A carrier cannot authenticate a customer by sending the customer a PIN (or any other type of carrier chosen method of authentication) to new contact information that the customer provides at the time of the customer's PIN (or other authentication) request. Carriers could also authenticate the customer by requesting that the customer present a valid photo ID at a carrier's retail location. A "valid photo ID" is a government-issued personal identification with a photograph such as a current driver's license, passport, or comparable ID.

58 *See, e.g.*, Sprint Nextel Reply at 7 (noting that most carriers already allow customers to choose password protection); Letter from Donna Epps, Vice President, Federal Regulatory, Verizon, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 2 (filed Dec. 22, 2006) (Verizon Dec. 22, 2006 *Ex Parte* Letter) (noting that Verizon already permits its customers to password protect telephone account access).

59 We agree with commenters that assert that individuals tend to choose passwords that are based on personal information and therefore pretexters can easily circumvent password protections. *See, e.g.*, Verizon Wireless Comments at 9; Sprint Nextel Reply at 8. To prevent this, we prohibit carriers from using prompts to request the customer's password based on readily available biographical information, or account information. If a customer cannot provide the correct password and the carrier does not offer a back-up authentication method to access call detail, the carrier must reauthenticate the customer. A carrier cannot disclose call detail information over the telephone during a customer-initiated telephone call until the carrier is able to reauthenticate the customer without the use of readily available biographical information, or account information.

60 *See, e.g.*, Verizon Wireless Comments at 9.

61 *See, e.g.*, Letter from Cynthia R. Southworth, Director of the Safety Net Project, National Network to End Domestic Violence, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 2 (filed Nov. 30, 2006) (NNEDV Nov. 30, 2006 *Ex Parte* Letter). We do not require carriers to adopt a specific back-up authentication method because we believe that by directing carriers to do so we might make it easier for pretexters to defeat the protections we adopt in this Order. *See, e.g.*, Verizon Wireless Reply at 9. If a customer cannot provide the correct response to the back-up authentication method to access call detail, the carrier must reauthenticate the customer. A carrier cannot disclose call detail information over the telephone during a customer-initiated telephone call until the carrier is able to reauthenticate the customer without the use of readily available biographical information, or account information.

62 *See* Attorneys General Comments at 16; *see also* Ohio PUC Comments at 9-10. A shared secret is one or more question-answer combinations that are known to the customer and the carrier but are not widely known. Thus, if the customer lost or forgot a password, the carrier could provide the pre-selected shared secret question, or set of shared secret questions, to the customer for authentication purposes.

63 *See, e.g.*, Virgin Mobile Reply at 5 n.3 (allowing the customer to create their own back-up authentication question).

64 The customer may also access call detail information by establishing an online account or by visiting a carrier's retail location. *See infra* Sections IV.A.2 and IV.A.3.

65 *See, e.g.*, BellSouth Comments at 16 (noting the use of an optional customer-provided password for the release of CPNI over the telephone).

66 *See* Verizon Dec. 22, 2006 *Ex Parte* Letter at 5 (arguing that "any password requirement would have to be narrowly crafted to address the specific problem of pretexters fraudulently obtaining call detail information").

67 *See, e.g.*, Letter from Charon Phillips, Verizon Wireless, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Dec. 1, 2006) (raising concerns about a carrier's ability to serve customers during customer service calls).

68 *See, e.g.*, Letter from William F. Maher, Jr., Counsel for T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 2 (filed Nov. 20, 2006); Verizon Dec. 14, 2006 *Ex Parte* Letter at 2.

69 *See, e.g.*, Letter from John T. Scott, III, Vice President & Deputy General Counsel Regulatory Law, Verizon Wireless, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Oct. 18, 2006) (Verizon Wireless Oct. 16 *Ex Parte* Letter) (arguing that carriers should require passwords for online access to CPNI); Verizon Dec. 22, 2006 *Ex Parte* Letter at 2 (supporting a proposal to require password protection for customer online account access because passwords are "routine and readily accepted by customers" in the online environment). We do not limit our online account access rules to just call detail because online account access presents a heightened security risk. Specifically, online account access allows a customer (or pretexter) to view and change personal information easily (including online passwords, addresses of record, and billing information) without carrier assistance. During a telephone conversation with the customer, a carrier is able to authenticate a customer and sense whether the customer is who he claims to be. In the online context, however, there is no person-to-person contact (or limited interactive voice recognition menu) and thus a pretexter, if he were able to circumvent online password protection, could obtain significant amounts of a customer's private information (including home address, plan information, billing information, and call detail records for months at a time) with only the click of a mouse. Thus, we believe that we must extend our online account access rules to include the disclosure of all CPNI to protect customer privacy. Furthermore, most carriers already require password protection for online accounts. *See, e.g.*, Verizon Dec. 22, 2006 *Ex Parte* Letter at 2. They do not differentiate their online account systems between access to call detail information and non-call detail CPNI, and requiring them to do so likely would impose significant costs. For these reasons, we find that our requirements in the online context are no more extensive than necessary to protect consumers' privacy. *See Central Hudson Gas & Elec. Corp. v. Public Service Comm'n of N.Y.*, 447 U.S. 557, 564-65 (1980).

70 *See* 47 U.S.C. § 222(a) (stating that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers").

71 For instance, pretexters have been able to access CPNI by deceiving customer service representatives or by exploiting security gaps in customers' online accounts. *See, e.g.*, EPIC Petition, Appendix C (providing a list of 40 web sites offering to sell CPNI to third parties); Attorneys General Comments at 3 (describing pretexters' use of online account access).

72 *See, e.g.*, EPIC Petition at 8, 11; *see also supra* para. 12 and accompanying notes.

73 *See, e.g.*, EPIC Petition at 8. The record in this proceeding reveals other holes in carriers' existing authentication measures, such as authenticating a customer's identity through information the carrier readily provides to any person purporting to be the customer without authentication, thus enabling a pretexter to obtain online access to CPNI by first calling the carrier to obtain the information. The requirements we adopt in this Order fix such flaws.

74 *See, e.g.*, EPIC *et al*. Comments at 12-13 (explaining that biographical identifiers are widely available on websites and easily obtained by pretexters); Centennial Reply at 6 (stating that biographical information like social security number can be found on the Internet).

75 For new customers, a carrier could request that a customer establish an online password at the time of service initiation. *See supra* note 54. Alternatively, for all customers, a carrier could use a PIN method, as described above, to authenticate a customer if necessary. *See supra* note 56.

76 Although we do not mandate what specific level of password protection carriers must provide for their customers for online access, we expect carriers to ensure that online access to CPNI is adequately password protected. For example, we believe it would be reasonable for carriers to block access to a customer's account after repeated unsuccessful attempts to log in to that account to prevent hackers from using a so-called "brute force attack" to discover account passwords. Carriers may also determine the password format they deem appropriate. For example, carriers may decide the length of the password, whether or not the password should be case-sensitive, or whether the password should require a mix of numerals, letters, and other symbols.

77 *See supra* note 60.

78 *See supra* Section IV.A.1. For existing online accounts, although we do not mandate that a carrier reinitialize those accounts, if a carrier provides a back-up authentication method that is not in conformance with this Order (*i.e.*, the method is based on carrier prompts for readily available biographical information, or account information), then a carrier must modify its back-up authentication method to comply with this Order.

79 This requirement extends to all online accounts regardless of whether the online account access existed prior to the effective date of these rules.

80 A "valid photo ID" is a government-issued personal identification with a photograph such as a current driver's license, passport, or comparable ID.

81 *See, e.g.*, Cingular Comments at 18 (requiring a photo ID before providing a customer a print of the bill at a retail location).

82 *See* Attorneys General Comments at 16.

[83] A customer response to a carrier-designed back-up means of authentication is the customer's pre-selected answer to the carrier's back-up authentication method in the event that the customer lost or forgot his password.

[84] This notification process is not required when the customer initiates service, including the selection of a password at service initiation.

[85] *See* New Jersey Ratepayer Advocate Comments at 4; *see also* Alltel Comments at 5 (noting that notice of certain account changes may protect subscriber's security); Ohio PUC Comments at 10 (asserting that providing notice to customers of changed passwords is an effective strategy for protecting CPNI).

[86] *See, e.g.*, Verizon Dec. 22, 2006 *Ex Parte* Letter at 6 (arguing against a "one-size-fits-all" requirement for notifying customers of account changes on First Amendment grounds). To protect the security of the potential victim of pretexting, such notification must not reveal the changed account information. Additionally, a carrier may not notify the customer of account changes by sending notice to the new account information, which might result in the customer not being notified of the change (*e.g.*, mailing a customer's change of address to a new address rather than to the former address of record).

[87] *See, e.g.*, NCTA Comments at 6 (arguing that a carrier generally does not know when a data broker breaches carrier security measures because the carrier believes the data broker is the customer); TWTC Comments at 13 (stating that carriers usually are not aware when pretexting occurs); Cingular Reply at 7 n.17 (arguing that the customer is usually aware of a security problem before the carrier).

[88] *See, e.g.*, Letter from Donna Epps, Vice President and Federal Regulatory, Verizon, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 2 (filed Dec. 14, 2006) (Verizon Dec. 14, 2006 *Ex Parte* Letter).

[89] *See, e.g.*, TWTC Comments at 19-20; Letter from John J. Heitmann and Jennifer M. Kashatus, Counsel to XO Communications, to Marlene Dortch, Secretary, FCC, CC Docket No. 96-115, at 2 (filed Oct. 19, 2006); Letter from Karen Reidy, Vice President, Regulatory Affairs, COMPTEL, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Dec. 18, 2006) (COMPTEL Dec. 18, 2006 *Ex Parte* Letter).

[90] These business customers are able to reach customer service representatives without going through a call center. If the business customer must go through a call center to reach a customer service representative then this exemption does not apply to that customer.

[91] *See* EPIC *et al*. Comments at 15; *see also, e.g.*, CaPUC Comments at 3 (recommending the adoption of a rule that carriers notify a customer when the carrier discloses a customer's CPNI without customer consent); MetroPCS Comments at 9 (stating that it notifies a customer through a text message anytime that it releases CPNI); Verizon Wireless Oct. 18, 2006 *Ex Parte* Letter at 2 (arguing that customers should be aware if a carrier disclosed their data to a third party); NNEDV Nov. 30, 2006 *Ex Parte* Letter at 3 (arguing for a victim to be notified prior to law enforcement).

[92] *See* DOJ/DHS Comments at 14; Letter from Paul J. McNulty, Deputy Attorney General, United States Department of Justice, to Kevin J. Martin, Chairman, FCC, CC Docket No. 96-115 (filed Dec. 28, 2006) (DOJ Dec. 28, 2006 *Ex Parte* Letter); Letter from

Joseph E. Springsteen, Trial Attorney, United States Department of Justice, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 (filed Mar. 13, 2007).

93 *See* DOJ Dec. 28, 2006 *Ex Parte* Letter; *see also* Cal. Civ. Code § 1798.82 (permitting law enforcement to delay customer notification of breaches of security if a law enforcement agency determines the notification will impede a criminal investigation); N.Y. Gen. Bus. Law § 899-aa (permitting law enforcement to delay customer notification of breaches of security if a law enforcement agency determines the notification impedes a criminal investigation).

94 Section 201(b) authorizes the Commission to "prescribes such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act," including section 222. 47 U.S.C. § 201(b). Section 1 charges the Commission with "promoting safety of life and property through the use of wire and radio communication." 47 U.S.C. § 151.

95 The Commission will maintain a link to the reporting facility at www.fcc.gov/eb/cpni.

96 If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, the law enforcement agency may direct the carrier not to disclose the breach for an initial 30-day period. This 30-day period may be extended by the law enforcement agency as reasonably necessary in the judgment of the agency. The law enforcement agency shall provide in writing to the carrier its initial direction to the carrier and any subsequent direction.

97 A telecommunications carrier should indicate its desire to notify its customer or class of customers immediately concurrent with its notice to the USSS and FBI of a breach.

98 *See, e.g.*, Charter Comments at 7-9 (discussing how market forces give carriers incentive to protect CPNI); Time Warner Comments at 6 (noting that AOL has market incentives to protect its subscribers' personal information).

99 *See, e.g.*, Charter Comments at 8 (noting that recent studies demonstrate that nearly 60% of consumers either terminate service or consider switching service providers when a company fails to protect personally identifiable information); NASUCA Comments at 26 (arguing that the Commission should not rely alone on the "good business sense" of carriers to notify their customers of a security breach).

100 As EPIC states by way of example, such notice will "allow individuals to take actions to avoid stalking or domestic violence. . . . and also allow individuals to pursue private claims against the pretexter or person employing the pretexter." EPIC *et al*. Comments at 15.

101 *See* DOJ/DHS Comments at 14. In particular, a carrier is not required to notify the subject of a lawful investigation that law enforcement has sought or obtained access to the subject's telephone records, which could jeopardize the investigation. As the Department of Justice explains, Congress already has established a structure for customer notification of law enforcement access to customer records for providers of certain services, and by our action today we do not disturb the balance Congress has struck on this issue for such providers. *See id*. at 15-16 (citing 18 U.S.C. §§ 2701 *et seq*.).

102 47 U.S.C. § 222(d); *see also* 18 U.S.C. § 2702.

103 NASUCA urges carriers to provide individualized notice to customers in the event of a security breach because notice in a bill may not be read by the customer. *See* NASUCA Comments at 7-8.

104 *See, e.g.*, CTIA Comments at 6 (explaining that carriers must respond to a constantly evolving threat from pretexters who become more knowledgeable with every call to a carrier's customer service representatives).

105 For example, several carriers already voluntarily refuse to divulge call detail information directly over the telephone even with password protection. *See, e.g.*, Letter from Brian F. Fontes, Vice President, Federal Relations, Cingular Wireless LLC, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 (filed Sept. 29, 2006); Letter from William F. Maher, Jr., Counsel for T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 2 (filed Dec. 4, 2006).

106 Section 222(a) of the Act imposes a generally duty on carriers to "protect the confidentiality of proprietary information of, and relating to . . . customers." 47 U.S.C. § 222(a).

107 *See, e.g.*, Missouri PSC Comments at 3 (pointing out that audit trails are useful when tracking and prosecuting entities that obtain CPNI dishonestly or inappropriately); NCTA Comments at 4 (arguing that while audit trails do not deter pretexting, they can help carriers identify and investigate security breaches after they have occurred).

108 Moreover, as numerous commenters observe, publishing criteria for identifying suspect calls or calling patterns or online attempts at access would aid pretexters more than it would enhance security. *See, e.g.*, CTIA Comments at 3; T-Mobile Comments at 4; US Telecom Comments at 3-4 (arguing that overly-specific rules risk giving pretexters a "roadmap").

109 This expectation is reasonable given that the problem of pretexting emerged notwithstanding the Commission's current rules.

110 47 U.S.C. § 222(c); 47 C.F.R. § 64.2009.

111 *See infra* Section IV.I.

112 *See* Further Notice at paras. 69-70.

113 *See* EPIC Petition at 11.

114 *See, e.g.*, AT&T Comments at 15-16; Cingular Comments at 13; Verizon Wireless Comments at 11.

115 *See, e.g.*, Centennial Reply at 7.

116 Commenters report that the expense of encryption would be substantial, and would be of limited value in protecting against pretexting. *See, e.g.*, Verizon Wireless Comments at 11. Some carriers nevertheless may find that encryption currently is a cost-effective way to increase the security of CPNI. *See, e.g.*, Alltel Comments at 6 (noting that Alltel is encrypting some data stores to stop potential hackers). In addition, if carriers begin to experience increased attempts to obtain CPNI through hacking or similar measures, we would expect all carriers to revisit whether encryption of CPNI databases would satisfy their obligation to take reasonable steps to protect CPNI databases from unauthorized third-party access.

117 We do not believe that this minor change to our rules will have a major effect on carriers because many carriers already do not disclose CPNI to third parties. *See, e.g.*, CTIA Comments at 12 (noting that most wireless carriers do not disclose CPNI to third parties or use it outside of a total service approach); US Cellular Reply at 2 (stating that it does not share CPNI other than in accordance with the total service approach). Additionally, we note that this opt-in regime does not in any way affect a carrier's permitted use of CPNI enumerated in section 222(d). 47 U.S.C. § 222(d).

118 *See Third Report and Order*, 17 FCC Rcd at 14875-75, para. 33; *see also, e.g.*, Joint Commenters Comments at 16 (stating that they do not dispute that the Commission has a substantial interest in protecting privacy).

119 *See Notice*, 21 FCC Rcd at 1788, para. 12.

120 *See* 47 C.F.R. § 64.2007(b)(1); *see also, e.g.*, NASUCA Comments at 9 (arguing that with an opt-out policy "there is no assurance that any implied consent would be truly informed").

121 *See, e.g., supra* para. 12 and accompanying notes; Telephone Records and Privacy Protection Act of 2006, H.R. 4709, 109th Cong. (2d Sess. 2006).

122 *See, e.g., supra* para. 12 and accompanying notes.

123 47 C.F.R. § 64.2007(b)(2).

124 *See, e.g.*, MoPSC Comments at 4 (asserting that there is a lack of control over third-party recipients of CPNI).

125 *See* 47 U.S.C. § 222.

126 *See, e.g.*, EPIC *et al*. Comments at 7; MoPSC Comments at 5.

127 *See* Attorneys General Comments at 6 (noting studies surrounding Gramm-Leach-Bliley Act, including a study by Harris Interactive, Inc.); MoPSC Comments at 5 (noting that during the state's rulemaking on CPNI protections, it found that the concept of opt-out was not understandable to the average consumer).

128 *See, e.g.*, Attorneys General Comments at 6 (arguing that most customers are unlikely to read opt-out notices and therefore not know that they are giving affirmative consent to share their information); NASUCA Comments at 9 (believing that customers might not read CPNI notices and thus they are unaware that they might need to take affirmative action to prevent the sharing of their personal information).

129 *See, e.g.*, EPIC *et al*. Comments at 9-10 (pointing to a series of studies finding that consumers support opt-in privacy policies generally); NASUCA Comments at 9 (arguing that opt-in approval better protects a customer's privacy and gives the customer more control over the sharing of their personal information); Privacy Rights Comments at 4 (arguing that only opt-in consent provides adequate privacy protection).

130 *See, e.g.*, Alltel Comments at 3-4; AT&T Comments at 17-19; Cingular Comments at 14; CTIA Comments at 12; Joint Commenters Comments at 12; TWTC Comments at 16; Verizon Comments at 22-26; Verizon Wireless Comments at 10; DMA Reply at 1-2.

131 Attorneys General Comments at 7-9 (noting that there are over 152 major security breaches reported since February 2005 resulting in the loss of information to at least 54 million Americans).

132 *See* 47 U.S.C. § 222; *see also supra* note 121.

133 *See, e.g.*, Cingular Comments at 14; COMPTEL Comments at 4.

134 We note that while our enforcement actions may act as a deterrent to a carrier's unauthorized use of CPNI, they cannot undo the harm to a customer after a breach.

135 *See, e.g.*, BellSouth Comments at 26-27.

136 *Compare* Verizon Comments at 26 *with* 47 U.S.C. § 222.

137 We note that this minor modification to our rules does not affect the opt-out regime for intra-company use of CPNI beyond the total service approach, or the disclosure of CPNI to a carrier's agents or affiliates that provide communications-related services.

138 *Central Hudson*, 447 U.S. at 564-65. The *Central Hudson* test provides that if the commercial speech concerns lawful activity and is not misleading, the government may restrict the speech only if it (1) "has a substantial state interest in regulating the speech, (2)

the regulation directly and materially advances that interest, and (3) the regulation is no more extensive than necessary to serve the interest." *Central Hudson*, 447 U.S. at 564-65.

139 *See, e.g.*, BellSouth Comments at 27; Joint Commenters Comments at 14-16; TWTC Comments at 16-17; Verizon Comments at 23-25; Verizon Wireless Comments at 11-12; BellSouth Reply at 3-9; Charter Reply at 3-14; Verizon Reply at 2-8.

140 *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999).

141 *Id*. at 1237.

142 *See supra* para. 10 and accompanying notes; s*ee also, e.g.*, Attorneys General Comments at 1-4; NASUCA Reply at 12.

143 Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568, § 2(5) (2007).

144 *U.S. West, Inc. v. FCC*, 182 F.3d at 1239.

145 *See supra* para. 36 & nn.124-25.

146 Attorneys General Comments at 6.

147 *See also U.S. West, Inc. v. FCC*, 182 F.3d at 1236.

148 EPIC *et al*. Comments at 9. Moreover, Verizon contends that consumers have found "the mechanics of the opt-in regime . . . confusing" and have been reluctant to use opt-in, that is based on its experiences following the Commission's 2001 *Clarification Order*. *See* Verizon Jan. 29 *Ex Parte* Letter, Verses Decl. at para. 16. We note, however, that in the intervening years the use of opt-in approval methods appear to have become increasingly common, such as in the mobile wireless context, and thus we do not find Verizon's past experiences persuasive. *See, e.g., The Mobile Revolution Will Be Advertised*, Wireless Business Forecast, 2006 WLNR 4911016 (Mar. 23, 2006) (discussing the use of opt-in approval processes in mobile wireless marketing); Betsy Spethmann, *Next-Tech.*, Promo, 2005 WLNR 10551271 (July 1, 2005) (discussing the use of an opt-in approval process by Verizon Wireless).

149 *See* Verizon Jan. 29, 2007 *Ex Parte* Letter at 3; Letter from William Maher, Jr., Counsel for T-Mobile USA, Inc. to Marlene Dortch, Secretary, FCC, CC Docket No. 96-115 at 3 (filed Jan. 25, 2007) (T-Mobile Jan. 25 *Ex Parte* Letter); Letter from Kathryn Marie Krause, Qwest, to Marlene Dortch, Secretary, FCC, CC Docket No. 96-115 at 3 (filed Jan. 18, 2007) (Qwest Jan. 18, 2007 *Ex Parte* Letter).

150 *See* Verizon Jan. 29, 2007 *Ex Parte* Letter at 20-22; Letter from Kent Nakamura, Vice President and Chief Privacy Officer, Sprint Nextel, to Marlene Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Jan. 26, 2007) Sprint Nextel Jan. 26, 2007 *Ex Parte*

Letter); Letter from James Jenkins, Vice President, United States Cellular Corp., to Marlene Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Feb. 5, 2007); T-Mobile Jan. 25, 2007 *Ex Parte* Letter at 3; Qwest Jan. 18, 2007 *Ex Parte* Letter at 3; Letter from Anisa Latif, AT&T, to Marlene Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Jan. 17, 2007).

151 *See* Telephone Records and Privacy Protection Act of 2006, § 2; NASUCA Reply at 12.

152 *See* Attorneys General Comments at 3; EPIC Comments at 5; NASUCA Reply at 11.

153 EPIC Comments at 6.

154 *See, e.g.*, EPIC Comments at 6; NASUCA Reply at 15.

155 See Sprint Nextel Jan. 26, 2007 *Ex Parte* Letter at 1.

156 Verizon Jan. 29, 2007 *Ex Parte* Letter at 22, 26.

157 *See supra* paras. 11, 13-15, 18-20.

158 Verizon Jan. 29, 2007 *Ex Parte* Letter at 22, 26.

159 *See* 47 U.S.C. § 222(a); 47 C.F.R. § 64.2007(b)(3).

160 *See* 18 U.S.C. § 1039 (prohibiting the sale, transfer, purchase or receipt of "confidential phone records information" as defined in subsection (h)(1)).

161 *See* http://www.t-mobile.com/shop/plans/detail.aspx?id=9d4cbda1-c54e-496c-b11f-d8b6da5798b9 (describing a myFaves plan); http:// www.alltelcircle.com/about.php (comparing my circle plan to competitors offerings). Under these plans, the telephone numbers of favorite contacts are CPNI because they relate to the service to which the customer subscribes. *See* 47 U.S.C. § 222(h)(1)(A).

162 *See, e.g.*, Letter from Kent Nakamura, Vice President and Chief Privacy Officer, Sprint Nextel, to Marlene Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Jan. 22, 2007).

163 *See, e.g.*, NASUCA Reply at 20.

164 *See Notice*, 21 FCC Rcd at 1793, para. 29. By the term "any action," we mean that carriers should report on proceedings instituted or petitions filed by a carrier at either state commissions, the court system, or at the Commission against data brokers. For the summary of customer complaints, carriers must report on the number of customer complaints a carrier has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information. Additionally, carriers must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps carriers are taking to protect CPNI.

165 *See, e.g.*, AT&T Comments at 14 (noting that the Commission could "reasonably conclude" that carriers should annually filing their certifications with the Commission to enable the Commission to more effectively monitor CPNI security measures). For this reason, we disagree with commenters that believe that the certification should not be filed with the Commission. *See, e.g.*, RCA Comments at 5 (arguing that the annual filing of the certification with an explanation of the carrier's actions against data brokers and a summary of the CPNI-related consumer complaints is unjustified).

166 *See* 47 C.F.R. § 64.2009(e); *see also CPNI Order*, 13 FCC Rcd 8061, 8199, para. 201 (1998) (requiring the annual certification to be made publicly available). As a reminder, the existing rules require the certification to be executed by an officer of the carrier. The officer of the carrier must state in the certification that he or she has "personal knowledge" that the carrier has established procedures adequate to ensure compliance with the Commission's CPNI rules. Further, the carrier must also provide an accompanying statement explaining how the carrier's procedures ensure that the carrier is or is not in compliance with the requirements set forth in sections 64.2100 through 64.2900 of the Commission's rules. For example, the carrier may explain the training its employees receive regarding protection of CPNI, the disciplinary process applicable to improper disclosure of CPNI, the process used to ensure that opt-out elections are recorded and followed, and other measures relevant to demonstrating compliance with the CPNI rules. Finally, we remind carriers that the certification is required even if the carrier does not use CPNI for marketing purposes, as the obligation to protect CPNI from improper disclosure exists regardless of whether the carrier uses it for marketing purposes.

167 *See, e.g., Alltel Corporation Apparent Liability for Forfeiture*, Notice of Apparent Liability for Forfeiture, 21 FCC Rcd 746 (2006); *AT&T Inc. Apparent Liability for Forfeiture*, Notice of Apparent Liability for Forfeiture, 21 FCC Rcd 751 (2006); *Cbeyond Communications, LLC Apparent Liability for Forfeiture*, Notice of Apparent Liability for Forfeiture, 21 FCC Rcd 4316 (2006). Because carriers currently are required to make such a certification, requiring that this filing be made to the Commission will be minimally burdensome to the industry. *See, e.g.*, AT&T Comments at 14; Cingular Comments at 17; CTIA Comments at 2-3; Kim Comments at 11; OPASTCO Comments at 2, 8-9; Verizon Comments at 9; Verizon Wireless Comments at 19; MetroPCS Reply at 18. The additional information required by the expanded reporting obligation should not require carriers to make significant changes to their procedures, and some carriers report that they already keep track of CPNI-related complaints and actions taken against data brokers. *See, e.g.*, Kim Comments at 11; Phan Comments at 6; Verizon Comments at 9; Verizon Wireless Comments at 19. We disagree with commenters who assert that such a filing requirement will disadvantage small and regional carriers. We are equally concerned about the privacy of customers of small and regional carriers as we are about the privacy of customers of larger carriers and find that the benefits of customer privacy protection are significantly outweighed by a carrier's costs to implement these CPNI rules. *See, e.g.*, EWA Comments at 5; MetroPCS Reply at 18. We recognize carrier concerns about providing a roadmap for pretexters with this annual filing, and thus we will allow carriers to submit their certifications confidentially with the Commission. *See, e.g.*, AT&T Comments at 15; Cingular Comments at 16-17; CTIA Comments at 9-10; Phan Comments at 15. Carriers should supply the Commission with redacted and non-redacted versions of their filings. A carrier may only redact specific data about its actual security procedures and actual complaints in its filing. A carrier may not redact summary data about the number or type of customer complaints or other aggregate or general data because we believe it is in the public's interest to have access to such data when selecting a service provider. Members of the public will have the opportunity to review redacted filings and bring to the attention of the Commission any potential violations or concerns identified in those filings.

168 *See, e.g.*, Joint Commenters Reply at 9 (requesting a date certain for this annual filing for administrative convenience).

169 *See, e.g.*, AT&T Comments at 15; Cingular Comments at 17; T-Mobile Comments at 13; Verizon Comments at 9.

170 The Commission defines "interconnected VoIP service" as "a service that: (1) enables real-time, two-way voice communications; (2) requires a broadband connection from the user's location; (3) requires Internet protocol-compatible customer premises equipment (CPE); and (4) permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network." 47 C.F.R. § 9.3; *see also IP-Enabled Services; E911 Requirements for IP-Enabled Service Providers*, First Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 10245, 10257-57, para. 24 (2005) (*VoIP 911 Order*), *aff'd, Nuvio Corp. v. FCC*, No. 473 F.3d 302 (D.C. Cir. 2006). We emphasize that interconnected VoIP service offers the *capability* for users to receive calls from and terminate calls to the PSTN; the obligations we establish apply to all VoIP communications made using an interconnected VoIP service, even those that do not involve the PSTN. *See, e.g., VoIP 911 Order*, 20 FCC Rcd at 10257-58, para. 24. As we have in the past, we limit our extension of the rules to interconnected VoIP service providers because we continue to believe that consumers have a reasonable expectation that such services are replacements for "regular telephone" service. *See, e.g., id*. at 10256, para. 23; *see also* Internet Companies Comments at 22; Time Warner Comments at 13.

171 *See IP-Enabled Services Notice*, 19 FCC Rcd at 4910, para. 71; *EPIC CPNI Notice*, 21 FCC Rcd at 1793, para. 28.

172 *See* 47 U.S.C. § 153(20), (46) (defining "information service" and "telecommunications service").

173 *See, e.g., VoIP 911 Order*, 20 FCC Rcd at 10261-65, paras. 26-32. We therefore disagree with commenters that we do not have statutory authority to extend the CPNI requirements to interconnected VoIP service providers. *See, e.g.*, Charter Comments at 36-37; Internet Companies Comments at 17-22.

174 47 U.S.C. § 222.

175 *See United States v. Southwestern Cable Co.*, 392 U.S. 157, 177-78 (1968) (*Southwestern Cable*). *Southwestern Cable*, the lead case on the ancillary jurisdiction doctrine, upheld certain regulations applied to cable television systems at a time before the Commission had an express congressional grant of regulatory authority over that medium. *See id*. at 170-71. In *Midwest Video I*, the Supreme Court expanded upon its holding in *Southwestern Cable*. The plurality stated that "the critical question in this case is whether the Commission has reasonably determined that its origination rule will 'further the achievement of long-established regulatory goals in the field of television broadcasting by increasing the number of outlets for community self-expression and augmenting the public's choice of programs and types of services.'" *United States v. Midwest Video Corp.*, 406 U.S. 649, 667-68 (1972) (*Midwest Video I*) (quoting *Amendment of Part 74, Subpart K, of the Commission's Rules and Regulations Relative to Community Antenna Television Systems; and Inquiry into the Development of Communications Technology and Services to Formulate Regulatory Policy and Rulemaking and/or Legislative Proposals*, Docket No. 18397, First Report and Order, 20 FCC 2d 201, 202 (1969) (*CATV First Report and Order*)). The Court later restricted the scope of *Midwest Video I* by finding that if the basis for jurisdiction over cable is that the authority is ancillary to the regulation of broadcasting, the cable regulation cannot be antithetical to a basic regulatory parameter established for broadcast. *See FCC v. Midwest Video Corp.*, 440 U.S. 689, 700 (1979) (*Midwest Video II*); *see also American Library Ass'n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005) (holding that the Commission lacked authority to impose broadcast content redistribution rules on equipment manufacturers using ancillary jurisdiction because the equipment at issue was not subject to the Commission's subject matter jurisdiction over wire and radio communications).

176 *Southwestern Cable*, 392 U.S. at 178.

177 *See Universal Service Contribution Methodology; Federal-State Joint Board on Universal Service; 1998 Biennial Regulatory Review -- Streamlined Contributor Reporting Requirements Associated with Administration of Telecommunications Relay Service, North American Numbering Plan, Local Number Portability, and Universal Service Support Mechanisms; Telecommunications Services for Individuals with Hearing and Speech Disabilities, and the Americans with Disabilities Act of 1990; Administration of the North American Numbering Plan and North American Numbering Plan Cost Recovery Contribution Factor and Fund Size; Number Resource Optimization; Telephone Number Portability; Truth-in-Billing and Billing Format; IP-Enabled Services*, Report and Order and Notice of Proposed Rulemaking, 21 FCC Rcd 7518, 7542, para. 47 (2006) (*Interim USF Order*), *appeal pending, Vonage Holdings Corp. v. FCC*, No. 06-1276 (D.C. Cir. filed July 18, 2006); *VoIP 911 Order*, 20 FCC Rcd at 10261-62, para. 28 ("[I]nterconnected VoIP services are covered by the statutory definitions of 'wire communication' and/or 'radio communication' because they involve 'transmission of [voice] by aid of wire, cable, or other like connection . . .' and/or 'transmission by radio . . .' of voice. Therefore, these services come within the scope of the Commission's subject matter jurisdiction granted in section 2(a) of the Act."). This determination was not challenged in the appeal of the *VoIP 911 Order*. *See supra* note 170.

178 47 U.S.C. § 222(a), (c)(1); *see also* 47 C.F.R. § 64.2001 *et seq*.

179 *See Interim USF Order*, 21 FCC Rcd at 7542-43, para. 48 (citing *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989, 15009-10, para. 42 (2005), *aff'd, American Council on Education v. FCC*, 451 F.3d 226 (D.C. Cir. 2006)); *see also* Attorneys General Comments at 11 (arguing that VoIP customers have the same privacy concerns as wireline and wireless customers).

180 To be clear, a service offering is "interconnected VoIP" if it offers the *capability* for users to receive calls from and terminate calls to the PSTN regardless of whether access to the PSTN is directly through the interconnected VoIP provider or through arrangements with a third party.

181 47 U.S.C. § 151 (emphasis added).

182 *See* 47 U.S.C. § 222; EPIC Petition at 5-10.

183 *Southwestern Cable*, 392 U.S. at 178.

184 *Midwest Video I*, 406 U.S. at 667-68 (quoting *CATV First Report and Order*, 20 FCC 2d at 202).

185 *See, e.g.*, AARP Comments at 2 (WC Docket No. 04-36); Arizona Commission Comments at 15-16 (WC Docket No. 04-36); California PSC Comments at 14 (WC Docket No. 04-36); CenturyTel Comments at 22-23 (WC Docket No. 04-36); CWA Comments at 23 (WC Docket No. 04-36); Missouri PSC Comments at 21 (WC Docket No. 04-36); NCL Comments at 5 (WC Docket No. 04-36); New Jersey Ratepayer Advocate Comments at 39-43 (WC Docket No. 04-36); New York Attorney General Comments at 10-11 (WC Docket No. 04-36); Ohio PUC Comments at 37-38 (WC Docket No. 04-36); Rural Carriers Comments at 7-8 (WC Docket No. 04-36); Texas Attorney General Comments at 20-21 (WC Docket No. 04-36); Time Warner Comments at 31-32 (WC Docket No. 04-36); DOJ Comments at 17-20 (WC Docket No. 04-36); APT Reply at 8-9 (WC Docket No. 04-36). We disagree with commenters that argue there is no clear justification for CPNI protections, including because there is sufficient competition for such services. *See, e.g.*, 8x8 Comments at 29 (WC Docket No. 04-36); AT&T Comments at 41 (WC Docket No. 04-36); SBC Comments at 124-25 (WC Docket No. 04-36); ALTS Reply at 1-2 (WC Docket No. 04-36). We find on the contrary that the continuing trend toward customer use of these services as a replacement for analog voice services in large measure justifies

the extension of our rules to these services to protect consumer privacy.

186 47 U.S.C. § 157 nt.

187 *See Availability of Advanced Telecommunications Capability in the United States*, Fourth Report to Congress, 20 FCC Rcd 20540, 20578 (2004) ("[S]ubscribership to broadband services will increase in the future as new applications that require broadband access, *such as VoIP*, are introduced into the marketplace, and consumers become more aware of such applications.") (emphasis added).

188 We do not believe that our actions today are in conflict or otherwise inconsistent with any provision of the Act. We acknowledge that section 230 of the Act provides that "[i]t is the policy of the United States -- to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." 47 U.S.C. § 230(b)(2). We do not believe, however, that this congressional policy statement precludes us from extending the CPNI obligations to interconnected VoIP service providers here. We note that the Commission's discussion of section 230 in the *Vonage Order* as cautioning against regulation was limited to "traditional common carrier economic regulations." *Vonage Holdings Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission*, Memorandum Opinion and Order, 19 FCC Rcd 22404, 22426, para. 35 (2004) (*Vonage Order*), *appeal pending, National Ass'n of State Util. Consumer Advocates v. FCC*, No. 05-71238 (9th Cir. filed Feb. 22, 2005).

189 *See, e.g.*, Centennial Comments at 5-6; USISPA Comments at 7; Verizon Wireless Comments at 14-16; Charter Reply at 20-21.

190 *See, e.g.*, Ohio PUC Comments at 32; PaPUC Comments at 3-4; NASUCA Reply at 28-30.

191 *See, e.g.*, Letter from Richard T. Ellis, Director -- Federal Regulatory Advocacy, Verizon, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 (filed Feb. 6, 2004) (Verizon Feb. 6 *Ex Parte* Letter) (expressing concern regarding state regulations of CPNI that are inconsistent with federal CPNI rules and citing the rules of California, Oregon and Washington). Verizon has not asked the Commission specifically to rule on whether those states' CPNI regulations should be preempted, and apparently obtained the preemption it sought regarding the Washington CPNI regulations from a U.S. District Court in Washington. *See id.*, Attach.; *see also* Ariz. Rev. Stat. § 40-202(C)(5) (conferring authority on the Arizona Corporation Commission to adopt rules that "customer information, account information and related proprietary information are confidential unless specifically waived by the customer in writing").

192 *See, e.g.*, Dobson Reply at 6; Verizon Wireless Reply at 13-14. The Commission reviews petitions for preemption of CPNI rules on a case-by-case basis. *See Third Report and Order*, 17 FCC Rcd at 14890-93, paras. 69, 74 ("By reviewing requests for preemption on a case-by-case basis, we will be able to make preemption decisions based on the factual circumstances as they exist at the time and on a full and a complete record."). Verizon and AT&T Wireless Services filed petitions for reconsideration of the *Third Report and Order* regarding preemption of state CPNI regulation. *See* Verizon Petition for Reconsideration (filed Oct. 21, 2002); AT&T Wireless Services, Inc. Petition for Reconsideration (filed Oct. 21, 2002). This Order does not constitute a decision on the merits of those petitions.

193 *See, e.g.*, Ellen Nakashima, *HP Scandal Shines Light on a Simple, Treacherous Act*, Wash. Post, Sept. 19, 2006, D1. Carriers of course may begin instituting our rules earlier to protect their customers' CPNI.

194 *See* 47 C.F.R. § 1.427(b). For this reason, we reject requests for longer implementation periods. *See, e.g.*, Letter from Kent Y. Nakamura, Vice President and Chief Privacy Officer, Sprint Nextel Corporation, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 2 (filed Dec. 11, 2006); Letter from Donna Epps, Vice President Federal Regulatory, Verizon, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 1-4 (filed Dec. 22, 2006); Letter from Anisa A. Latif, Associate Director Federal Regulatory, AT&T, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Jan. 10, 2007); Letter from Indra Sehdev Chalk, Counsel for USTelecom, to Marlene Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Jan. 18, 2007); Letter from William F. Maher, Counsel for T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 4 (filed Jan. 25, 2007).

195 While the recent passage of the Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039, which imposes new criminal penalties against pretexters, should reduce pretexting, we believe that our Order today is necessary to protect customer privacy and help bring an end to the unauthorized access to CPNI. We disagree with commenters that argue that we should allow the law to take effect and reassess the situation later because the actions we take today go beyond the legislation to ensure the privacy of CPNI by focusing on carriers that have not vigilantly discharged their obligations under section 222 to adequately protect CPNI. *See, e.g.*, Dobson Comments at 3; COMPTEL Dec. 18, 2006 *Ex Parte* Letter at 1.

196 The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." 5 U.S.C. § 601(6). The term "small business" has the same meaning as the term "small business concern" under the Small Business Act. 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such terms which are appropriate to the activities of the agency and publishes such definitions(s) in the Federal Register."

197 We find this implementation period is reasonable for small carriers to avoid disruption and inconvenience to consumers.

198 *See* 47 U.S.C. § 222(a).

199 *See, e.g.*, Cingular Comments at 31-33 (stating that the Commission should follow FTC Safeguards Rule issued pursuant to Section 501(b) of Gramm Leach Bliley Act (15 U.S.C. §6801(b)), and should offer safe harbor inducement to follow standards); Qwest Comments at 2-3 (arguing in favor of safe harbor procedures); AT&T Comments at n.7 (arguing that carriers with good personnel training, audit trails, and adequate customer authentication procedures should enjoy a safe harbor).

200 *See, e.g.*, CTIA Comments at 13 (supporting a safe harbor for carriers that disclose account information to any person who provides a correct password); Qwest Comments at 2-3 (urging the Commission to find that carriers are already subject to the right balance of CPNI regulatory oversight, or alternatively pronounce guidelines that would frame a safe harbor for a carrier incorporating those guidelines into its operating practices).

201 *See, e.g.*, Centennial Reply at 4; CTIA Comments at 14 (stating that even in the case of pretexting, the customer service representatives' annotations would note that CPNI was given out at the customer's request).

202 *See, e.g.*, Charter Comments at 36; Dobson Comments at 6; OPATSCO Comments at 4; TWTC Comments at 14; Verizon Comments at 13. We note that the Commission in the *1999 Reconsideration Order* previously weighed the costs and benefits of establishing audit trails and decided not to require audit trails. *See 1999 Reconsideration Order*, 13 FCC Rcd at 8101-02, para. 126.

203 Commenters may request confidential treatment for the information that they submit in response to this Further Notice if they are concerned about compromising their physical safeguard measures. *See* 47 C.F.R. § 0.459.

204 *See* DOJ/DHS Comments at 3 (stating that CPNI is an invaluable investigative resource, the mandatory destruction of which would severely impact the DOJ/DHS's ability to protect national security and public safety).

205 *See, e.g.*, 47 C.F.R. § 42.6 (requiring that carriers retain telephone toll records for 18 months), § 42.7 (establishing record retention requirements for documents on a carrier's master index of records, and for documents relevant to complaint proceedings and certain Commission inquiries and proceedings).

206 *See* Cingular Comments at 25-26 (reporting that Cingular's experience is that most data brokers are focusing on the last 100 calls made or calls within the last 90 days).

207 *See, e.g.*, EPIC Petition at 11-12 (suggesting that carriers should "de-identify" records, that is, separate data that identify a particular caller from the general transaction records); *but see, e.g.*, Ohio PUC Comments at 17-18 (arguing that de-identifying records would frustrate customer's ability to dispute billing).

208 *See* Letter from Governor Rod R. Blagojevich, Governor of Illinois, to Deborah Platt Majoras, Chairperson, Federal Trade Commission, and Kevin J. Martin, Chairman, Federal Communications Commission (dated Sept. 5, 2006); *see also* Ted Brindis, *Secrets Linger on Old Cell Phones*, Houston Chronicle.com (Aug. 31, 2006) (reporting that someone was able to retrieve a company's plans regarding a multi-million dollar federal transportation contract, bank account information, and passwords from discarded mobile devices).

209 Cell phones may be refurbished and provided to a different customer as a replacement for a cell phone that has malfunctioned. The original customer's private information may remain on the cell phone. *See* Andrew Brandt, *Privacy Watch: Wipe Your Cell Phone's Memory Before Giving It Away*, PC World, *available at* http://www.pcworld.com/printable/articl/id,124157/printable.html (Jan. 30, 2006).

210 47 C.F.R. §§ 1.200 *et seq*.

211 *See* 47 C.F.R. § 1.1206(b)(2).

212 47 C.F.R. § 1.1206(b).

213 47 C.F.R. §§ 1.415, 1.419.

214 *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. §§ 601-12, has been amended by the Small Business Regulatory Enforcement Fairness

Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

215 *See EPIC CPNI Notice*, 21 FCC Rcd at 1794, para. 31 & Appendix B; *IP-Enabled Services Notice*, 19 FCC Rcd at 4917, para. 91 & Appendix A.

216 *See EPIC CPNI Notice*, 21 FCC Rcd at 1794, para. 31 & Appendix B; *IP-Enabled Services Notice*, 19 FCC Rcd at 4917, para. 91 & Appendix A.

217 *See* 5 U.S.C. § 604.

218 *See* Alexicon Comments at 1-9; NTCA Comments at 1-5; OPASTCO Comments at 1-9.

219 *See* Alexicon Comments at 7.

220 *See* Alexicon Comments at 2, n.6.

221 *See, e.g.*, NTCA Comments at 3-4; OPASTCO Comments at 2-7.

222 *See, e.g.*, NTCA Comments at 4.

223 *See* Order at paras. 13-22.

224 *See, e.g.*, Alexicon Comments at 8; NTCA Comments at 3.

225 *See* Order at para. 61.

226 *See* SBA Comments; Menard Comments; Menard Reply.

227 *See* SBA Comments at 2, 4, 6; Menard Comments; Menard Reply at 4.

228 The *IP-Enabled Services Notice* specifically sought comment on whether the CPNI requirements should apply to any provider of interconnected VoIP service, and the Commission published a summary of that notice in the Federal Register. *See IP-Enabled Services Notice*, 19 FCC Rcd at 4910, para. 71; *Regulatory Requirements for IP-Enabled Services*, WC Docket No. 04-36, Notice of Proposed Rulemaking, 69 Fed. Reg. 16193-01 (Mar. 29, 2004). We note that a number of small entities submitted comments in

this proceeding. *See supra* Appendix A.

229 *See* Order at para. 61.

230 5 U.S.C. §§ 603(b)(3), 604(a)(3).

231 5 U.S.C. § 601(6).

232 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such terms which are appropriate to the activities of the agency and publishes such definitions(s) in the Federal Register."

233 15 U.S.C. § 632.

234 *See* SBA, Programs and Services, SBA Pamphlet No. CO-0028, at page 40 (July 2002).

235 Independent Sector, The New Nonprofit Almanac & Desk Reference (2002).

236 5 U.S.C. § 601(5).

237 U.S. Census Bureau, Statistical Abstract of the United States: 2006, Section 8, page 272, Table 415.

238 We assume that the villages, school districts, and special districts are small, and total 48,558. *See* U.S. Census Bureau, Statistical Abstract of the United States: 2006, section 8, page 273, Table 417. For 2002, Census Bureau data indicate that the total number of county, municipal, and township governments nationwide was 38,967, of which 35,819 were small. *Id*.

239 15 U.S.C. § 632.

240 Letter from Jere W. Glover, Chief Counsel for Advocacy, SBA, to William E. Kennard, Chairman, FCC (May 27, 1999). The Small Business Act contains a definition of "small-business concern," which the RFA incorporates into its own definition of "small business." *See* 15 U.S.C. § 632(a) (Small Business Act); 5 U.S.C. § 601(3) (RFA). SBA regulations interpret "small business concern" to include the concept of dominance on a national basis. *See* 13 C.F.R. § 121.102(b).

241 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

242 FCC, Wireline Competition Bureau, Industry Analysis and Technology Division, "Trends in Telephone Service" at Table 5.3, page 5-5 (April 2005) ("Trends in Telephone Service"). This source uses data that are current as of October 1, 2004.

243 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

244 "Trends in Telephone Service" at Table 5.3.

245 13 C.F.R. § 121.201, NAICS code 517310 (changed from 513330 in Oct. 2002).

246 "Trends in Telephone Service" at Table 5.3.

247 13 C.F.R. § 121.201, NAICS code 517310 (changed from 513330 in Oct. 2002).

248 "Trends in Telephone Service" at Table 5.3.

249 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

250 "Trends in Telephone Service" at Table 5.3.

251 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

252 "Trends in Telephone Service" at Table 5.3.

253 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

254 "Trends in Telephone Service" at Table 5.3.

255 13 C.F.R. § 121.201, NAICS code 517310 (changed from 513330 in Oct. 2002).

256 "Trends in Telephone Service" at Table 5.3.

257 We include all toll-free number subscribers in this category, including those for 888 numbers.

258 13 C.F.R. § 121.201, NAICS code 517310 (changed from 513330 in Oct. 2002).

259 *See* FCC, Common Carrier Bureau, Industry Analysis Division, *Study on Telephone Trends*, Tables 21.2, 21.3, and 21.4 (Feb. 1999).

260 13 C.F.R. § 121.201, NAICS codes 517410 and 517910.

261 U.S. Census Bureau, "2002 NAICS Definitions: 517410 Satellite Telecommunications" (www.census.gov, visited Feb. 2006).

262 U.S. Census Bureau, 2002 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 517410 (issued Nov. 2005).

263 *Id*. An additional 38 firms had annual receipts of $25 million or more.

264 U.S. Census Bureau, "2002 NAICS Definitions: 517910 Other Telecommunications" (www.census.gov, visited Feb. 2006).

265 U.S. Census Bureau, 2002 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 517910 (issued Nov. 2005).

266 *Id*. An additional 14 firms had annual receipts of $25 million or more.

267 13 C.F.R. § 121.201, NAICS code 513321 (changed to 517211 in October 2002).

268 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

269 U.S. Census Bureau, 2002 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms for the United States: 2002, NAICS code 517211 (issued November 2005).

270 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer

employees; the largest category provided is firms with "1000 employees or more."

271 U.S. Census Bureau, 2002 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms for the United States: 2002, NAICS code 517212 (issued November 2005).

272 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is firms with "1000 employees or more."

273 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

274 U.S. Census Bureau, 2002 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms for the United States: 2002, NAICS code 517212 (issued November 2005).

275 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is firms with "1000 employees or more."

276 "Trends in Telephone Service" at Table 5.3.

277 *Id*.

278 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

279 U.S. Census Bureau, 2002 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms for the United States: 2002, NAICS code 517211 (issued November 2005).

280 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is firms with "1000 employees or more."

281 *Amendment of Part 90 of the Commission's Rules to Provide for the Use of the 220-222 MHz Band by the Private Land Mobile Radio Service*, PR Docket No. 89-552, Third Report and Order and Fifth Notice of Proposed Rulemaking, 12 FCC Rcd 10943, 11068-70, paras. 291-295, 62 FR 16004 (Apr. 3, 1997).

282 *See* Letter to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC, from A. Alvarez, Administrator, SBA (Dec. 2, 1998) (SBA Dec. 2, 1998 Letter).

283 *Revision of Part 22 and Part 90 of the Commission's Rules to Facilitate Future Development of Paging Systems*, Memorandum Opinion and Order on Reconsideration and Third Report and Order, 14 FCC Rcd 10030, paras. 98-107 (1999).

284 *Id*. at 10085, para. 98.

285 "Trends in Telephone Service" at Table 5.3.

286 *Id*.

287 SBA Dec. 2, 1998 letter.

288 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

289 *Id*.

290 "Trends in Telephone Service" at Table 5.3.

291 *See Amendment of Parts 20 and 24 of the Commission's Rules -- Broadband PCS Competitive Bidding and the Commercial Mobile Radio Service Spectrum Cap*, WT Docket No. 96-59, Report and Order, 11 FCC Rcd 7824, 61 FR 33859 (July 1, 1996) (*PCS Order*); *see also* 47 C.F.R. § 24.720(b).

292 *See PCS Order*, 11 FCC Rcd 7824.

293 *See, e.g., Implementation of Section 309(j) of the Communications Act -- Competitive Bidding*, PP Docket No. 93-253, Fifth Report and Order, 9 FCC Rcd 5332, 59 FR 37566 (July 22, 1994).

294 FCC News, Broadband PCS, D, E and F Block Auction Closes, No. 71744 (rel. Jan. 14, 1997); *see also Amendment of the Commission's Rules Regarding Installment Payment Financing for Personal Communications Services (PCS) Licenses*, WT Docket No. 97-82, Second Report and Order, 12 FCC Rcd 16436, 62 FR 55348 (Oct. 24, 1997).

295 *Amendment of the Commission's Rules to Establish New Personal Communications Services, Narrowband PCS*, Docket No. ET 92-100, Docket No. PP 93-253, Second Report and Order and Second Further Notice of Proposed Rulemaking, 15 FCC Rcd 10456, 65 FR 35875 (June 6, 2000).

296 *See* SBA Dec. 2, 1998 Letter.

297 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

298 U.S. Census Bureau, 1997 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms Subject to Federal Income Tax: 1997, NAICS code 513322 (issued October 2000).

299 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is "Firms with 1000 employees or more."

300 *See* U.S. Census Bureau, 2002 Economic Census, Industry Series: "Information," Table 2, Comparative Statistics for the United States (1997 NAICS Basis): 2002 and 1997, NAICS code 513322 (issued Nov. 2004). The preliminary data indicate that the total number of "establishments" increased from 2,959 to 9,511. In this context, the number of establishments is a less helpful indicator of small business prevalence than is the number of "firms," because the latter number takes into account the concept of common ownership or control. The more helpful 2002 census data on firms, including employment and receipts numbers, will be issued in late 2005.

301 *220 MHz Third Report and Order*, 12 FCC Rcd 10943, 11068-70, paras. 291-295 (1997).

302 *Id*. at 11068, para. 291.

303 *See* Letter to D. Phythyon, Chief, Wireless Telecommunications Bureau, Federal Communications Commission, from A. Alvarez, Administrator, Small Business Administration (Jan. 6, 1998).

304 *See generally* Public Notice, "220 MHz Service Auction Closes," 14 FCC Rcd 605 (1998).

305 *See, e.g.*, Public Notice, "FCC Announces It is Prepared to Grant 654 Phase II 220 MHz Licenses After Final Payment is Made," 14 FCC Rcd 1085 (1999).

306 Public Notice, "Phase II 220 MHz Service Spectrum Auction Closes," 14 FCC Rcd 11218 (1999).

307 47 C.F.R. § 90.814(b)(1).

308 *See Service Rules for the 746-764 MHz Bands, and Revisions to part 27 of the Commission's Rules*, WT Docket No. 99-168, Second Report and Order, 65 FR 17599 (Apr. 4, 2000).

309 *See generally* Public Notice, "220 MHz Service Auction Closes," Report No. WT 98-36 (Oct. 23, 1998).

310 Public Notice, "700 MHz Guard Band Auction Closes," DA 01-478 (rel. Feb. 22, 2001).

311 The service is defined in section 22.99 of the Commission's Rules, 47 C.F.R. § 22.99.

312 BETRS is defined in sections 22.757 and 22.759 of the Commission's Rules, 47 C.F.R. §§ 22.757 and 22.759.

313 13 C.F.R. § 121.201, NAICS code 517212.

314 The service is defined in section 22.99 of the Commission's Rules, 47 C.F.R. § 22.99.

315 13 C.F.R. § 121.201, NAICS codes 517212.

316 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

317 *Amendment of the Commission's Rules Concerning Maritime Communications*, PR Docket No. 92-257, Third Report and Order and Memorandum Opinion and Order, 13 FCC Rcd 19853 (1998).

318 This service is governed by Subpart I of Part 22 of the Commission's rules. *See* 47 C.F.R. §§ 22.1001-22.1037.

319 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

320 *Id*.

321 *See Amendment of the Commission's Rules Regarding the 37.0-38.6 GHz and 38.6-40.0 GHz Bands*, ET Docket No. 95-183, Report and Order, 63 Fed. Reg. 6079 (Feb. 6, 1998).

322 *Id*.

323 *See* Letter to Kathleen O'Brien Ham, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC,

from Aida Alvarez, Administrator, SBA (Feb. 4, 1998).

324 *Amendment of Parts 21 and 74 of the Commission's Rules with Regard to Filing Procedures in the Multipoint Distribution Service and in the Instructional Television Fixed Service and Implementation of Section 309(j) of the Communications Act -- Competitive Bidding*, MM Docket No. 94-131 and PP Docket No. 93-253, Report and Order, 10 FCC Rcd 9589, 9593, para. 7 (1995).

325 47 C.F.R. § 21.961(b)(1).

326 13 C.F.R. § 121.201, NAICS code 513220 (changed to 517510 in October 2002).

327 U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)", Table 4, NAICS code 513220 (issued October 2000).

328 In addition, the term "small entity" within SBREFA applies to small organizations (nonprofits) and to small governmental jurisdictions (cities, counties, towns, townships, villages, school districts, and special districts with populations of less than 50,000). 5 U.S.C. §§ 601(4)-(6). We do not collect annual revenue data on ITFS licensees.

329 *See Local Multipoint Distribution Service*, Second Report and Order, 12 FCC Rcd 12545 (1997).

330 *Id*.

331 *See id*.

332 *See* Letter to Dan Phythyon, Chief, Wireless Telecommunications Bureau, FCC, from Aida Alvarez, Administrator, SBA (Jan. 6, 1998).

333 *Implementation of Section 309(j) of the Communications Act -- Competitive Bidding*, PP Docket No. 93-253, Fourth Report and Order, 59 Fed. Reg. 24947 (May 13, 1994).

334 *Amendment of Part 95 of the Commission's Rules to Provide Regulatory Flexibility in the 218-219 MHz Service*, WT Docket No. 98-169, Report and Order and Memorandum Opinion and Order, 64 Fed. Reg. 59656 (Nov. 3, 1999).

335 *Amendment of Part 95 of the Commission's Rules to Provide Regulatory Flexibility in the 218-219 MHz Service*, WT Docket No. 98-169, Report and Order and Memorandum Opinion and Order, 64 Fed. Reg. 59656 (Nov. 3, 1999).

336 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

337 U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Employment Size of Firms Subject to Federal Income Tax: 1997," Table 5, NAICS code 513322 (issued Oct. 2000).

338 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is "Firms with 1,000 employees or more."

339 Teligent acquired the DEMS licenses of FirstMark, the only licensee other than TRW in the 24 GHz band whose license has been modified to require relocation to the 24 GHz band.

340 *Amendments to Parts 1,2, 87 and 101 of the Commission's Rules to License Fixed Services at 24 GHz*, Report and Order, 15 FCC Rcd 16934, 16967 (2000); *see also* 47 C.F.R. § 101.538(a)(2).

341 *Amendments to Parts 1,2, 87 and 101 of the Commission's Rules to License Fixed Services at 24 GHz*, Report and Order, 15 FCC Rcd 16934, 16967 (2000); *see also* 47 C.F.R. § 101.538(a)(1).

342 *See* Letter to Margaret W. Wiener, Deputy Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC, from Gary M. Jackson, Assistant Administrator, SBA (July 28, 2000).

343 13 C.F.R. § 121.201, North American Industry Classification System (NAICS) code 513220 (changed to 517510 in October 2002).

344 U.S. Census Bureau, 2002 Economic Census, Subject Series: Information, Table 4, Receipts Size of Firms for the United States: 2002, NAICS code 517510 (issued November 2005).

345 *Id*. An additional 61 firms had annual receipts of $25 million or more.

346 47 C.F.R. § 76.901(e). The Commission determined that this size standard equates approximately to a size standard of $100 million or less in annual revenues. *Implementation of Sections of the 1992 Cable Act: Rate Regulation,* Sixth Report and Order and Eleventh Order on Reconsideration, 10 FCC Rcd 7393, 7408 (1995).

347 47 C.F.R. § 76.901(c).

348 47 U.S.C. § 543(m)(2); *see* 47 C.F.R. § 76.901(f) & nn. 1-3.

349 *See* Public Notice, *FCC Announces New Subscriber Count for the Definition of Small Cable Operator*, DA 01-158 (Cable Services Bureau, Jan. 24, 2001).

350 47 C.F.R. § 76.901(f).

351 The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(f) of the Commission's rules. *See* 47 C.F.R. § 76.909(b).

352 *See* 47 U.S.C. § 573.

353 13 C.F.R. § 121.201, NAICS code 513220 (changed to 517510 in October 2002).

354 *See* < http://www.fcc.gov/csb/ovs/csovscer.html> (current as of March 2002).

355 U.S. Census Bureau, "2002 NAICS Definitions: 518111 Internet Service Providers" (Feb. 2004) <www.census.gov>.

356 13 C.F.R. § 121.201, NAICS code 518111 (changed from previous code 514191, "On-Line Information Services," in Oct. 2002).

357 U.S. Census Bureau, 2002 Economic Census, Subject Series: Information, Table 4, Receipts Size of Firms for the United States: 2002, NAICS code 518111 (issued November 2005).

358 *Id*. An additional 45 firms had annual receipts of $25 million or more.

359 U.S. Census Bureau, "2002 NAICS Definitions: 518112 Web Search Portals" (Feb. 2004) <www.census.gov>.

360 13 C.F.R. § 121.201, NAICS code 518112 (changed from 514199 in Oct. 2002).

361 U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 514199 (issued Oct. 2000). This category was created for the 2002 Economic Census by taking a portion of the superseded 1997 category, "All Other Information Services," NAICS code 514199. The data cited in the text above are derived from the superseded category.

362 U.S. Census Bureau, "2002 NAICS Definitions: 518210 Data Processing, Hosting, and Related Services" (Feb. 2004)

<www.census.gov>.

363 13 C.F.R. § 121.201, NAICS code 518210 (changed from 514210 in Oct. 2002).

364 U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 514210 (issued Oct. 2000).

365 U.S. Census Bureau, "2002 NAICS Definitions: 519190 All Other Information Services" (Feb. 2004) <www.census.gov>.

366 13 C.F.R. § 121.201, NAICS code 519190 (changed from 514199 in Oct. 2002).

367 U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 514199 (issued Oct. 2000). This category was created for the 2002 Economic Census by taking a portion of the superseded 1997 category, "All Other Information Services," NAICS code 514199. The data cited in the text above are derived from the superseded category.

368 U.S. Census Bureau, "2002 NAICS Definitions: 516110 Internet Publishing and Broadcasting" (Feb. 2004) <www.census.gov>.

369 13 C.F.R. § 121.201, NAICS code 516110 (derived from 514199 and other 1997 codes).

370 U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 514199 (issued Oct. 2000). This category was created for the 2002 Economic Census by taking portions of numerous 1997 categories.

371 13 C.F.R. § 121.201, NAICS codes 511210, 541511, and 541519.

372 U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 511210 (issued Oct. 2000).

373 U.S. Census Bureau, 1997 Economic Census, Subject Series: Professional, Scientific, and Technical Services, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4a, NAICS code 541511 (issued Oct. 2000).

374 U.S. Census Bureau, 1997 Economic Census, Subject Series: Professional, Scientific, and Technical Services, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4a, NAICS code 541519 (issued Oct. 2000).

375 Office of Management and Budget, North American Industry Classification System 308-09 (1997) (NAICS code 334220).

376 13 C.F.R. § 121.201, NAICS code 334220.

377 The number of "establishments" is a less helpful indicator of small business prevalence in this context than would be the number of "firms" or "companies," because the latter take into account the concept of common ownership or control. Any single physical location for an entity is an establishment, even though that location may be owned by a different establishment. Thus, the numbers given may reflect inflated numbers of businesses in this category, including the numbers of small businesses. In this category, the Census breaks-out data for firms or companies only to give the total number of such entities for 1997, which were 1,089.

378 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Industry Statistics by Employment Size," Table 4, NAICS code 334220 (issued Aug. 1999).

379 *Id*. at Table 5.

380 Office of Management and Budget, North American Industry Classification System 308 (1997) (NAICS code 334210).

381 *Id*.

382 13 C.F.R. § 121.201, NAICS code 334210.

383 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Telephone Apparatus Manufacturing," Table 4, NAICS code 334210 (issued Sept. 1999).

384 Office of Management and Budget, North American Industry Classification System 306 (1997) (NAICS code 334111).

385 13 C.F.R. § 121.201, NAICS code 334111.

386 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Electronic Computer Manufacturing," Table 4, NAICS code 334111 (issued Aug. 1999).

387 Office of Management and Budget, North American Industry Classification System 307 (1997) (NAICS code 334113).

388 13 C.F.R. § 121.201, NAICS code 334113.

389 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Computer Terminal Manufacturing," Table 4, NAICS code 334113 (issued Aug. 1999).

390 Office of Management and Budget, North American Industry Classification System 307-08 (1997) (NAICS code 334119).

391 13 C.F.R. § 121.201, NAICS code 334119.

392 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Other Computer Peripheral Equipment Manufacturing," Table 4, NAICS code 334119 (issued Aug. 1999).

393 Office of Management and Budget, North American Industry Classification System 330 (1997) (NAICS code 335921).

394 13 C.F.R. § 121.201, NAICS code 335921.

395 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Fiber Optic Cable Manufacturing," Table 4, NAICS code 335921 (issued Nov. 1999).

396 Office of Management and Budget, North American Industry Classification System 331 (1997) (NAICS code 335929).

397 13 C.F.R. § 121.201, NAICS code 335929.

398 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Other Communication and Energy Wire Manufacturing," Table 4, NAICS code 335929 (issued Nov. 1999).

399 U.S. Census Bureau, "2002 NAICS Definitions: 334310 Audio and Video Equipment Manufacturing" (Feb. 2004) <www.census.gov>.

400 13 C.F.R. § 121.201, NAICS code 334310.

401 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Audio and Video Equipment Manufacturing," Table 4, NAICS code 334310 (issued Aug. 1999).

402 U.S. Census Bureau, "2002 NAICS Definitions: 334411 Electron Tube Manufacturing" (Feb. 2004) <www.census.gov>.

403 13 C.F.R. § 121.201, NAICS code 334411.

404 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Electron Tube Manufacturing," Table 4, NAICS code 334411 (issued July 1999).

405 U.S. Census Bureau, "2002 NAICS Definitions: 334412 Bare Printed Circuit Board Manufacturing" (Feb. 2004) <www.census.gov>.

406 13 C.F.R. § 121.201, NAICS code 334412.

407 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Bare Printed Circuit Board Manufacturing," Table 4, NAICS code 334412 (issued Aug. 1999).

408 U.S. Census Bureau, "2002 NAICS Definitions: 334413 Semiconductor and Related Device Manufacturing" (Feb. 2004) <www.census.gov>.

409 13 C.F.R. § 121.201, NAICS code 334413.

410 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Semiconductor and Related Device Manufacturing," Table 4, NAICS code 334413 (issued July 1999).

411 U.S. Census Bureau, "2002 NAICS Definitions: 334414 Electronic Capacitor Manufacturing" (Feb. 2004) <www.census.gov>.

412 13 C.F.R. § 121.201, NAICS code 334414.

413 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Electronic Capacitor Manufacturing," Table 4, NAICS code 334414 (issued July 1999).

414 U.S. Census Bureau, "2002 NAICS Definitions: 334415 Electronic Resistor Manufacturing" (Feb. 2004) <www.census.gov>.

415 13 C.F.R. § 121.201, NAICS code 334415.

416 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Electronic Resistor Manufacturing," Table 4,

NAICS code 334415 (issued Aug. 1999).

417 U.S. Census Bureau, "2002 NAICS Definitions: 334416 Electronic Coil, Transformer, and Other Inductor Manufacturing" (Feb. 2004) <www.census.gov>.

418 13 C.F.R. § 121.201, NAICS code 334416.

419 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Electronic Coil, Transformer, and Other Inductor Manufacturing," Table 4, NAICS code 334416 (issued Aug. 1999).

420 U.S. Census Bureau, "2002 NAICS Definitions: 334417 Electronic Connector Manufacturing" (Feb. 2004) <www.census.gov>.

421 13 C.F.R. § 121.201, NAICS code 334417.

422 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Electronic Connector Manufacturing," Table 4, NAICS code 334417 (issued July 1999).

423 U.S. Census Bureau, "2002 NAICS Definitions: 334418 Printed Circuit Assembly (Electronic Assembly) Manufacturing" (Feb. 2004) <www.census.gov>.

424 13 C.F.R. § 121.201, NAICS code 334418.

425 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Printed Circuit Assembly (Electronic Assembly) Manufacturing," Table 4, NAICS code 334418 (issued Sept. 1999).

426 U.S. Census Bureau, "2002 NAICS Definitions: 334419 Other Electronic Component Manufacturing" (Feb. 2004) <www.census.gov>.

427 13 C.F.R. § 121.201, NAICS code 334419.

428 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Other Electronic Component Manufacturing," Table 4, NAICS code 334419 (issued Aug. 1999).

429 U.S. Census Bureau, "2002 NAICS Definitions: 334112 Computer Storage Device Manufacturing" (Feb. 2004)

<www.census.gov>.

430 13 C.F.R. § 121.201, NAICS code 334112.

431 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Computer Storage Device Manufacturing," Table 4, NAICS code 334112 (issued July 1999).

432 *See* Order at paras. 51-53.

433 *See id*. at para. 51.

434 *See id*.

435 *See id*. at paras. 37-50.

436 *See id*. at paras. 26-32.

437 *See id*. at paras. 13-23.

438 *See id*. at paras. 20-22.

439 *See id*. at para. 61.

440 *See id*. at para. 24.

441 *See id*. at paras. 26-26.

442 5 U.S.C. § 603(c).

443 *See Notice*, 21 FCC Rcd at 1787-89, 1790-91, 1793, paras. 11, 12, 16, 18, 19, 23, 29, 30.

444 *See id.* at 1793, para. 30.

445 *See id.* at 1787-88, para. 11.

446 *See id.* at 1789, para. 16.

447 *See id.* at 1790, para. 18.

448 *See id.* at 1790, para. 19.

449 *See id.* at 1791, para. 23.

450 *See id.* at 1793, paras. 29-30.

451 *See* Order at para. 61.

452 *See, e.g., id.* at para. 5.

453 *See* 5 U.S.C. § 801(a)(1)(A).

454 *See* 5 U.S.C. § 604(b).

455 *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. §§ 601-12, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

456 *See* 5 U.S.C. § 603(a).

457 *See* 5 U.S.C. § 603(a).

458 *See* Further Notice at paras. 68-70.

459 *See id*. at para. 72.

460 *See id*.

461 *See id*. at paras. 68-72.

462 5 U.S.C. §§ 603(b)(3), 604(a)(3).

463 5 U.S.C. § 601(6).

464 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such terms which are appropriate to the activities of the agency and publishes such definitions(s) in the Federal Register."

465 15 U.S.C. § 632.

466 *See* SBA, Programs and Services, SBA Pamphlet No. CO-0028, at page 40 (July 2002).

467 Independent Sector, The New Nonprofit Almanac & Desk Reference (2002).

468 5 U.S.C. § 601(5).

469 U.S. Census Bureau, Statistical Abstract of the United States: 2006, Section 8, page 272, Table 415.

470 We assume that the villages, school districts, and special districts are small, and total 48,558. *See* U.S. Census Bureau, Statistical Abstract of the United States: 2006, section 8, page 273, Table 417. For 2002, Census Bureau data indicate that the total number of county, municipal, and township governments nationwide was 38,967, of which 35,819 were small. *Id*.

471 15 U.S.C. § 632.

472 Letter from Jere W. Glover, Chief Counsel for Advocacy, SBA, to William E. Kennard, Chairman, FCC (May 27, 1999). The Small Business Act contains a definition of "small-business concern," which the RFA incorporates into its own definition of "small business." *See* 15 U.S.C. § 632(a) (Small Business Act); 5 U.S.C. § 601(3) (RFA). SBA regulations interpret "small business

concern" to include the concept of dominance on a national basis. *See* 13 C.F.R. § 121.102(b).

473 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

474 FCC, Wireline Competition Bureau, Industry Analysis and Technology Division, "Trends in Telephone Service" at Table 5.3, page 5-5 (April 2005) ("Trends in Telephone Service"). This source uses data that are current as of October 1, 2004.

475 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

476 "Trends in Telephone Service" at Table 5.3.

477 13 C.F.R. § 121.201, NAICS code 517310 (changed from 513330 in Oct. 2002).

478 "Trends in Telephone Service" at Table 5.3.

479 13 C.F.R. § 121.201, NAICS code 517310 (changed from 513330 in Oct. 2002).

480 "Trends in Telephone Service" at Table 5.3.

481 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

482 "Trends in Telephone Service" at Table 5.3.

483 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

484 "Trends in Telephone Service" at Table 5.3.

485 13 C.F.R. § 121.201, NAICS code 517110 (changed from 513310 in Oct. 2002).

486 "Trends in Telephone Service" at Table 5.3.

487 13 C.F.R. § 121.201, NAICS code 517310 (changed from 513330 in Oct. 2002).

488 "Trends in Telephone Service" at Table 5.3.

489 We include all toll-free number subscribers in this category, including those for 888 numbers.

490 13 C.F.R. § 121.201, NAICS code 517310 (changed from 513330 in Oct. 2002).

491 *See* FCC, Common Carrier Bureau, Industry Analysis Division, *Study on Telephone Trends*, Tables 21.2, 21.3, and 21.4 (Feb. 1999).

492 13 C.F.R. § 121.201, NAICS codes 517410 and 517910.

493 U.S. Census Bureau, "2002 NAICS Definitions: 517410 Satellite Telecommunications" (www.census.gov., visited Feb. 2006).

494 U.S. Census Bureau, 2002 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 517410 (issued Nov. 2005).

495 *Id*. An additional 38 firms had annual receipts of $25 million or more.

496 U.S. Census Bureau, "2002 NAICS Definitions: 517910 Other Telecommunications" (www.census.gov, visited Feb. 2006).

497 U.S. Census Bureau, 2002 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 517910 (issued Nov. 2005).

498 *Id*. An additional 14 firms had annual receipts of $25 million or more.

499 13 C.F.R. § 121.201, NAICS code 513321 (changed to 517211 in October 2002).

500 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

501 U.S. Census Bureau, 2002 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms for the United States: 2002, NAICS code 517211 (issued November 2005).

502 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is firms with "1000 employees or more."

503 U.S. Census Bureau, 2002 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms for the United States: 2002, NAICS code 517212 (issued November 2005).

504 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is firms with "1000 employees or more."

505 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

506 U.S. Census Bureau, 2002 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms for the United States: 2002, NAICS code 517212 (issued November 2005).

507 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is firms with "1000 employees or more."

508 "Trends in Telephone Service" at Table 5.3.

509 *Id*.

510 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

511 U.S. Census Bureau, 2002 Economic Census, Subject Series: "Information," Table 5, Employment Size of Firms for the United States: 2002, NAICS code 517211 (issued November 2005).

512 *Id*. The census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is firms with "1000 employees or more."

513 *Amendment of Part 90 of the Commission's Rules to Provide for the Use of the 220-222 MHz Band by the Private Land Mobile Radio Service*, PR Docket No. 89-552, Third Report and Order and Fifth Notice of Proposed Rulemaking, 12 FCC Rcd 10943, 11068-70, paras. 291-295, 62 FR 16004 (Apr. 3, 1997).

514 *See* Letter to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC, from A.

Alvarez, Administrator, SBA (Dec. 2, 1998) (SBA Dec. 2, 1998 Letter).

515 *Revision of Part 22 and Part 90 of the Commission's Rules to Facilitate Future Development of Paging Systems*, Memorandum Opinion and Order on Reconsideration and Third Report and Order, 14 FCC Rcd 10030, paras. 98-107 (1999).

516 *Id*. at 10085, para. 98.

517 "Trends in Telephone Service" at Table 5.3.

518 *Id*.

519 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

520 *Id*.

521 "Trends in Telephone Service" at Table 5.3.

522 *See Amendment of Parts 20 and 24 of the Commission's Rules -- Broadband PCS Competitive Bidding and the Commercial Mobile Radio Service Spectrum Cap*, WT Docket No. 96-59, Report and Order, 11 FCC Rcd 7824, 61 FR 33859 (July 1, 1996) (*PCS Order*); *see also* 47 C.F.R. § 24.720(b).

523 *See PCS Order*, 11 FCC Rcd 7824.

524 *See, e.g., Implementation of Section 309(j) of the Communications Act -- Competitive Bidding*, PP Docket No. 93-253, Fifth Report and Order, 9 FCC Rcd 5332, 59 FR 37566 (July 22, 1994).

525 FCC News, Broadband PCS, D, E and F Block Auction Closes, No. 71744 (rel. Jan. 14, 1997); *see also Amendment of the Commission's Rules Regarding Installment Payment Financing for Personal Communications Services (PCS) Licenses*, WT Docket No. 97-82, Second Report and Order, 12 FCC Rcd 16436, 62 FR 55348 (Oct. 24, 1997).

526 *Amendment of the Commission's Rules to Establish New Personal Communications Services, Narrowband PCS*, Docket No. ET 92-100, Docket No. PP 93-253, Second Report and Order and Second Further Notice of Proposed Rulemaking, 15 FCC Rcd 10456, 65 FR 35875 (June 6, 2000).

527 *See* SBA Dec. 2, 1998 Letter.

528 The service is defined in section 22.99 of the Commission's Rules, 47 C.F.R. § 22.99.

529 BETRS is defined in sections 22.757 and 22.759 of the Commission's Rules, 47 C.F.R. §§ 22.757 and 22.759.

530 13 C.F.R. § 121.201, NAICS code 517212.

531 The service is defined in section 22.99 of the Commission's Rules, 47 C.F.R. § 22.99.

532 13 C.F.R. § 121.201, NAICS codes 517212.

533 This service is governed by Subpart I of Part 22 of the Commission's rules. *See* 47 C.F.R. §§ 22.1001-22.1037.

534 13 C.F.R. § 121.201, NAICS code 513322 (changed to 517212 in October 2002).

535 *Id*.

536 13 C.F.R. § 121.201, North American Industry Classification System (NAICS) code 513220 (changed to 517510 in October 2002).

537 U.S. Census Bureau, 2002 Economic Census, Subject Series: Information, Table 4, Receipts Size of Firms for the United States: 2002, NAICS code 517510 (issued November 2005).

538 *Id*. An additional 61 firms had annual receipts of $25 million or more.

539 47 C.F.R. § 76.901(e). The Commission determined that this size standard equates approximately to a size standard of $100 million or less in annual revenues. *Implementation of Sections of the 1992 Cable Act: Rate Regulation,* Sixth Report and Order and Eleventh Order on Reconsideration, 10 FCC Rcd 7393, 7408 (1995).

540 47 C.F.R. § 76.901(c).

541 47 U.S.C. § 543(m)(2); *see* 47 C.F.R. § 76.901(f) & nn. 1-3.

542 *See* Public Notice, *FCC Announces New Subscriber Count for the Definition of Small Cable Operator*, DA 01-158 (Cable Services Bureau, Jan. 24, 2001).

543 47 C.F.R. § 76.901(f).

544 The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(f) of the Commission's rules. *See* 47 C.F.R. § 76.909(b).

545 *See* 47 U.S.C. § 573.

546 13 C.F.R. § 121.201, NAICS code 513220 (changed to 517510 in October 2002).

547 *See* < http://www.fcc.gov/csb/ovs/csovscer.html> (current as of March 2002).

548 U.S. Census Bureau, "2002 NAICS Definitions: 518111 Internet Service Providers" (Feb. 2004) <www.census.gov>.

549 13 C.F.R. § 121.201, NAICS code 518111 (changed from previous code 514191, "On-Line Information Services," in Oct. 2002).

550 U.S. Census Bureau, 2002 Economic Census, Subject Series: Information, Table 4, Receipts Size of Firms for the United States: 2002, NAICS code 518111 (issued November 2005).

551 *Id*. An additional 45 firms had annual receipts of $25 million or more.

552 U.S. Census Bureau, "2002 NAICS Definitions: 519190 All Other Information Services" (Feb. 2004) <www.census.gov>.

553 13 C.F.R. § 121.201, NAICS code 519190 (changed from 514199 in Oct. 2002).

554 U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization)," Table 4, NAICS code 514199 (issued Oct. 2000). This category was created for the 2002 Economic Census by taking a portion of the superseded 1997 category, "All Other Information Services," NAICS code 514199. The data cited in the text above are derived from the superseded category.

555 Office of Management and Budget, North American Industry Classification System 308-09 (1997) (NAICS code 334220).

556 13 C.F.R. § 121.201, NAICS code 334220.

557 The number of "establishments" is a less helpful indicator of small business prevalence in this context than would be the number of "firms" or "companies," because the latter take into account the concept of common ownership or control. Any single physical location for an entity is an establishment, even though that location may be owned by a different establishment. Thus, the numbers given may reflect inflated numbers of businesses in this category, including the numbers of small businesses. In this category, the Census breaks-out data for firms or companies only to give the total number of such entities for 1997, which were 1,089.

558 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Industry Statistics by Employment Size," Table 4, NAICS code 334220 (issued Aug. 1999).

559 *Id*. Table 5.

560 Office of Management and Budget, North American Industry Classification System 308 (1997) (NAICS code 334210).

561 *Id*.

562 13 C.F.R. § 121.201, NAICS code 334210.

563 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Telephone Apparatus Manufacturing," Table 4, NAICS code 334210 (issued Sept. 1999).

564 U.S. Census Bureau, "2002 NAICS Definitions: 334413 Semiconductor and Related Device Manufacturing" (Feb. 2004) <www.census.gov>.

565 13 C.F.R. § 121.201, NAICS code 334413.

566 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Semiconductor and Related Device Manufacturing," Table 4, NAICS code 334413 (issued July 1999).

567 U.S. Census Bureau, "2002 NAICS Definitions: 334112 Computer Storage Device Manufacturing" (Feb. 2004) <www.census.gov>.

568 13 C.F.R. § 121.201, NAICS code 334112.

569 U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Computer Storage Device Manufacturing," Table 4, NAICS code 334112 (issued July 1999).

570 *See* Further Notice at para. 68.

571 *See* Further Notice at paras. 69, 71.

572 *See* Further Notice at para. 70.

573 *See* Further Notice at para. 72.

574 *See* Further Notice at paras. 68-72.

575 5 U.S.C. § 603(c).

576 *See* Further Notice at paras. 68-72.

22 FCC Rcd. 6927 (F.C.C.), 22 F.C.C.R. 6927, 40 Communications Reg. (P&F) 1282, 2007 WL 983953

28 FCC Rcd. 9609 (F.C.C.), 28 F.C.C.R. 9609, 58 Communications Reg. (P&F) 739, 2013 WL 3271062

Federal Communications Commission (F.C.C.)
Declaratory Ruling

IN THE MATTER OF IMPLEMENTATION OF THE TELECOMMUNICATIONS ACT OF 1996: TELECOMMUNICATIONS CARRIERS' USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION AND OTHER CUSTOMER INFORMATION

CC Docket No. 96-115
FCC
13
-
89
Adopted: June 27, 2013
Released:June 27, 2013

****1 *9609** By the Commission: Acting Chair woman Clyburn and Commissioner Rosenworcel issuing separate statements; Commissioner Pai approving in part, concurring in part and issuing a statement.

I. INTRODUCTION

1. In this *Declaratory Ruling*, we address the real privacy and security risks that consumers face when telecommunications carriers use their control of customers' mobile devices to collect information about their customers' use of the network. Absent carriers' adoption of adequate security safeguards, consumers' sensitive information, such as the numbers a wireless customer has called, the time calls are made, and where the customer was located when he or she made a call, can be disclosed to third parties without consumers' knowledge or consent. The Commission acts now to clarify existing lawso that consumers will know that their carriers must safeguard thesekinds of information so long as the information is collected by or at the direction of the carrier and the carrier or its designee[1] has access to or control over the information.

2. Technology now allows consumers to use wireless devices that provide powerful computing, as well as communications, capabilities. Carriers, which most often control the initial configuration of these devices, can use their unique position as the provider of the wireless service and the device to configure their customers' devices in ways that will serve their needs as service providers.In particular, carriers can cause the devices to collect information that includessuch things as lists of numbers called and calls received and the locations from which calls have been made. While residing on the device, that sensitive information is potentially vulnerable to acquisition by others. It is thus important that the Commission clarifycarriers' statutory and regulatory obligations with respect to information that they collect from their customers.

3. The actual risks to consumers of unauthorized disclosure of sensitive information—and the need for Commission action—are demonstrated by the insecure way in which some carriers caused software provided by Carrier IQ, Inc. (Carrier IQ) to be installed on some mobile devices. Carrier IQ's diagnostic software can be installed on a mobile device to provide carriers with information about how ***9610** their network and devices on their network are functioning.[2] In November 2011, a researcher discovered security vulnerabilities that permitted third parties to access the information collected by the Carrier IQ software, resulting in the potential for consumers' location and other data to be accessed and disclosed.[3] This discovery led to calls for an investigation into the overall security of sensitive information throughout the mobile services ecosystem.[4]

****2** 4. To clarify these issues, this *Declaratory Ruling* addresses howsection 222 of the Communications Act of 1934, as amended (the Act), and the Commission's implementing rules apply to information relating to telecommunications service and interconnected voice over Internet Protocol (VoIP) service that fits the statutory definition of customer proprietary network information(CPNI)[5] when such information is collected by the customer's device, provided the collection is

undertaken at the mobile wireless carrier's direction and the carrier or its designee has access to or control over the information.

5. We acknowledge that there may well be good reasons for carriers to collect CPNI on mobile devices,and we are not barring them from doing so. We are simply clarifying that if they choose to do so, they must protect the confidentiality of such CPNI as required by section 222and may use it only as permitted by law.We take this action so that carriers understand their legal responsibility to protect CPNI collected in this manner just as they must protect CPNI collected and stored in other ways. In this regard, this *Declaratory Ruling* takes into consideration developments in technologies and business practices in the market for mobile communications services and the record developed in response to a Public Notice issued by the Wireline Competition Bureau, Wireless Telecommunications Bureau, and Office of General Counsel in May 2012.[6]

6. The legal issue here arises under 47 U.S.C. § 222. Section 222 establishes the duty of every telecommunications carrier to "protect the confidentiality of proprietary information of, and relating to ... customers."[7] Furthermore,a carrier that receives or obtains CPNI by virtue of its provision of a telecommunications service may use, disclose, or permit access to such information only in limited circumstances.[8] The Commission has adopted rules to implement those obligations.[9] The Commission ***9611** also has extended application of the CPNI requirements to providers of interconnected VoIP service.[10]

7. We conclude that the definition of CPNI in section 222 and the obligations flowing from that definition apply to information that telecommunications carriers cause to be stored on their customers'devices when carriers or their designees have access to or control over that information. When providers of mobile telecommunications service leverage their control of their customers' mobile devices to collect information that relates to the quantity, technical configuration, type, destination, location, and amount of use of the telecommunications service,[11] that information is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship"[12] and therefore is CPNI. A telecommunications carrier that collects CPNI by virtue of its control over its customer's mobile device is obligated to protect that information by the Act and by the Commission's rules.[13]

****3** 8. We do not, at this time, adopt or propose any new rules to apply specific new obligations to carriers that collect CPNI in this manner. Rather, this *Declaratory Ruling* discusses the applicability of existing standards and requirements to this context.

II. BACKGROUND

9. Congress, through the Communications Act, requires communications providers to protect consumers' sensitive personal information to which they have access as a result of their unique position as network operators.Section 222, which became part of the Act in 1996, obligates telecommunications carriers to protect the privacy and security of information about their customers. Its most specific obligations[14] concern CPNI, which includes information about a customer's use of the service that is made available to the carrier by virtue of the carrier-customer relationship. As the Commission has explained, "[p]ractically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting."[15]

***9612** 10. Congress enacted section 222 to "define[] three fundamental principles to protect all consumers. These principles are: (1) the right of consumers to know the specific information that is being collected about them; (2) the right of consumers to have proper notice that such information is being used for other purposes; and (3) the right of consumers to stop the reuse or sale of that information."[16] The Commission's implementation of section 222 to date has focused on rules governing the use and disclosure of CPNI, including the extent to which section 222 permits carriers to use CPNI to render the telecommunications service from which the CPNI was derived,[17] the types of consent that a carrier must obtain for use and disclosure, and safeguards to protect against unauthorized use or disclosure of CPNI.[18] In 2007, the Commission extended application of its CPNI rules to providers of interconnected VoIP service,[19] concluding that the rules would apply whether interconnected VoIP service is a telecommunications service or an information service.[20]

11. The last time the Commission updated its CPNI rules, in 2007, its focus was on the then-increasing practice of "pretexting," which refers to "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records."[21] The Commission concluded that "pretexters have been successful at gaining unauthorized access to CPNI"[22] and that "carriers' record on protecting CPNI

demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI."[23] The Commission therefore imposed security requirements on carriers' disclosure of CPNI to customers over the telephone and online, required that law enforcement and customers be notified of security breaches involving CPNI, and required affirmative customer consent ("opt-in consent") before a carrier could disclose a customer's CPNI to a carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer.[24]

****4** 12. In a Further Notice of Proposed Rulemaking (FNPRM) that accompanied the 2007 order, the Commission suggested that section 222 imposes an obligation on carriers to protect information stored on customers' devices. At that time, the Commission was addressing an emerging security concern: the security of information stored on mobile communications devices, particularly at the time such devices are returned for refurbishment and resale. The Commission sought comment on carriers' practices for erasing customer information in those circumstances and "whether the Commission should ***9613** require carriers to permanently erase, or allow customers to permanently erase, customer information in such circumstances."[25] In response, carriers argued against the appropriateness or the Commission's authority to adopt such a requirement,emphasizing consumers' control of, and the carriers' lack of control of, information residing on consumers' devices. For example, AT&T Inc. commented that "decisions about what personal data to store, or not to store, on a mobile device rest with the consumer. Carriers do not typically have access to such information and play no role in determining what information a consumer chooses to store on mobile devices or how that information is used."[26] Sprint Nextel Corporation commented that " [w]ireless carriers are not well-positioned to guarantee the privacy of customer information stored on devices" because those devices are manufactured by suppliers and "in the physical control and custody of customers."[27] Sprint added that "none of the information (e.g., songs, photographs and address books) stored on a handset is CPNI and thus [it] is not addressed by section 222 of the Act."[28]

13. In May 2012, the Wireline Competition Bureau, the Wireless Telecommunications Bureau, and the Office of General Counsel issued aPublic Notice in this docket(the *Mobile Device Privacy and Security Public Notice*) in response to more recent technological and business developments, particularly the growing practice of mobile carriers collecting and storing customer-specific information on their customers' mobile devices using software tools. The Public Notice observed that the comments in response to the 2007 FNPRM, which had emphasized the carriers' lack of control of information stored on communications devices, were out of date, and it sought comment to refresh the record concerning the practices of mobile wireless service providers with respect to information stored on their customers' mobile communications devices.[29]

14. One such software tool has beenprovided to various carriers by Carrier IQ, Inc.[30] As discussed above, Carrier IQ's diagnostic software can be installed on a mobile device to provide carriers with information about how their network and devices on their network are functioning.[31] Based on specifications determined by the carrier, such information may include dialed phone numbers and calling behavior, location coordinates, and mobile subscriber numbers, among other data elements.[32] In November 2011, a researcher discovered security vulnerabilities that permitted others to access the sensitive information collected by the Carrier IQ software, resulting in the potential for users' location and other data to be accessed and disclosed.[33] In response to congressional inquiries, carrierssaid that they had been using Carrier IQ's tool in order to enhance their ability to evaluate and improve their network services and to improve the ability of customer-service representatives to assist their customers ***9614** with problems, and that they were doing so in compliance with privacy laws.[34]

****5** 15. After the Commission began this proceeding, the Federal Trade Commission (FTC) announced that mobile-device manufacturer HTC America (HTC) had agreed to settle charges that it had "failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk."[35] The FTC's complaint charged that HTC had insecurely implemented two logging applications, Carrier IQ and HTC Loggers, creating vulnerabilities that compromised the functionality of devices and sensitive information stored on those devices. For example, according to the consent order, avulnerability on certain HTC devices would allow any third-party application that could connect to the Internet to intercept information being collected by the Carrier IQ software.[36]

III. DISCUSSION

16. After review of the record in response to the*Mobile Device Privacy and Security Public Notice*, we conclude that there is uncertainty in the industry about obligations to protect CPNI collected by mobile devices. To address that uncertainty, and to

ensure that potentially sensitive consumer information is handled appropriately, we issue this ruling declaring that section 222 applies to information that fits the statutory definition of CPNI when such information is collected by the subscriber's mobile device, provided the collection is undertaken at the carrier's direction and that the carrier or its designee has access to or control over that information. By issuing this *Declaratory Ruling*, we do not prohibit such information collection, which may well have beneficial uses for improved network operations, but we make clear that telecommunications carriers are responsible for securing the information and that the Commission will hold carriers responsible for compliance with their statutory and regulatory obligations.

17. We disagree with commenters who claim that section 222 is too rigid or outdated to apply to mobile devices. The relationship between a telecommunications carrier and its customer is one of particular sensitivity, given the special position that a carrier occupies as its customers' gatekeeper to the network, and Congress recognized that special position in enacting section 222. This is no less the case when the information is stored at the carrier's direction on a mobile device. In this regard, we note that Verizon Wireless argues that "precise location information warrants different protections than anonymous or aggregate data" and, therefore, "the extent of notice provided, and necessity or manner of consumer consent, will vary depending on the circumstances."[37] This illustration is fully consistent with ***9615** our conclusion. Aggregate customer information is not subject to the privacy obligations in section 222(c)(1).[38] Rather, section 222 is calibrated to apply its strongest protections to "individually identifiable" CPNI.[39]

****6** 18. We take this action not because the practice of collecting CPNI from customers' mobile devices is inherently improper or to prevent providers from doing so, but because these actions create risks and thus impose reasonable responsibilities on the carriers that engage in such practice. As pointed out by many commenters, collecting customer information from mobile devices can benefit consumers.Although other information in a carrier's network might enable a network operator to become aware that calls are being dropped or that a specific geographic area has poor reception, the mobile device itself is in a better position to collect information about the reason for a dropped call or other failure.[40] Data from mobile devices can also be useful in responding to customer requests for assistance with device, service, and performance issues.[41] It can also help a network operator determine which parts of its network are most in need of improvement and whether particular models of phones are experiencing more problems than others.[42]

19. There are thus legitimate reasons for mobile providers to collect information on their customers' mobile devices. Doing so, however, also creates risks to the privacy and security of consumers' information. In theexample that led Commission staff to issue the *Mobile Device Privacy and Security Public Notice*, it appears that at least some smartphones that carriers equipped with the Carrier IQ software were configured in such a way as to store a great deal of sensitive customer information in an insecure manner, creating the possibility that it could be captured by malicious third-party applications.[43] Even to the extent that customers may have known about or consented to the service provider's collection and use of data in this manner,[44] a customer's consent to the collection and use of data to maintain and improve the network would not constitute consent for other use, disclosure, or permission of access (such as storing it in an insecure manner), nor would it negate section 222(a)'s duty to protect proprietary information from unauthorized access or disclosure.

20. In this *Declaratory Ruling*, we do not reach any conclusions about whether carriers have violated the Act as a result of the Carrier IQ event discussed above. Rather, we issue this *Declaratory Ruling* because there is a need to clarify the obligations of mobile providers when they or their designees collect and have access to or control over sensitive customerinformation by virtue of their control of customers' devices.

A. Data Collected by Mobile Devices May Be CPNI.

21. We conclude that customer-specific information collected by mobile devices can include ***9616** information that fits the statutory definition of CPNI.The statute defines CPNI to include the following:
(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

****7** (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.[45]

22. Application of this definition is straightforward. Information collected by a mobile device can include "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer," such as the telephone numbers of calls dialed and received and the location of the device at the time of the calls — information that is recorded by the Carrier IQ software.[46] The Commission has previously made clear that "CPNI includes information such as the phone numbers called by a consumer [and] the frequency, duration, and timing of such calls."[47] The location of a customer's use of a telecommunications service also clearly qualifies as CPNI.[48]

23. We also conclude that information that a carrier causes to be stored on its customer's device in order to allow the information to be shared with the carrier is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[49] This is true whether the carrier itself installs, or directs the installation of, the software that collects the information, and whether the information is shared directly with the carrier or with its designee.[50] A carrier is in a unique position with respect to its customers when it configures a mobile device to collect the information before the device is sold to a customer.[51] This unique position satisfies the "carrier-customer relationship" element of the definition of CPNI.

***9617** 24. We disagree with CTIA's argument that "data stored on mobile devices is not CPNI within the meaning of Section 222 because it is not 'information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service."[52] Although it is certainly true that *some* of the information that carriers have collected and stored on mobile devices is not CPNI,[53] it is equally clear that some of it is.[54] In any event, if the information a carrier collects in the future does not meet the statutory definition, then section 222 will not apply. To reiterate, the Commission is clarifying only that information that meets the definition of CPNI is subject to section 222, just as the same information would be subject to section 222 if it were stored elsewhere on a carrier's network.

25. We also disagree with CTIA and some other commenters' contention that "[n]etwork diagnostic information and other information acquired from wireless devices is not CPNI because it does not contain personally identifiable call data."[55] The examples CTIA cites, such as "data on when and where calls fail" and "the location, date, and time a handset experiences a network event, such as a dialed or received telephone call [or] a dropped call,"[56] do reveal call details, which we conclude do fall within the statutory definition of CPNI.[57]

****8** 26. We alsodo not interpret section 222 or the Commission's rules in the limited way suggested by Verizon Wireless,which contends that the Commission's CPNI rules "are targeted at information related to a telecommunications carrier's provision of telecommunications services available via its network, and at activities and operations relating to a carrier's network and back-office systems."[58] The language of section 222 and the Commission's implementing rules do not specifically exclude information collected on mobile devices. The record developed in response to the Carrier IQ controversy and the subsequent *Mobile Device Privacy and Security Public Notice* demonstrates that carriers can and do exercise control over the wireless devices used to connect to their networks. They can determine, for instance, what CPNI the device will collect, how it will be stored, and when such information will be transmitted back to the carrier, without the customer's specific knowledge or ability to change those parameters in the device settings. Accordingly, the carrier is in a position to protect the privacy and ***9618** security of information collected in that manner. We therefore decline to limit the "carrier-customer relationship" element of the definition of CPNI to exclude information that resides on devices.

27. The fact that CPNI is on a device and has not yet been transmitted to the carrier's own servers also does not remove the data from the definition of CPNI, if the collection has been done at the carrier's direction.[59] CPNI is defined as information that is *made available to the carrier*;[60] even if that information has not yet been transmitted from the mobile device to the carrier, the configuration of the device has made the information available to the carrier. Nor do we read the language in paragraph (c)(1), which imposes obligations on a telecommunications carrier "that receives or obtains [CPNI] by virtue of its provision of a telecommunications service," as excluding information that has not yet been transmitted to the carrier's back-office systems. We reach this conclusion for two independent reasons: First, that provision does not limit a carrier's obligations to CPNI that it has received.[61] Second, we conclude that information stored on a customer's device at the carrier's direction for the purpose of transmitting it to the carrier or its designee (and accessible to or controlled by the carrier or its designee) has, for this purpose, been obtained by the carrier.[62] Such information is under the carrier's control for all practical purposes, and the statutory obligations should and do apply.[63] We also note that subsection (a)'s obligation to protect

customer information is not limited to CPNI that the carrier has obtained or received.[64] This statutory obligation provides independent support for requiring carriers to secure the CPNI that they have caused to be stored on a customer's device.[65]

**9 28. We recognize that not all of the information collected on mobile wireless devices is CPNI. Some of the information that software such as the Carrier IQ agent can record does not pertain to a telecommunications service or might otherwise not relate to the quantity, technical configuration, type, destination, location, or amount of use of a telecommunications service, as required by the statutory *9619 definition of CPNI.[66] In addition, modern mobile operating systems enable consumers to install applications developed by third parties that can collect sensitive personal information. Such third-party applications may raise privacy concerns. They are, however, generally beyond the scope of section 222 and our rules. For example, third-party applications might collect the same or different kinds of data,[67] some of which might be CPNI if collected at the carrier's direction; wheresuch information is not collected by or at the direction of a carrier or its agent, it is not "made available to the carrier ... by virtue of the carrier-customer relationship."[68] Furthermore, information stored on a mobile device that is not under the carrier's control and not intended to be transmitted to the carrier or otherwise not accessible by the carrier, as may be the case with a contact list or call log, is not CPNI because it is not "made available to the carrier,"[69] even if it would otherwise satisfy the definition of CPNI if made available to the carrier.

B. Telecommunications Carriers Have Statutory Obligations to Protect CPNI That They Collect on a Mobile Device.

29. We do not, at this time, adopt or propose any new rules governing the protection, use, or disclosure of individually identifiable CPNI that carriers collect by virtue of their control of customers' mobile devices. Rather, this *Declaratory Ruling* removes uncertainty about whether the obligations that already exist under the statute and our rules apply to CPNI collected in this manner. For example, section 222(a) of the Act provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to... customers,"[70] and section 222(c)(1)'s restriction on "disclos[ure]" of "individually identifiable" CPNI would appear to make carriers liable for inadvertent disclosures.[71] Such obligations apply equally to CPNI that carriers collect via their customers' devices.

30. The Commission has made clear that carriers must "take[] reasonable precautions to prevent the unauthorized disclosure of a customer's CPNI."[72] To the extent that a carrier's failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, we believe that a violation of section 222 may have occurred. Any decision would depend on the facts and circumstances in a particular case.[73]

**10 31. Some commenters note that third-party applications commonly store personal data on mobile devices and that wireless carriers have no ability to restrict the ability of those applications to *9620 access data stored on a mobile device.[74] To the extent that is true, it imposes an obligation on carriers to ensure that, if they choose to collect or store CPNI on a device and have access to or control over that data, they take reasonable precautions to protect it from unauthorized access and disclosure by such third-party applications, whether by storing the CPNI in a location or form that it is protected or otherwise.

32. Section 222 does not require mobile carriers to protect their customers against all possible privacy and security risks related to non-CPNI on a mobile device, including risks created by third-party applications. The openness of modern smartphones and the ability that they provide consumers to install applications that they desire has produced tremendous benefits.[75] While those benefits also come with risks to the privacy and security of consumers' information, those are risks that other parties may have a responsibility to address or that consumers might assume by their use of such applications.

33. We also reiterate that section 222(c)(1) allows a telecommunications carrier to use, disclose, or permit access to this CPNI "in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service."[76] A carrier thus may use, disclose, or permit access to such information "to initiate, render, bill, and collect for telecommunications services" or "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[77] These provisions should allow a carrier that collects CPNI from customers' devices to use that information to assess and improve the performance of its network and to provide information to customer-support representatives without the customer's specific approval.[78] Verizon Wireless, for example, argues that "it is legitimate for service providers to use diagnostic tools to ensure network performance, provided they employ adequate data security protections."[79] We do not prohibit such practices. Our rules also allow a wireless provider to "use, disclose, or permit access

to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s)."[80]

34. Furthermore, as noted above,[81] neither section 222 nor the Commission's implementing rules restrict carriers' use of aggregate customer information. The statute defines "aggregate customer ***9621** information" to mean "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[82] It makes clear that a telecommunications carrier is not subject to the CPNI restrictions in using, disclosing, or permitting access to aggregate customer information.[83] For example, the Commission has said that carriers are free to use aggregate information "to assist in product development and design, as well as in tracking consumer buying trends, without customer approval."[84] Accordingly, a carrier may store or use aggregate information collected from customers' devices without violating section 222.[85] The exception for aggregate customer information and the other exceptions in section 222(d) do not, however, remove the obligations of a telecommunications carrier to protect the confidentiality of CPNI and to prevent unauthorized use, disclosure, or access.[86]

C. This *Declaratory Ruling* Is Consistent With Other Privacy Regimes.

****11** 35. CTIA argues that the Stored Communications Act (SCA), adopted as part of the Electronic Communications Privacy Act in 1986,[87] "confirms the lack of Commission authority in this area because it gives wireless providers broad authority to access and use their customers' information for network diagnostic purposes."[88] But an examination of the provisions cited by CTIA shows that the SCA poses no conflict: The SCA is a general criminal prohibition on voluntary disclosure of customer records; its exceptions carve certain disclosures out of that general prohibition. For example, the SCA's provision that appears to allow a provider to divulge records "to any person other than a governmental entity"[89] cannot reasonably be understood as authority for unlimited disclosure of personal information. Rather, it is an exception only to the general criminal prohibition on voluntary disclosure, as the structure of 18 U.S.C. § 2702 makes clear.[90] Furthermore, its provision allowing a provider to divulge records pertaining to its service "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service"[91] is consistent with section 222's provisions allowing a carrier to disclose CPNI in its provision of the telecommunications service from which it is derived or services necessary to, or used in, the provision of such service,[92] "to initiate, render, bill, and collect for ***9622** telecommunications services,"[93] and "to protect the rights or property of the carrier."[94] Finally, we observe that section 222 was enacted in 1996, ten years after the SCA,[95] and therefore CTIA's suggestion that the SCA should carry more weight than the later-enacted statute has no merit.[96]

36. Several commenters urge the Commission to allow industry-developed best practices and codes of conduct to determine the applicable obligations in this context. Doing so, they say, would result in more consistency across related industries and technologies and would enable more flexible approaches.[97] For example, ATIS describes the work of some of its committees that focus on network security, reliability, and privacy. Its Network Reliability Steering Committee has developed Best Practice 8-8-8769, which "notes that service providers should protect such information against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data" and "note that policies for personal information protection should be clearly identified and enforced."[98] The National Telecommunications and Information Administration (NTIA) currently is leading a multistakeholder process, the goal of which is "to develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data."[99] The process emerged from a February 2012 framework issued by the White House, sometimes referred to as the Privacy Blueprint, which set forth a "consumer privacy bill of rights" and envisioned a multistakeholder process to specify how its principles would apply in particular business contexts. The framework urged Congress to provide the FTC and state attorneys general with specific authority to enforce those rights.[100] It noted that companies choosing to adopt a code of conduct would be subject to enforcement by the FTC under that agency's authority to prevent deceptive acts or practices as well as its unfairness jurisdiction.[101] The FTC's authority, however, does not extend to common carriers.[102]

****12** 37. The Commission has statutory responsibilities to enforce the Communications Act, and, although we welcome these other complementary initiatives, none of them is a substitute for the Commission fulfilling its statutory role. Section 222 provides the Commission with a clear directive to protect the privacy of consumers utilizing the communications infrastructure, and the Commission's rules ***9623** implementing section 222 are longstanding, well-known, and judicially tested.[103] The nature of the communications marketplace has changed since the Commission's last pronouncement on CPNI, and thus we act here to affirm our commitment to fulfilling our statutory directive to ensure that carriers are protecting

consumer informationto which they have access because of their unique position as the gatekeeper to their customers' access to the network. By this *Declaratory Ruling*, we clarify that we will apply section 222 and our rules to the type of CPNI described herein to avoid a potential gap in consumers' privacy protections.

IV. ORDERING CLAUSES

38. Accordingly, IT IS ORDERED, pursuant to sections 1, 4, 201, 222, and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154, 201, 222, 303(r), and section 1.2 of the Commission's rules, 47 C.F.R. § 1.2, that this *Declaratory Ruling* in CC Docket No. 96-115 IS ADOPTED.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

***9624 STATEMENT OF ACTING CHAIRWOMAN MIGNON CLYBURN**
****13** *Re: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*,CC Docket No. 96-115.

Protecting consumer privacy is a key component of our mission to serve the public interest. Changes in technology and market practices have raised many new concerns when it comes to privacy. But today's action affirms the Commission's commitment to the protection of wireless consumers by clarifying the FCC's customer proprietary network information — or CPNI — policies.

Consumers rightfully expect that private information — for example, numbers called, the times of those calls, and the locations from which a customer makes those calls — will be safeguarded, whether it's retained on their mobile device, or in a carrier's back-office system. That is why this declaratory ruling clarifies that a carrier has "received or obtained" CPNI when the carrier causes that information to be stored on the deviceand it or its designee has access to or control over that information. Carriers should be responsible for safeguarding the customer information that they collect wherever it's stored. Today's decision ensures that it will be.

It is also worth noting what this Declaratory Ruling does not do. It does not affect third-party app developers or apps that customers might install from an app store. It does not prohibit carriers from collecting information needed to improve networks. In fact, we recognize the benefits of such data collection. However, while there can be benefits to carrier data collection using customers' devices, the fact that such sensitive information is stored on each subscriber's mobile device emphasizes the need to ensure such information is protected. Also, we do not require carriers to implement any particular type of protection. Instead, we allow them to choose their own method of safeguarding CPNI, as long as it provides appropriate protection against unauthorized access. I do want to make clear, however, that if a carrier fails to protect CPNI, the Commission stands ready to use its enforcement authority, including its authority to order forfeitures.

In sum, today's Declaratory Ruling demonstrates that, while technology and consumer behavior evolve, we will continue to exercise our statutory authority to protect consumers. I would like to thank my colleagues for their support of the item, as well as the tireless efforts of Sean Lev, Jennifer Tatel, Douglas Klein, and other members of the Office of General Counsel, for presenting us with such an important item.

***9625 STATEMENT OF COMMISSIONER JESSICA ROSENWORCEL**
Re: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,CC Docket No. 96-115.

It has been over six years since the Commission last updated its customer proprietary network information (CPNI) rules. Think about that. Our last major decision was released before the introduction of the iPhone. Before any one of us thought it was normal to tap on a screen—any screen—and expect an Internet-enabled response based on the swipe of a finger. Before

streaming any video in our palms and laps was even imaginable. Before the applications economy grew to provide 500,000 new jobs. It was a long time ago.

**14 In the intervening years, several trends have collided to make the values that inform our CPNI rules both more important and more complicated.

First, connection is no longer merely convenient. We live in an age of always-on connectivity. We are a nation with more wireless phones than people. One in three adults now has a tablet computer. Our commercial and civic lives are migrating online with ferocious force and speed. Simply put, the opportunity to opt out of this new digital age is limited. Its advances are too bountiful, they save us time and money, and they inform and support all aspects of modern life.

Second, it used to be that the communications relationship was primarily between a customer and his or her carrier. But the number of third parties participating in our digital age connections and transactions has multiplied exponentially. Dial a call, write an e-mail, make a purchase, post an online update to a social network, read a news site, store your family photographs in the cloud, and you should assume that service providers, advertising networks, and companies specializing in analytics have access to your personal information. Lots of it—and for a long time. Our digital footprints are hardly in sand; they are effectively in wet cement.

Third, the monetization of data is big business. The cost of data storage has declined dramatically. The market incentives to keep our data and slice and dice it to inform commercial activity are enormous. They are only going to grow.

Going forward, I think the Commission needs to take note of these trends. They are the impetus, I believe, for last year's Administration blueprint for consumer data privacy in the 21st Century. It is a blueprint I support.

But against this background, we also need to do simple things at the Commission, like enforce our rules.

To this end, in Section 222 of the Communications Act, Congress sought to guard consumers by defining CPNI rights in their relationship with their telecommunications carriers: the right to know what information is being collected about them; the right to get notice when information is being used for other purposes; and the right to be able to stop the reuse or sale of that information. Today's decision advances these principles. It clarifies that our CPNI rules and obligations apply to information that carriers cause to be stored on their customer's devices, like wireless phones. As a result, carriers may only use and disclose such information consistent with our rules. This means wireless carriers must protect CPNI data from unauthorized disclosure and inform subscribers in the event of a security breach.

However, it is also important to be clear about what our decision does not do. Our CPNI *9626 protections at issue in this decision involve carriers. They do not apply to the manufacturers of wireless phones. They do not apply to the developers of operating systems.

**15 So let's be honest. Consumers can be confused by these distinctions. But the scope of this proceeding and Section 222 are limited. So I hope the agency can be proactive and help consumers better understand the different ways their personal data may be collected on a mobile phones, what rules apply, and how they can protect themselves. Furthermore, I think we should take on this task in cooperation with our colleagues at the Federal Trade Commission. Because consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected. We should strive to simplify privacy policies across all platforms and aim for more consistency. But in the interim, it is also essential we enforce our rules. That is what we do here and that is why I am pleased to support this declaratory ruling.

***9627 STATEMENT OF COMMISSIONER AJIT PAI APPROVING IN PART AND CONCURRING IN PART**
Re: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,CC Docket No. 96-115.

The privacy of Americans' phone records is a topic that has been in the news quite a bit lately. But this morning, the Commission tackles a small piece of this subject that hasn't made the headlines. In today's Declaratory Ruling, we seek to clarify both when data stored on a mobile device constitutes customer proprietary network information (CPNI) and when

carriers must protect such CPNI pursuant to section 222 of the Communications Act.

I want to start by thanking my colleagues for their willingness to incorporate many of my suggestions into the item and especially commend Chairwoman Clyburn for her leadership, which was critical in reaching this result. I had serious concerns with the original version of this item. But over the last several days, substantial changes to the Declaratory Ruling have largely allayed those concerns. Therefore, I am voting this morning to approve in part and concur in part.

Four factors are critical to my decision. *First*, I agree that there is no "mobile device exception" to either section 222 or our CPNI rules. If information is covered by the statutory definition of CPNI set forth in section 222(h)(1), then it is CPNI, regardless of whether it is located on a mobile device.

Second, today's Declaratory Ruling is limited in scope. It only applies to information that is both: (1) collected by or at the direction of the carrier; and (2) may be accessed or controlled by the carrier or its designee. If a carrier is not responsible for the collection of certain data, then it may not be held responsible for protecting that data. Likewise, if a carrier doesn't have access to or control over information, then it is not obligated to safeguard it.

**16 *Third*, the Commission provides carriers with maximum flexibility in carrying out their statutory responsibilities with respect to CPNI stored on mobile devices. In today's item, we do not opine on various practices and hypotheticals in the absence of a fully developed factual record and concrete set of facts. Given the complex and quickly evolving technologies at issue, this restraint is wise.

Fourth, and perhaps most important, this Declaratory Ruling does not seek to hold carriers liable for compliance with voluntary codes of conduct under section 201(b) of the Communications Act. I believe the Commission should welcome the development of private-sector solutions to some of the challenges facing the industry. Imbuing such codes of conduct with the force of law, however, would have precisely the opposite effect. Carriers, of course, would be worse off if we changed the meaning of "voluntary" in "voluntary codes of conduct." But consumers ultimately would be worse off too; if we effectively ensure that no good deed goes unpunished, the industry will be less likely to take joint, consumer-friendly action of its own accord.

To be sure, I do not agree with every legal theory set forth in today's item. That's why I am concurring in part. Specifically, I do not join the item's discussion of section 222(c)(1) and in particular its claim that the provision makes a carrier responsible for CPNI that it has neither received nor obtained. On the whole, however, I believe that today's Declaratory Ruling arrives at a reasonable result, one that is fair to both consumers and carriers.

Finally, I would like to thank Sean Lev, Jennifer Tatel, and Doug Klein of the Office of General Counsel as well as Michele Ellison, Dave Grimaldi, and Louis Peraertz in the Office of the Chairwoman *9628 for their hard work on this item, including the fruitful discussions that led to this happy outcome. This item might not receive the same media attention as other recent issues related to privacy, but you deserve public recognition for your efforts.

STATEMENT OF ACTING CHAIRWOMAN MIGNON CLYBURN
Re:*Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, *CC Docket No. 96-115*

Protecting consumer privacy is a key component of our mission to serve the public interest. Changes in technology and market practices have raised many new concerns when it comes to privacy. But today's action affirms the Commission's commitment to the protection of wireless consumers by clarifying the FCC's customer proprietary network information — or CPNI — policies.

Consumers rightfully expect that private information — for example, numbers called, the times of those calls, and the locations from which a customer makes those calls — will be safeguarded, whether it's retained on their mobile device, or in a carrier's back-office system. That is why this declaratory ruling clarifies that a carrier has "received or obtained" CPNI when the carrier causes that information to be stored on the deviceand it or its designee has access to or control over that information. Carriers should be responsible for safeguarding the customer information that they collect wherever it's stored. Today's decision ensures that it will be.

**17 It is also worth noting what this Declaratory Ruling does not do. It does not affect third-party app developers or apps that customers might install from an app store. It does not prohibit carriers from collecting information needed to improve networks. In fact, we recognize the benefits of such data collection. However, while there can be benefits to carrier data collection using customers' devices, the fact that such sensitive information is stored on each subscriber's mobile device emphasizes the need to ensure such information is protected. Also, we do not require carriers to implement any particular type of protection. Instead, we allow them to choose their own method of safeguarding CPNI, as long as it provides appropriate protection against unauthorized access. I do want to make clear, however, that if a carrier fails to protect CPNI, the Commission stands ready to use its enforcement authority, including its authority to order forfeitures.

In sum, today's Declaratory Ruling demonstrates that, while technology and consumer behavior evolve, we will continue to exercise our statutory authority to protect consumers. I would like to thank my colleagues for their support of the item, as well as the tireless efforts of Sean Lev, Jennifer Tatel, Douglas Klein, and other members of the Office of General Counsel, for presenting us with such an important item.

STATEMENT OF COMMISSIONER JESSICA ROSENWORCEL
Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, CC Docket 96-115 (June 27, 2013)

It has been over six years since the Commission last updated its customer proprietary network information (CPNI) rules. Think about that. Our last major decision was released before the introduction of the iPhone. Before any one of us thought it was normal to tap on a screen—any screen—and expect an Internet-enabled response based on the swipe of a finger. Before streaming any video in our palms and laps was even imaginable. Before the applications economy grew to provide 500,000 new jobs. It was a long time ago.

In the intervening years, several trends have collided to make the values that inform our CPNI rules both more important and more complicated.

First, connection is no longer merely convenient. We live in an age of always-on connectivity. We are a nation with more wireless phones than people. One in three adults now has a tablet computer. Our commercial and civic lives are migrating online with ferocious force and speed. Simply put, the opportunity to opt out of this new digital age is limited. Its advances are too bountiful, they save us time and money, and they inform and support all aspects of modern life.

Second, it used to be that the communications relationship was primarily between a customer and his or her carrier. But the number of third parties participating in our digital age connections and transactions has multiplied exponentially.Dial a call, write an e-mail, make a purchase, post an online update to a social network, read a news site, store your family photographs in the cloud, and you should assume that service providers, advertising networks, and companies specializing in analytics have access to your personal information. Lots of it—and for a long time. Our digital footprints are hardly in sand; they are effectively in wet cement.

**18 Third, the monetization of data is big business. The cost of data storage has declined dramatically. The market incentives to keep our data and slice and dice it to inform commercial activity are enormous. They are only going to grow.

Going forward, I think the Commission needs to take note of these trends. They are the impetus, I believe, for last year's Administration blueprint for consumer data privacy in the 21st Century. It is a blueprint I support.

But against this background, we also need to do simple things at the Commission, like enforce our rules.

To this end, in Section 222 of the Communications Act, Congress sought to guard consumers by defining CPNI rights in their relationship with their telecommunications carriers: the right to know what information is being collected about them; the right to get notice when information is being used for other purposes; and the right to be able to stop the reuse or sale of that information. Today's decision advances these principles. It clarifies that our CPNI rules and obligations apply to information that carriers cause to be stored on their customer's devices, like wireless phones. As a result, carriers may only use and disclose such information consistent with our rules. This means wireless carriers must protect CPNI data from unauthorized

disclosure and inform subscribers in the event of a security breach.

However, it is also important to be clear about what our decision does not do. Our CPNI protections at issue in this decision involve carriers. They do not apply to the manufacturers of wireless phones. They do not apply to the developers of operating systems.

So let's be honest. Consumers can be confused by these distinctions. But the scope of this proceeding and Section 222 are limited. So I hope the agency can be proactive and help consumers better understand the different ways their personal data may be collected on a mobile phones, what rules apply, and how they can protect themselves. Furthermore, I think we should take on this task in cooperation with our colleagues at the Federal Trade Commission. Because consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected. We should strive to simplify privacy policies across all platforms and aim for more consistency. But in the interim, it is also essential we enforce our rules. That is what we do here and that is why I am pleased to support this declaratory ruling.

STATEMENT OF COMMISSIONER AJIT PAI APPROVING IN PART AND CONCURRING IN PART
Re: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,CC Docket No. 96-115.

The privacy of Americans' phone records is a topic that has been in the news quite a bit lately. But this morning, the Commission tackles a small piece of this subject that hasn't made the headlines. In today's Declaratory Ruling, we seek to clarify both when data stored on a mobile device constitutes customer proprietary network information (CPNI) and when carriers must protect such CPNI pursuant to section 222 of the Communications Act.

****19** I want to start by thanking my colleagues for their willingness to incorporate many of my suggestions into the item and especially commend Chairwoman Clyburn for her leadership, which was critical in reaching this result. I had serious concerns with the original version of this item. But over the last several days, substantial changes to the Declaratory Ruling have largely allayed those concerns. Therefore, I am voting this morning to approve in part and concur in part.

Four factors are critical to my decision. *First*, I agree that there is no "mobile device exception" to either section 222 or our CPNI rules. If information is covered by the statutory definition of CPNI set forth in section 222(h)(1), then it is CPNI, regardless of whether it is located on a mobile device.

Second, today's Declaratory Ruling is limited in scope. It only applies to information that is both: (1) collected by or at the direction of the carrier; and (2) may be accessed or controlled by the carrier or its designee. If a carrier is not responsible for the collection of certain data, then it may not be held responsible for protecting that data. Likewise, if a carrier doesn't have access to or control over information, then it is not obligated to safeguard it.

Third, the Commission provides carriers with maximum flexibility in carrying out their statutory responsibilities with respect to CPNI stored on mobile devices. In today's item, we do not opine on various practices and hypotheticals in the absence of a fully developed factual record and concrete set of facts. Given the complex and quickly evolving technologies at issue, this restraint is wise.

Fourth, and perhaps most important, this Declaratory Ruling does not seek to hold carriers liable for compliance with voluntary codes of conduct under section 201(b) of the Communications Act. I believe the Commission should welcome the development of private-sector solutions to some of the challenges facing the industry. Imbuing such codes of conduct with the force of law, however, would have precisely the opposite effect. Carriers, of course, would be worse off if we changed the meaning of "voluntary" in "voluntary codes of conduct." But consumers ultimately would be worse off too; if we effectively ensure that no good deed goes unpunished, the industry will be less likely to take joint, consumer-friendly action of its own accord.

To be sure, I do not agree with every legal theory set forth in today's item. That's why I am concurring in part. Specifically, I do not join the item's discussion of section 222(c)(1) and in particular its claim that the provision makes a carrier responsible for CPNI that it has neither received nor obtained. On the whole, however, I believe that today's Declaratory Ruling arrives at

a reasonable result, one that is fair to both consumers and carriers.

****20** Finally, I would like to thank Sean Lev, Jennifer Tatel, and Doug Klein of the Office of General Counsel as well as Michele Ellison, Dave Grimaldi, and Louis Peraertz in the Office of the Chairwoman for their hard work on this item, including the fruitful discussions that led to this happy outcome. This item might not receive the same media attention as other recent issues related to privacy, but you deserve public recognition for your efforts.

Footnotes

1 For purposes of this ruling, a "designee" is an entity to which the carrier has transmitted, or directed the transmission of, CPNI or is the carrier's agent.

2 Carrier IQ, *Understanding Carrier IQ Technology: What Carrier IQ Does and Does Not Do* (Dec. 15, 2011), at 2, *available at* http: // www.carrieriq.com/documents/understanding-carrier-iq-technology/6461/ (*Understanding Carrier IQ Technology*) (last visited June 26, 2013).

3 *See id.* at 8.

4 *See, e.g.*, Letter from The Honorable Al Franken, United States Senate, to Larry Lenhart, President and CEO, Carrier IQ, Inc. (Nov. 30, 2011), *available at* http: //www.franken.senate.gov/files/letter/111201_Letter_to_CarrierIQ.pdf.

5 Section 222 of the Act defines CPNI to mean "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information." 47 U.S.C. § 222(h)(1).

6 *Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, Public Notice, DA 12-818, 27 FCC Rcd 5743 (2012) (*Mobile Device Privacy and Security Public Notice*); *see* 77 Fed. Reg. 35,336 (2012).

7 47 U.S.C. § 222(a).

8 *See* 47 U.S.C. § 222(c); *see also* 47 C.F.R. §§ 64.2001-.2011.

9 *See*47 C.F.R. §§ 64.2001-.2011; *see also, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) (*1998 CPNI Order*); Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002) (*2002 CPNI Order*); Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*).

10 47 C.F.R. § 64.2003(o) (defining "telecommunications carrier" or "carrier," for purposes of the CPNI rules only, to include an

entity that provides interconnected VoIP service as that term is defined in § 9.3); *see2007 CPNI Order*, 22 FCC Rcd at 6954-57 ¶¶ 54-59 (2007). The Commission also earlier this month adopted rules modeled on the CPNI rules in order to apply similar protections to Telecommunications Relay Service and point-to-point video services offered by Video Relay Service providers. *SeeStructure and Practices of the Video Relay Service Program; Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, Report and Order and Further Notice of Proposed Rulemaking, FCC 13-82 ¶¶ 155-172 (2013).

11 47 U.S.C. § 222(h)(1) (defining "customer proprietary network information"); *see also* § 222(f)(1) (requiring express prior authorization of the customer for the use or disclosure of or access to location information).Subsequent to the adoption of section 222(c)(1), Congress added subsection (f). Section 222(f) provides that, for purposes of section 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location information concerning the user of a commercial mobile service or (2) automatic crash notification information of any person other than for use in the operation of an automatic crash notification system. 47 U.S.C. § 222(f).

12 47 U.S.C. § 222(h)(1).

13 *See* 47 U.S.C. § 222(a); § 222(c)(1); 47 C.F.R. §§ 64.2001— .2011.

14 *See2007 CPNI Order*, 22 FCC Rcd at 6930 ¶ 4 (explaining that "[t]he section 222 framework calibrates the protection of [customer information] from disclosure based on the sensitivity of the information").

15 *2007 CPNI Order*, 22 FCC Rcd at 6931 ¶ 4.

16 H.R. Conf. Rep. No. 458, 104th Cong., 2d Sess. 204 (1996) (Joint Explanatory Statement of the Committee of Conference); *see also* H.R. Rep. No. 204, 104th Cong., 1st Sess. 91 (1995); *id.* at 90 (explaining that section 222 balances "the need for customers to be sure that personal information that carriers may collect is not misused" with customers' expectation that "the carrier's employees will have available all relevant information about their service").

17 *1998 CPNI Order*, 13 FCC Rcd at 8080 ¶ 23; 47 C.F.R. § 64.2005.

18 *See* 47 C.F.R. §§ 64.2009-.2011; *e.g., 1998 CPNI Order*, 13 FCC Rcd at 8195-200 ¶¶ 193-202; *2007 CPNI Order*, 22 FCC Rcd at 6933-54 ¶¶ 12-53.

19 47 C.F.R. § 64.2003(o) (defining "telecommunications carrier" or "carrier," for purposes of the CPNI rules only, to include an entity that provides interconnected VoIP service as that term is defined in § 9.3).

20 *See2007 CPNI Order*, 22 FCC Rcd at 6954-57 ¶¶ 54-59.

21 *Id.*at 6928 ¶ 1 n.1.

22 *Id.* at 6934 ¶ 12.

23 *Id.*

24 *Seeid*. at 6929 ¶ 3. Prior to these amendments, carriers could share CPNI with joint venture partners and independent contractors for the purposes of marketing communications-related services after providing only a notice to a customer (i.e., opt-out consent). *Id.* at 6947 ¶ 38.

25 *Id.* at 6962 ¶ 72.

26 Comments of AT&T Inc., CC Docket No. 96-115 (July 9, 2007), at 9, *quoted in Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5744.

27 Comments of Sprint Nextel Corporation, CC Docket No. 96-115 and WC Docket No. 04-36, at 21 (July 9, 2007), *quoted in Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5745.

28 Reply Comments of Sprint Nextel Corporation, CC Docket No. 96-115 and WC Docket No. 04-36, at 14 (Aug. 7, 2007), *quoted in Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5745 n.9.

29 *Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5745-46.

30 *Id.*at 5745.

31 *Understanding Carrier IQ Technology* at 2.

32 *See id.* at Exh. B.

33 *See id.* at 8.

34 *Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5744 & n.7, 5745 & nn. 10-13; Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T Services, Inc., to The Honorable Al Franken, United States Senate (Dec. 14, 2011), *available at* http:// apps.fcc.gov/ecfs/document/view?id=7021920018 (AT&T letter to Sen. Franken); Letter from Vonya B. McCann, Senior Vice President, Government Affairs, Sprint Nextel, to The Honorable Al Franken, United States Senate

(Dec. 14, 2011), *available at* http://apps.fcc.gov/ecfs/document/view?id=7021920019 (Sprint Letter to Sen. Franken); Letter from Thomas J. Sugrue, Senior Vice President, Regulatory and Legal Affairs, T-Mobile USA, Inc., to The Honorable Al Franken, United States Senate (Dec. 20, 2011), *available at* http:// apps.fcc.gov/ecfs/document/view?id=7021920020 (T-Mobile Letter to Sen. Franken).

35 Federal Trade Commission, *HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers*, News Release, Feb. 22, 2013, *available at* http: //www.ftc.gov/opa/2013/02/htc.shtm. The FTC investigated HTC pursuant to its authority to prevent persons subject to its jurisdiction "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(2). That authority includes manufacturers of telecommunications equipment but not common carriers subject to the Act, which are addressed by Title II (including section 222) of the Act.

36 Federal Trade Commission, Agreement Containing Consent Order, *HTC America, Inc.*, File No. 122 3049, at 11, *available at* http: // www.ftc.gov/os/caselist/1223049/130222htcorder.pdf.

37 Verizon Wireless Comments at 9.

38 47 U.S.C. § 222(h)(2) (defining *aggregate information*); § 222(c)(3) (providing that a telecommunications carrier "may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1)"); *see infra* para. 34.

39 47 U.S.C. § 222(c)(1); *see2007 CPNI Order*, 22 FCC Rcd at 6930 ¶ 4.

40 CTIA Comments at 1-2; AT&T Comments at 19 ("Indeed, when a device fails to connect at all, the network will not even know of the failure.").

41 T-Mobile Reply Comments at 5.

42 AT&T Comments at 19; T-Mobile Reply Comments at 6; ITIF Comments at 3.

43 Federal Trade Commission, Complaint, *HTC America, Inc.*, File No. 122 3049, at 4-5, *available at* http:// ftc.gov/os/caselist/1223049/130222htccmpt.pdf.

44 *See, e.g.*, CTIA Comments at 2 ("Consumers are well aware of this practice because carriers clearly and conspicuously disclose that they gather this type of information to improve network performance and the user's experience."); AT&T Comments at 20.

45 47 U.S.C. § 222(h)(1). "Subscriber list information" is defined in § 222(h)(3).

46 *Understanding Carrier IQ Technology*at 9 (stating that recording phone numbers dialed and received "allows a Network Operator to understand both ends of a problem" by, for example, enabling the carrier to determine which customer's device caused a dropped call); *id.* at 4, 11 (explaining the recording and use of location information to diagnose dropped calls or areas with no service).

47 *2007 CPNI Order*, 22 FCC Rcd at 6931 ¶ 5.

48 *See* 47 U.S.C. § 222(h)(1)(A) (defining CPNI to include "information that relates to the ... location ... of a telecommunications service subscribed to by any customer of a telecommunications carrier").

49 47 U.S.C. § 222(h)(1)(A).

50 *See* 47 U.S.C. § 217 (establishing that a common carrier is responsible for the act, omission, or failure of its agent); *see also* Letter from Dale Sohn, President and Chief Executive Officer, Samsung Telecommunications America, LLC, to The Honorable Al Franken, United States Senate (Dec. 14, 2011), at 1, *available at* http: //www.franken.senate.gov/files/letter/111214_ Samsung_Response_to_Sen_Franken_CarrierIQ.pdf (Samsung Letter to Sen. Franken) ("Pursuant to the carriers' agreements with [Samsung], some of those cellular carriers required Samsung to pre-install Carrier IQ software on some of the devices prior to the sale of those devices to the carrier (and before the sale of the devices to the consumer by the distributor, carrier or its agent)."); CDT Comments at 5-6. To the extent that the relationship between carrier, manufacturer, and customer may be different, this principle may not apply.

51 This may also be true if a carrier leverages its control of a customer's device to install such a collection capability after the initial sale, such as through a forced update of the operating system or embedded software.

52 CTIA Comments at 3.

53 We reject any suggestion that we refrain from applying section 222 to information that meets the statutory definition just because some information collected in the same manner does not meet the statutory definition.*See, e.g.*, AT&T Comments at 10-11 ("It would thus not be in the public interest for the Commission to develop a new set of balkanized regulations or declaratory rulings for the small percentage of data stored on mobile devices that falls within the Commission's purview."). Doing so could leave a gap in the privacy and security obligations where section 222, by its terms, applies, leaving consumers unprotected.

54 *See* New America Foundation Reply Comments at 3-6. We find no reason at this time to set out a comprehensive list of data elements that pertain to a telecommunications service and satisfy the definition of CPNI and those data elements that do not.The Commission has never before created such a comprehensive list of CPNI, and we have had no indication that the absence of such a list has caused any significant confusion in the industry. Thus we do not decide today whether or under what circumstances "the locations where customers have problems accessing the network" qualifies as CPNI, *see* CTIA Comments at 8, though we note that location information in particular can be very sensitive customer information.

55 CTIA Comments at 7.

56 CTIA Comments at 8.

57 *See* ITIF Comments at 2 (arguing that the Commission should "continue to limit its authority" to types of information that carriers have historically been able to access about their customers, such as "the amount and type of services used, the destination of communication, the location of the customers, and technical information about the devices used").

58 Verizon Wireless Comments at 7.

59 *See Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5746 (observing that the phrase "'that is made available to a carrier by the customer solely by virtue of the carrier-customer relationship' ... on its face could apply to information collected at a carrier's direction even before it has been transmitted to the carrier" and seeking comment on that analysis).

60 47 U.S.C. § 222(h)(1)(A) (defining CPNI to include "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship").

61 A carrier that receives or obtains CPNI by virtue of its provision of a telecommunications service has obligations as to all "individually identifiable customer proprietary network information." 47 U.S.C. § 222(c)(1). Congress could have limited the obligations imposed by paragraph (c)(1) to the CPNI that the carrier has received or obtained by referring to "such CPNI," but it did not.

62 *See Black's Law Dictionary* 1078 (6th ed. 1990) (defining "obtain" as "[t]o get hold of by effort; to get possession of; to procure; to acquire, *in any way*") (emphasis added).

63 *See* CTIA *ex parte* presentation at 1 (June 19, 2013) ("CPNI requirements only apply to carriers if a carrier directed or caused CPNI to be on a mobile device and that the carrier has access to that CPNI.").

64 *See* 47 U.S.C. § 222(a) (requiring "[e]very telecommunications carrier ... to protect the confidentiality of proprietary information of, and relating to, ... customers").

65 *See, e.g.*,*2007 CPNI Order*, 22 FCC Rcd at 6943 ¶ 27 ("In conjunction with the general rulemaking authority under the Act, section 222(a), which imposes a duty on '[e]very telecommunications carrier ... to protect the confidentiality of proprietary information,' provides ample authority for the Commission to require carriers to report CPNI breaches to law enforcement ...." (footnote omitted)); *id.* at 6952 ¶ 48 ("[A]ll CPNI constitutes sensitive information that is protected under the Communications Act and our rules."); *id.* at6959 ¶ 64& n.198 (citing subsection (a) in support of the expectation that carriers will "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information").

66 For example, according to Carrier IQ, its software is capable of recording information that pertains to the device's access of the carrier's data network, web URLs visited in a browser, and applications installed and used. *See Understanding Carrier IQ*

Technology at Exh. B; *see also* AT&T Comments at 10 ("Section 222 applies by its express terms only to telecommunications carriers. It does not apply to information service providers or other non-carrier entities, nor does it apply to telecommunications carriers when they are not acting in their capacity as such.").

67 *See* CDT Comments at 7-8 (noting that other entities are capable of acquiring similar information).

68 47 U.S.C. § 222(h)(1)(A).

69 47 U.S.C. § 222(h)(1)(A).

70 47 U.S.C. § 222(a).

71 *See* 47 U.S.C. § 222(c)(1).

72 *See2007 CPNI Order*, 22 FCC Rcd at 6959-60 ¶¶ 63-66; *see also* 47 C.F.R. § 64.2010(a) ("Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.").

73 *2007 CPNI Order*, 22 FCC Rcd at 6959-60 ¶¶ 63-66. In this regard, we note that the Commission has said, for example, that it "expect[s] a carrier to encrypt its CPNI databases if doing so would provide significant additional protection against the unauthorized access to CPNI at a cost that is reasonable given the technology a carrier already has implemented." *Id.* at 6959 ¶ 64.

74 *See, e.g.*, CTIA Comments at 4-5; Verizon Wireless Comments at 2-4.

75 *See generally* Federal Communications Commission, *Location-Based Services: An Overview of Opportunities and Other Considerations* (May 2012), *available at* http://www.fcc.gov/document/location-based-services-report; *see also*Roger Entner, Recon Analytics, *The Wireless Industry: The Essential Engine of U.S. Economic Growth* (May 2012), *available at* http://reconanalytics.com/wp-content/uploads/2012/04/Wireless-The-Ubiquitous-Engine-by-Recon-Analytics-1.pdf.

76 47 U.S.C. § 222(c)(1).

77 47 U.S.C. § 222(d)(1), (2).

78 *See generally* 47 C.F.R. § 64.2005 ("Use of customer proprietary network information without customer approval."). Commenters emphasize that this use of network diagnostic information collected from wireless devices benefits consumers. *See, e.g.*, CTIA Comments at 8.

79 Verizon Wireless Comments at 8; *see also id.* at 9 (arguing that "certain uses of information would not warrant customer consent, such as information used for monitoring network performance; many other types of more sensitive uses, however, would warrant notice and consent," though also arguing that "[b]est practices or codes of conduct ... are the best methods for addressing these issues").

80 47 C.F.R. § 64.2005(b)(1); *see1999 CPNI Order*, 14 FCC Rcd at 14430-35 ¶¶ 39-47 (finding that the phrase "services necessary to, or used in, the provision of such telecommunications service" includes customer-premises equipment and certain information services).

81 *See supra* para. 17.

82 47 U.S.C. § 222(h)(2).

83 47 U.S.C. § 222(c)(3). For a local exchange carrier, such use of aggregate customer information is subject to a requirement that it provide the information on a nondiscriminatory basis to other persons upon reasonable request. *Id.*; *see1998 CPNI Order*, 18 FCC Rcd at 8165-71 ¶¶ 143-153.

84 *1998 CPNI Order*, 13 FCC Rcd at 8169 ¶ 149.

85 *See* AT&T Comments at 20 n.56.

86 47 U.S.C. § 222(a), (c)(1).

87 18 U.S.C. §§ 2701-2712.

88 CTIA Comments at 3; *see id.* at 10-11.

89 18 U.S.C. § 2702(c)(6).

90 If the SCA were read as authorizing unlimited disclosure of personal information notwithstanding other provisions of law, as CTIA appears to be suggesting, it would nullify section 222 in nearly all respects, not just in the context of CPNI collected by mobile devices. It clearly does not do so. Courts have confirmed that section 222 restricts the use, disclosure, and permission of access to CPNI. *SeeNational Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (upholding the Commission's opt-in requirement for disclosure of CPNI to a carrier's joint-venture partner or independent contractor for the purposes of marketing communications-related services to that customer).

91 18 U.S.C. § 2702(c)(3).

92 47 U.S.C. § 222(c)(1).

93 47 U.S.C. § 222(d)(1).

94 47 U.S.C. § 222(d)(2).

95 *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 702, 110 Stat. 56, 148-49 (adding new section 222 to Title II of the Communications Act of 1934).

96 *SeeFDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133, 143 (2000) ("[T]he meaning of one statute may be affected by other Acts, particularly where Congress has spoken subsequently and more specifically to the topic at hand."); CTIA Comments at 10 & n.30 (citing *FDA v. Brown & Williamson Tobacco Corp.*) (noting that the meaning of one statute may be affected by others, particularly subsequent enactments).

97 *See, e.g.*, CTIA Comments at 5-6; Consumer Electronics Association Comments at 11-13; AT&T Comments at 8-13; ITIF Comments at 4.

98 ATIS Comments at 3; *see*Protection of Personally Identifiable Information (PII), NRIC Best Practice No. 8-8-8769, *available at* http: // www.atis.org/bestpractices/BPDetail.aspx?num=8-8-8769.

99 *See* National Telecommunications and Information Administration, *Privacy Multistakeholder Process: Mobile Application Transparency, available at* http: //www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency. We note that this first multistakeholder process is focused on developers of mobile applications and not on the obligations of telecommunications carriers.

100 The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012) (*White House Privacy Blueprint*), *available at* http: // www.whitehouse.gov/sites/default/files/privacy-final.pdf.

101 *See id.* at 27 & n.32.

102 *See* 15 U.S.C. § 45(a)(2); *see also supra* para. 15 & n.35.

103 *See* *National Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009).

28 FCC Rcd. 9609 (F.C.C.), 28 F.C.C.R. 9609, 58 Communications Reg. (P&F) 739, 2013 WL 3271062

29 FCC Rcd. 13325 (F.C.C.), 29 F.C.C.R. 13325, 61 Communications Reg. (P&F) 652, 2014 WL 5439575

Federal Communications Commission (F.C.C.)
Notice of Apparent Liability for Forfeiture

IN THE MATTER OF TERRACOM, INC. AND YOURTEL AMERICA, INC.
Apparent Liability for Forfeiture

File No.: EB-TCD-13-00009175
NAL/Acct. No.: 201432170015
FRNs: 0010103745 and 0020097572
FCC
14
-
173
Released: October 24, 2014
Adopted: October 24, 2014

***1** By the Commission: Chairman Wheeler and Commissioner Clyburn issuing separate statements; Commissioners Pai and O'Reilly dissenting and issuing separate statements.

I. INTRODUCTION

1. The Commission is committed to protecting the sensitive personal information of American consumers from misappropriation, breach, and unlawful disclosure. Today, we take action against two companies that collected names, addresses, Social Security numbers, driver's licenses, and other proprietary information (PI) belonging to low-income Americans and stored them on unprotected Internet servers that anyone in the world could access with a search engine and basic manipulation. The companies stored such consumer PI in two publicly accessible folders on the Internet without password protection or encryption. By not employing appropriate or even reasonable security measures, the companies exposed their customers to an unacceptable risk of identity theft and other serious consumer harms.

2. We find that TerraCom, Inc. (TerraCom) and YourTel America, Inc. (YourTel) (collectively, the Companies) apparently willfully and repeatedly violated the law when they allegedly: (i) failed to properly protect the confidentiality of consumers' PI they collected from applicants for the Companies' wireless and wired Lifeline telephone services; (ii) failed to employ reasonable data security practices to protect consumers' PI; (iii) engaged in deceptive and misleading practices by representing to consumers in the Companies' privacy policies that they employed appropriate technologies to protect consumers' PI when, in fact, they had not; and (iv) engaged in unjust and unreasonable practices by not fully informing consumers that their PI had been compromised by third-party access. Based on our review of the facts and circumstances surrounding these apparent violations of Sections 201(b) and 222(a) of the Communications Act of 1934, as amended (Communications Act or Act) and our rules, we propose a forfeiture of $10,000,000.

II. BACKGROUND

3. Both TerraCom and YourTel are common carriers providing telecommunications services as part of the Lifeline program.[1] TerraCom provides prepaid local, intrastate, and interstate telecommunications services to low-income residential customers in Oklahoma and Texas. TerraCom is a certified competitive local exchange carrier and wireline eligible telecommunications carrier (ETC).[2] TerraCom is also a wireless ETC for Lifeline services in fourteen states, Puerto Rico, and the Virgin Islands.[3] YourTel provides wireless Lifeline telephone service as an ETC in eight states, and wireline Lifeline service in three.[4]

TerraCom and YourTel have common shareholders, share key management employees,[5] and are joint owners of a third company, BrightStar Global Solutions, LLC (BrightStar),[6] but are separate corporate entities headquartered in Oklahoma and Missouri, respectively.[7]

***2** 4. Low income consumers who wish to obtain Lifeline services provided by TerraCom or YourTel are required to submit information and documents demonstrating that they have an income that is at or below 135% of the federal Poverty Guidelines, or that they participate in one or more of several state and federal government assistance programs (such as Medicaid, Supplemental Nutrition Assistance Program (SNAP), public housing assistance, and others). Applicants must submit, among other things, their name and address, date of birth, Social Security Number, and driver's license or state ID card. In addition, in order to determine income eligibility for Lifeline service, the Companies collect additional information from applicants, such as their annual statement of government benefits; the prior year's state, federal or Tribal tax return; paycheck stubs; Social Security benefit statements; Veterans Administration benefit statements; retirement or pension information; Unemployment or Workers' Compensation benefit statements; Federal or Tribal notice letters of participation in General Assistance; divorce decrees or child support awards; or other official documents establishing the applicant's income level.[8]

5. Applicants for the Companies' services submitted PI on electronic application forms and supplemented the applications with scanned images of PI-laden supporting documentation (described above) to establish proof of eligibility. The Companies collected this information through their respective websites and, through BrightStar, their commonly owned contracting company, retained CallCenters India, Inc., d/b/a Vcare Corporation (Vcare), to provide them with call center, back office support systems, hosted billing, and other services to support their Lifeline offerings.[9] Part of the "hosted" services that the Companies' purchased from Vcare included software and electronic storage on dedicated data servers to house the collected documents and applications. From September 30, 2012, through April 26, 2013, the Companies stored these electronic forms and scanned documents on Vcare's servers in ***.[10] The Companies stored the PI-containing documents in clear, readable text and in electronic format accessible via the Internet.

6. In early 2013, an investigative reporter working for Scripps Howard News Service (Scripps) discovered that the Companies were storing PI and documents submitted by low income Lifeline service applicants on an unprotected Internet site. Between March 24, 2013, and April 26, 2013, Scripps accessed at least 128,066[11] confidential records and documents submitted by subscribers and applicants for the Companies' services.[12] Scripps located a consumer's data file by conducting a simple Google search.[13] Once it had located a single file, Scripps shortened that file's URL and obtained access to the entire directory of applicant and subscriber data.[14] On April 26, 2013, Scripps alerted the Companies that it had accessed their servers and had retrieved the PI of subscribers and applicants stored there.[15]

***3** 7. On April 30, 2013, TerraCom and YourTel sent a "cease and desist" letter to Scripps, referring to Scripps' reporters as "hackers" who had illegally accessed "directories on Vcare's servers that contained all of the Lifeline applications processed by Vcare since April 2012."[16] According to the letter, between March 24, 2013, and April 26, 2013, Scripps employees downloaded at least 19,000 applications for Lifeline service and 127,000 files containing eligibility/income documentation.[17]

8. On May 7, 2013, the Companies contacted the Enforcement Bureau (Bureau), about the data breach.[18] TerraCom and YourTel claimed that the Companies "were victims of a security breach resulting from unauthorized access to personal data by an investigative reporter from [Scripps]."[19] TerraCom and YourTel stated that the compromised data belonged to "applicants seeking enrollment in the Lifeline program."[20] Additionally, the evidence shows that 343 records "were viewed by unknown, and potentially unauthorized, individuals."[21]

9. Ten days after alerting the Enforcement Bureau to Scripps' access to the data, the Companies sent a letter to the FCC's Wireline Competition Bureau to explain that their service provider, Vcare, was retaining ***.[22]

10. On June 17, 2013, the Bureau sent a letter of inquiry (LOI) jointly to TerraCom and YourTel directing each company to provide information regarding the reported security breach, among other tilings.[23] The Companies provided their response on July 17, 2013.[24]

III. DISCUSSION

11. As discussed at length below, Section 222(a) imposes a duty on TerraCom and YourTel to protect the confidentiality of this information.[25] Likewise. Section 201(b) of the Act requires TerraCom's and YourTel's practices related to such information and consumers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.[26]

12. As discussed more fully below, we charge TerraCom and YourTel with apparently violating (1) Section 222(a) of the Act for failing to protect the confidentiality of PI that consumers provided to demonstrate eligibility for Lifeline telecommunications services; (2) Section 201(b) of the Act by failing to employ reasonable data security practices to protect consumers' PI; (3) Section 201(b) of the Act by representing in their privacy policies that they protected customers' personal information, when in fact they did not; and (4) Section 201(b) of the Act by failing to notify all customers whose personal information could have been breached by the Companies' inadequate data security policies.
· TerraCom and YourTel apparently violated Section 222(a) of the Act for failing to protect the confidentiality of PI that consumers provided to demonstrate eligibility for Lifeline services. The Companies collected consumers' PI through the Companies' websites[27] and until April 26, 2013, stored, or their vendor stored, this PI in clear, readable text on one or more servers in *** that were accessible via the Internet.

**4 · By failing to employ reasonable data security practices to protect consumers' PI, the Companies also engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) of the Act. They failed to use even the most basic and readily available technologies and security features and thus created an unreasonable risk of unauthorized access.

· TerraCom and YourTel also apparently violated Section 201(b) of the Act by representing in their privacy policies that they protected customers' personal information, when in fact they did not. The Companies' privacy policies and statements on their websites inform consumers that they have "implemented technology and security features to safeguard the privacy of your customer specific information from unauthorized access or improper use" and that they "continue to enhance its security measures as technology becomes available."[28] The evidence shows, however, that TerraCom and YourTel, in fact, collected PI through their websites and failed to employ reasonable practices to safeguard this information as they represented, expressly or by implication, in their privacy policies.

· Finally, we find that the Companies engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) by failing to notify all customers whose personal information could have been breached by the Companies' inadequate data security policies. The Companies exposed over 300,000 consumers to potential data security breaches through their lax and virtually non-existent security practices. When learning that a security breach had occurred, the Companies failed to notify all potentially affected consumers and thereby deprived them of any opportunity to take steps to protect their PI from misappropriation by third parties.

Each of the above charges is discussed more fully below.

A. TerraCom and YourTel Apparently Violated Section 222(a) of the Communications Act By Breaching Their Statutory Duty to Protect the Privacy of Proprietary Information

13. We find that TerraCom and YourTel apparently willfully and repeatedly violated Section 222(a) of the Act. Section 222(a) imposes a duty on every telecommunications carrier "to protect the confidentiality of proprietary information of, and relating to ... customers."[29] The Commission has made clear that section 222(a) requires carriers to "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information"[30] and that it was "committing to taking resolute enforcement action to ensure that the goals of section 222 are achieved."[31] As discussed below, the information that TerraCom and YourTel collected from consumers when applying for their Lifeline services was "proprietary information of, and relating to" their customers. The evidence shows that TerraCom and YourTel failed to fulfill their duty to protect that information.

1. The Information TerraCom and YourTel Collected from Consumers was """"Proprietary Information" Under Section 222(a)

**5 14. Congress added Section 222—entitled "Privacy of Customer Information"—to the Communications Act as part of the Telecommunications Act of 1996.[32] Section 222(a) of the Communications Act imposes a duty on every telecommunications carrier to protect the confidentiality of "proprietary information" of its customers. In the context of Section 222, it is clear

that Congress used the term "proprietary information" broadly to encompass all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy. That meaning is clear from how the word "privacy" is used in the section heading and in the heading of paragraph (c)(1), which, although it refers to "customer proprietary network information," is titled "Privacy requirements for telecommunications carriers." We therefore interpret ""proprietary information" in Section 222(a), as applied to customers, as clearly encompassing private information that customers have an interest in protecting from public exposure. The Commission has consistently interpreted Section 222(a) as requiring telecommunications carriers to protect sensitive private information,[33] and we affirm that view here.

15. It is also clear that the scope of "proprietary information" protected by Section 222(a) is broader than the statutorily defined term "customer proprietary network information" (CPNI). Had Congress wanted to limit the protections of subsection (a) to CPNI, it could have done so. This interpretation of Section 222(a) is consistent with other provisions of the Communications Act that use the term "proprietary information." In the context of public broadcasting, for example, the Corporation for Public Broadcasting (CPB) must maintain for public inspection certain financial information about programming grants. But Congress also recognized that "proprietary, confidential, or privileged information" should not be made public, and Congress thus expressly excluded such information from public disclosure.[34] Similarly, in the context of establishing rules for fair competition in the telephone equipment manufacturing market in 1996, Congress added non-discrimination rules applicable to standards-setting and certification entities that review telephone equipment for interoperability and engineering purposes. Recognizing that such entities necessarily gain access to extremely valuable trade secrets, Congress explicitly prohibited those review entities from "releasing or otherwise using any proprietary information" belonging to the manufacturer without written authorization.[35]

16. The overarching principle is that we should interpret the term ""proprietary information" in the commonly understood sense of information that should not be exposed widely to the public, so when applied to information about individuals, the term must include personal data that customers expect their carriers to keep private,[36] including information a carrier may possess that is not subject to the additional restrictions afforded to carrier treatment of CPNI.[37]

***6** 17. As evidenced by the foregoing examples, the term "proprietary information" in Section 222(a) broadly encompasses such confidential information as privileged information, trade secrets, and personally identifiable information (PII). In general, PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Additionally, while we do not formally adopt it here, we find the definition of PII used by the National Institute of Standards and Technology (NIST) to be informative. Under the definition used by NIST, PII is "(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[38]

18. In the context of Lifeline service at issue here, "proprietary information" includes all documentation submitted by a consumer or collected by an ETC to determine a consumer's eligibility for Lifeline service, as well as all personally identifiable information contained therein. Specifically, information such as a consumer's (i) first and last name; (ii) home or other physical address; (iii) email address or other online contact information, such as an instant messaging screen name that reveals an individual's email address; (iv) telephone number; (v) Social Security Number, tax identification number, passport number, driver's license number, or any other government-issued identification number that is unique to an individual; (vi) account numbers, credit card numbers, and any information combined that would allow access to the consumer's accounts; (vii) Uniform Resource Locator ("URL") or Internet Protocol ("IP") address or host name that identifies an individual; or (viii) any combination of the above, constitutes "proprietary information" protected by Section 222(a).

19. In recognizing the application of "proprietary information" in this way, we maintain the high expectations for protection that the Commission has previously articulated in other Lifeline orders. In a rulemaking order creating the National Lifeline Accountability Database, which now receives and processes from ETCs the same type of sensitive information about consumers that is at issue here, the Commission identified subscriber eligibility information as sensitive personal information.[39] Specifically, in the *Lifeline Reform Order* the Commission identified Lifeline program enrollment information as ""particularly sensitive information" that "must be subject to the highest protections."[40] Just as the Commission recognized the sensitivity of this type of information in designing its own protections, to satisfy their duty under Section 222(a) to protect the confidentiality of customers' PI, carriers should know that they must likewise subject such information to the highest

protections.

***7** 20. The information that the Companies collected falls squarely within the definition of "proprietary information" described above. A sampling of that information includes "completed Lifeline application forms that contain the names, addresses, social security numbers and telephone numbers of applicants ... [and] account numbers for government programs."[41] The "[d] ata accessed also included copies of 'Proof Documents' demonstrating each applicant's eligibility for the Lifeline program ... [which] included driver's licenses, benefits statements, benefit program cards, tax forms and other government forms."[42] Thus, we find that the eligibility information the Companies collected falls within the statutory protections afforded consumers under Section 222(a).

2. Lifeline Applicants Provided the Companies with Information that was """"Relating to ... Customers" Under Section 222(a)

21. The Lifeline eligibility information that TerraCom and YourTel collected related to the Companies' customers. The Companies argue that they collected the eligibility information merely from *applicants* seeking service and that applicants are not "customers" for which a duty arises under Section 222(a). Further, the Companies argue that a portion of these "applicants" were rejected and never became customers.[43] The essence of the Companies' argument is that a carrier's duty to protect a consumer's PI under Section 222(a) is not triggered unless and until that consumer becomes an actual subscriber of service. We disagree.

22. First, consumers applying for telecommunications services have a reasonable expectation that the carrier will protect the confidentiality of the PI they provide as part of that transaction. This is especially true in the Lifeline context where carriers offer a subsidized service pursuant to a government program that requires collection of PI to determine eligibility. The fact that our rules require carriers to collect PI and determine eligibility for Lifeline service *before* providing the service (i.e., before the consumer becomes a subscriber) does not change the consumers' expectations or the carrier's duty under Section 222(a) to protect consumers' PI.[44] This is no different, for example, than a consumer entering a wireless carrier's retail store and applying for service. As part of the transaction, the clerk typically asks the consumer to divulge his or her name, address, and credit card information, among other things. In handing over that information, the consumer places trust and confidence in the carrier to protect his or her privacy and the customer relationship is established for purposes of Section 222(a).[45]

23. Moreover, the Commission has recognized the applicability of privacy laws, including Section 222(a), at the pre-subscriber stage of a transaction. In the *Lifeline Reform Order* the Commission discussed carriers' responsibility to determine eligibility and recognized that to satisfy this obligation, they would collect information about prospective customers that is particularly sensitive at the application stage.[46] The Commission drew no distinction between an applicant for service and a subscriber. Thus, we find that the carrier/customer relationship commences when a consumer applies for service. The duty to protect the confidentiality of PI is triggered when the carrier accepts confidential private information as part of that transaction.

***8** 24. Additionally, the Companies themselves recognize that applicants for their services are "customers." Both TerraCom and YourTel invite consumers to apply for Lifeline service on their websites, and draw absolutely no distinctions between "applicants" and "customers." Both TerraCom and YourTel require applicants to complete a "Lifeline Certification Form" and to provide information sufficient to prove eligibility. The Companies' Lifeline Certification Form identifies persons completing the form (i.e., persons applying for Lifeline service) as "customers." In fact, the Companies use """"customer" on every applicable section of the form, including the certification and signature block ("Customer Signature"). TerraCom and YourTel cannot have it both ways. They cannot invite consumers to apply for Lifeline services and upload PI on their respective websites, ignoring any distinctions on one hand, and then on the other hand, argue that the Lifeline eligibility documents these very same consumers were invited to upload are not PI and should not be protected because the applicants are not customers.

25. Further, in their privacy policies the Companies draw no distinction between "applicants" and "customers." By way of example, the Companies invite each applicant for Lifeline service to upload his or her eligibility documents directly from their privacy policy page on their websites. The Companies' privacy policies assure those persons submitting "[c]ustomer specific information" through their website that they will protect that information and, in fact, inform such applicants that "[b]y providing us with your information, you acknowledge that you have read this privacy policy, understand it, agree to its

terms and consent to the transfer of such information outside your resident jurisdiction."[47] Based on the forgoing, any consumer acting reasonably under the circumstances, when confronted with the paperwork and privacy policy provided by each company for completing an application, would certainly understand himself or herself to be a customer of TerraCom or YourTel at the application stage prior to becoming a subscriber.[48] Indeed, under the Companies' logic, a mere "applicant" would be consenting to a privacy policy that does not even apply to a person with that status; in other words, if applicants are not customers, there would be no point in asking such persons to agree to something that is irrelevant to them.

26. Third, for the reasons discussed above and to give effect to the purpose of Section 222(a), we interpret "customer" to include both an applicant for service and a subscriber of the service.[49] Sections 222(a), (b), and (c) protect three types or categories of confidential information: (1) subsection (a) protects "proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunications carriers reselling telecommunications services provided by a telecommunications carrier;"[50] (2) subsection (b) protects proprietary information that a carrier receives or obtains "from another carrier" (i.e., carrier information);[51] and (3) subsection (c) protects "customer proprietary network information" or CPNI.[52] Section 222(a) is the broadest of the three subsections and encompasses the other two.[53] While both subsections (a) and (c) use the term "customer," we read them flexibly to give effect to the information each subsection seeks to protect.[54]

***9** 27. In this regard, subsection (c) protects customers' CPNI and subsection (a) imposes a duty on carriers to protect customers' PI. The statute defines CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and ... information contained in the bills pertaining to ... service received by a customer of a carrier."[55] The statute's use of the term "customer" in this context is integrally tied to the service purchased by a consumer. Thus, consistent with the CPNI definition, our rules define "customer" as "a person or entity to which the telecommunications carrier is currently providing service."[56] Subsection (a)'s protections, however, are broader than CPNI and impose a duty on carriers to protect PI that a carrier obtains both at the application stage when a consumer provides the carrier with such information and reasonably relies on the carrier to protect his or her PI, as well as after the consumer becomes a subscriber.[57] Thus, our inclusion of applicants in the definition of customer in the context of Section 222(a) gives effect to the broader duty and privacy protections.

28. We therefore find that a plain and practical reading of the protections afforded to consumers' PI under Section 222(a) requires us to interpret the statute's reference to "customer" to include applicants as well as subscribers of a telecommunications service. Having found that Section 222(a) applies, we conclude that TerraCom and YourTel had a duty to protect the confidentiality of the PI given to them by consumers.

3. TerraCom and YourTel Apparently Breached Their Duty Under Section 222(a) to Protect Lifeline Data Belonging to Their Customers

29. The evidence shows that the Companies' security measures lacked even the most basic features to protect consumers' PI. According to Scripps and Sensei Enterprises, Inc., a company hired by the Companies to investigate the breach, the PI hosted by Vcare on its server was widely available on public websites online through a simple Google search.[58] The Enforcement Bureau independently confirmed that search engines had, in fact, not only found TerraCom's applications containing PI but downloaded and archived at least two such applications and posted them openly on the Internet. The applications remained available to anyone using the Internet as late as June 30, 2014.[59] The Companies knew or should have known that the use of random URLs without more (e.g., encryption) to protect applicant records provided inadequate security and left the documents vulnerable to exposure via search engines—which operate by visiting websites, indexing all or much of the content available on them, and then delivering links to the indexed results to anyone that queries the engine.[60]

***10** 30. By not employing appropriate security measures, TerraCom and YourTel exposed their customers to potentially substantial injury. The exposed PI—in particular, financial information and Social Security numbers—invites identify theft and other serious consumer harms. Further, the Companies' choice to store, or its vendor's choice to store, files containing the PI of customers in a publicly accessible folder on the Internet, without password protection or encryption, is the practical equivalent of having provided no security at all. Based upon the foregoing, we find that TerraCom and YourTel collected PI submitted by consumers and failed to provide adequate protection of the PI in apparent violation of Section 222(a) of the Act.

B. The Companies Failed to Employ Just or Reasonable Data Security Practices to Protect Consumers' Proprietary Information in Apparent Violation of Section 201(b)

31. TerraCom and YourTel's failure to protect and secure the PI of their customers also constitutes an unjust and unreasonable practice in apparent violation of Section 201(b) of the Act. Section 201(b) of the Act states, in pertinent part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio]. shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."[61]

32. We find the Companies' data security practices unjust and unreasonable for at least two reasons. First, the Companies failed to employ even the most basic and readily available technologies and security features for protecting consumers' PI. As discussed above, consumers' PI was stored on servers that were accessible over the public Internet. The Companies stored, or their vendor stored, this information in clear, readable text on one or more servers in *** that were accessible to anyone using a simple search technique. The data was not password protected or encrypted;[62] in fact, the Companies' agreement with its vendor Vcare ***.[63] As we said in the context of protecting CPNI—a subset of "proprietary information"—'Fcarriers' existing statutory obligations to protect their customers' CPNI include a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI."[64] We do not hold here that encrypting without more would satisfy a carrier's duty under Section 222(a) or render a carrier's data security practices just and reasonable under Section 201(b); however, given the state of the technology, we believe the lack of encryption clearly evidences the unjust and unreasonable nature of the Companies' data security practices.

33. Secondly, the Companies' data security practices created an unreasonable risk of unauthorized access. As discussed above, the Companies used random URLs to protect their customers' PI. Further, the Companies' URL naming convention for one of the folders containing PI that was stored on Vcare's server also exposed the names of the applicants or customers directly in the URL. further demonstrating the lack of security of the records.[65] In relevant part, the Sensei Forensic Report states:
***11** ***

***

***[66]

In other words, the companies used URLs that contained the names of Lifeline applicants in plain text. This made it exceptionally easy to locate the confidential files to which the URLs pointed by conducting a simple Google search for names.[67]

34. The evidence shows that the Companies' data security practice of using these naming conventions was wholly insufficient to protect consumers' PI. In fact, the evidence shows that as a result of the Companies' practices, between March 24, 2013 and April 26. 2013.[68] Scripps accessed and downloaded approximately 128.066 proprietary records.[69] Further, after the breach, the Companies hired a digital forensics consultant (Sensei) to investigate the breach. Sensei traced some of the ***[70] Additionally, the evidence shows that a number of the IP addresses that accessed this data were from foreign countries, including Russia. China. Ukraine. Norway. Poland, and Slovenia.[71] reported that at least ***, all from ***, and described this as ""***."[72] These countries are often identified as hot spots for identity theft.[73]

35. In light of the Companies' practices related to their lack or near lack of any data security and the magnitude or potential for harm when consumer's PI is accessed (e.g., identify theft), we find the Companies' data security practices unjust and unreasonable in apparent violation of Section 201(b) of the Act.[74]

C. TerraCom and Your Tel Engaged in Deceptive Practices by Misrepresenting Their Security Measures to Consumers in Apparent Violation of Section 201(b) of the Act

36. Since approximately September 30, 2012, TerraCom and YourTel have disseminated privacy policies and statements on

their respective websites that represent expressly or imply that they employ reasonable security measures to protect the private information of customers signing up for service on their websites. The Companies also represent that they continually update these measures to incorporate the latest technologies as they became available. For example. TerraCom made the following representation to consumers via its privacy policy at the time that it was storing PI on unsecured Internet servers in *** and ***:

TerraCom Wireless has implemented technology and security features to safeguard the privacy of your customer specific information from unauthorized access or improper use and will continue to enhance its security measures as technology becomes available. Unfortunately, there is no such thing as foolproof security on the internet, and therefore. TerraCom Wireless makes no guaranties with regard to the sufficiency of our security measures.[75]

YourTel had identical language on its website.[76]

37. As discussed above, the evidence proves that no such safeguards were in place for prospective customers' Lifeline applications.[77] The Companies, in fact, employed virtually no technology or security features for this information—other than what the Companies assert were complicated URLs and passwords when their own employees sought to access the data through a dedicated portal.[78] Further, the Companies did not implement or otherwise ""enhance" (as promised in their privacy policies) security measures and technologies until they were informed of a data security breach.[79] The Companies informed the Enforcement Bureau that, sometime after April 26. 2013, they instructed Vcare to: (i) use a "***"; (ii) restrict "***"; (iii) assign """***"; (iv) use a "***"; and (v) ***.[80]

***12** 38. Thus, we find the Companies' representations in their privacy policies were false, deceptive, and misleading to consumers who gave TerraCom and YourTel personal and private information as part of their application for the Companies' Lifeline service. We also find the Companies' disclaimers, when read in context (i.e.. immediately following clear and unambiguous language representing that the Companies had implemented the necessary security features to protect private information), wholly ineffective and misleading as well.[81] The Commission has previously found that deceptive practices are unjust and unreasonable practices that violate Section 201(b) of the Act.[82] Accordingly, we find TerraCom's and YourTel's practices unjust and unreasonable in apparent violation of Section 201(b).[83]

D. TerraCom and YourTel Engaged in Unjust and Unreasonable Practices by Failing to Notify all Consumers Affected by the Security Breach in Apparent Violation of Section 201(b) of the Act

39. The Companies initially told the Commission that all of the subscribers or potential subscribers whose personal information had been exposed were notified of the security breach. The evidence, however, shows that TerraCom and YourTel only notified 35,129 of the over 300,000 persons whose data was exposed.[84] The Companies state that these notices were provided based on the "state-specific notification requirements for the state of residence of the affected applicant."[85] We find the Companies' notification of anything less than all potentially affected consumers unjust and unreasonable, in violation of Section 201(b) of the Act. We find the Companies' failure to notify all affected consumers of the breach unjust and unreasonable because it left consumers ignorant about the risks of identity theft problems that may occur due in whole or part to the breach—a problem made even more troubling in light of the Companies' admission that they do not know the extent or breadth of the breach.

40. The Companies' practices of limited notification when a data security breach occurs— exposing PI to potential harms such as identify theft—were unjust and unreasonable. TerraCom and YourTel stored the PI of approximately 305,000 customers in an unsecure manner, open to easy access by third parties.[86] The Companies admit that a data breach occurred.[87] The Companies' best guess of the extent of records containing PI accessed by unauthorized third-parties is 128,066 records. The Companies admit, however, that they do not know how many records were accessed between September 2012 and April 2013— the 128.066 number is just an estimate.[88]

41. Moreover, the Companies' estimate has been an evolving story. The Companies initially told Staff in May 2013. and reiterated in June 2013, that "343 individuals had their records accessed."[89] By November 2013 the Companies "best estimate" was up to 128.066.[90] Sensei identified *** as having *** and that overall Sensei was not able *** to determine "***", the SenSei Forensic Report further identified at least ***, as well as ***.[9192] " In addition, the evidence shows that there are IP addresses accessing the Vcare server from China, the Ukraine. Poland, Russia, and Norway, among others.[93] The

Companies speculate that these and other IP addresses cannot be confirmed because they could be accessed by their employees or other authorized personnel using home computers and other devices outside the office.[94] We do not find the Companies' explanations credible. The evidence overwhelmingly shows that the Companies simply do not know how many records containing customer PI were accessed by unauthorized third parties. In fact, because web crawlers were able to access the PI stored on Vcare's servers, it is highly unlikely that the Companies will ever have a full understanding of how many files were accessed.

***13** 42. During the investigation. Staff found two TerraCom customer applications that a web crawler had retrieved, archived, and made publically available online.[95] While Staff contacted the web service and requested that these applications be taken down, Staff did not undertake a comprehensive search of other web-crawler sites. The absence of any Company notification concerning these applications and the fact that they remained exposed to anyone using the Internet as late as June 27, 2014, leads us to believe that the Companies were completely unaware of these security breaches.

43. Because all of the records stored on Vcare's servers between September 2012 and April 26, 2013 were at risk, we find that TerraCom and YourTel acted unjustly and unreasonably by failing to notify all customers whose Lifeline enrollment information was exposed to actual and potential data security breaches (i.e., stored on Vcare's servers during this time).[96] We expect carriers to act in an abundance of caution—even to the extent of being overly inclusive—in their practices with respect to notifying consumers of security breaches. We will review a carrier's notification practices on a case-by-cases basis to determine whether it acted justly towards consumers and in a reasonable manner under the factual circumstances of a given case (i.e., taking into account the sensitivity of the consumer information, the scale and scope of a breach, the clarity and means of notification, among other things).[97]

44. Accordingly, we find that TerraCom's and YourTel's practices with respect to notifying consumers of the security breach is unjust and unreasonable in apparent violation of Section 201(b) of the Communications Act.

IV. PROPOSED FORFEITURE

45. Section 503(b)(1) of the Act states that any person who willfully or repeatedly fails to comply with any provision of the Act or any rule, regulation, or order issued by the Commission, shall be liable to the United States for a forfeiture penalty.[98] Section 503(b)(2)(B) of the Act empowers the Commission to assess a forfeiture of up to $150,000 against a common carrier for each willful or repeated violation of the Act or of any rule, regulation, or order issued by the Commission under the Act.[99] For a violation to be willful, it need not be intentional.[100] In exercising our forfeiture authority, we are required to take into account "the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[101] In addition, the Commission has established forfeiture guidelines, which set forth base penalties for certain violations and identify criteria that we consider in exercising our discretion in determining the penalties to apply in any given case.[102] Pursuant to the guidelines, we may adjust a forfeiture upward for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator.[103]

***14** 46. In determining the proper forfeiture in this case, we are guided by the principle that the protection of consumer PI is a fundamental obligation of all telecommunications carriers. Consumers are increasingly concerned about their privacy and the security of the sensitive, personal data that they must entrust to service providers of all stripes. Given the increasing concern about the security of personal data, we must take aggressive, substantial steps to ensure that carriers implement necessary and adequate measures to protect consumers' PI. In this case, the evidence shows that TerraCom and YourTel have not taken those obligations seriously. For the reasons articulated below, we propose a total forfeiture of $10,000,000 for the apparent violations in this case.

A. Section 222(a) Violations

1. Base Forfeiture for Section 222(a) Violations

47. Neither the Commission's forfeiture guidelines nor its case law establishes a base forfeiture for violations of Section 222(a). Thus, we look to the base forfeitures established or issued in analogous cases for guidance.

48. In 2011 and 2012, the Bureau issued Forfeiture Orders for failure to timely file the annual CPNI compliance certifications required by Section 64.2009(e) of the Commission's rules (CPNI Cases).[104] Similar to this case, the driving purpose behind the Commission's actions in the CPNI Cases was enforcing the protections that Congress established in Section 222(c) for consumers' proprietary information. In the CPNI Cases, the base forfeiture was between $20,000 and $29,000 for failure to file or failure to respond to a Bureau order to file certain information regarding the carriers' CPNI filings. Alternatively, the Commission has established a $40,000 base forfeiture amount for violations of Section 201(b)'s prohibition against unjust and unreasonable carrier practices in the context of deceptive marketing to consumers.[105]

49. We find that the Companies' actions were much more egregious than the actions of the carriers in the CPNI cases; likewise, the potential harm that flowed from the Companies' failure to secure the confidential personal information of consumers from unauthorized access was significantly greater than the harm posed by a carrier's failure to file CPNI certifications in a timely manner. As discussed below, hundreds of thousands of individuals were placed at risk of exposure of very sensitive personal information, including information about their income, their eligibility for and participation in federal assistance programs, their family members, and more. This exposure could, among other potential harms, put those individuals at risk of identity theft. The affected consumers face years of hassle and significant expense of credit monitoring to prevent permanent financial harm. Similarly, while the Commission's deceptive marketing cases are broadly analogous to this case, the potential harms to individuals whose personal and financial information is exposed to the public vastly outstrip the harms typically suffered by consumers who fall prey to misleading advertising messages.

2. Number of Violations

***15** 50. As discussed above, the Companies state that from September 2012 until late April 2013, the Companies stored personal data records belonging to approximately 305,065 customers and applicants on unsecured servers.[106] The Companies stated that they do not know the total number of related document files stored on the servers during that period.[107] Although it is likely that some customers submitted personal information on multiple documents—for example, a basic document containing name, address, and Social Security number paired with income verification documents such as SNAP benefits or federal public housing assistance benefits statements—we will assume for the purposes of calculating the forfeiture that each of the 305,065 customers and applicants had just one document stored on the unsecured servers.[108] Each document containing PI that the Companies failed to protect constitutes a separate violation for which a forfeiture may be assessed.[109] In addition, the failure by TerraCom and YourTel to protect the PI of customers constituted a continuing violation that continued for each day during the period within the statute of limitations of this case.[110] Each unprotected document constitutes a continuing violation that occurred on each of the 81 days that elapsed between February 4, 2013, and the date that the Companies remedied the failure on April 26, 2013.

3. Calculation of Proposed Forfeiture

51. Pursuant to the guidance of Section 1.80 of the FCC's rules, we look to a number of factors when we calculate a forfeiture. In this case, the Companies' apparently unlawful actions took place repeatedly and affected hundreds of thousands of consumers. Moreover, the harm caused by the Companies' actions affected an already vulnerable population—low income Americans. The Companies' apparently unlawful actions were long in duration, widespread in scope, and egregious in nature.

52. As explained above, in the past the Commission has used a base forfeiture of $29,000 per violation or day of a continuing violation that the Commission applied in prior CPNI cases. A direct application of a $29,000 base forfeiture amount to 305,065 personal data records (again, conservatively estimating that each affected customer or applicant had just one record on the Companies' unprotected servers) would result in a proposed forfeiture approaching $9 billion. Weighing the facts before us and taking into account the extent and gravity of the circumstances, we believe that a proposed forfeiture of $8,500,000[111] is sufficient to protect the interests of consumers and to deter future violations of the Act.[112]

B. Section 201(b) Violations

53. The Commission's forfeiture guidelines do not establish a base forfeiture for violations of Section 201(b). However, in other cases involving violations of Section 201(b) in the deceptive marketing and cramming contexts, the Commission has established a base forfeiture of $40,000 for each action that constitutes an unjust and unreasonable practice by a carrier.[113] As discussed above, the Companies' website privacy policies made false representations and promises to customers by assuring

them that the Companies would protect the sensitive personal information customers submitted when in fact the Companies did not protect it. The Companies' website privacy policies state that by submitting customer specific information to their website, "you acknowledge that you have read this privacy policy, understand it, agree to its terms and consent to the transfer of such information outside your jurisdiction."[114] These false promises of security are clearly unjust and unreasonable and thus violated Section 201(b). Moreover, the violations occurred on a continuing basis from February 4, 2013, until April 26, 2013. Accordingly, for the continuing violation of Section 201(b) caused by the Companies' false and misleading privacy policies, we propose a forfeiture of $1,500,000. However, in light of the fact that this is the first time we declare a carrier's practices unjust and unreasonable under Section 201(b) for failures related to (i) data security and (ii) notice to consumers in connection with a security breach, combined with the fact that we are imposing $10 million in penalties for the other violations at issue here, we exercise our discretion not to assess a forfeiture here for these apparent violations. But carriers are now on notice that in the future we fully intend to assess forfeitures for such violations.[115]

V. CONCLUSION

***16** 54. Based on the facts and record before us, we have determined that TerraCom, Inc. and YourTel America, Inc. have apparently willfully and repeatedly violated Sections 222(a) and 201(b) of the Communications Act of 1934, as amended.

VI. ORDERING CLAUSES

55. Accordingly, **IT IS ORDERED**, pursuant to Section 503(b) of the Communications Act of 1934, as amended, 47 U.S.C. § 503(b), and Section 1.80 of the Commission's rules, 47 C.F.R. § 1.80, that TerraCom, Inc., and YourTel America, Inc. are hereby **NOTIFIED** of this **APPARENT JOINT AND SEVERAL LIABILITY FOR FORFEITURE** in the amount of ten million dollars ($10,000,000), for willful and repeated violations of Sections 222(a) and 201(b) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 222(a), 201(b).

56. **IT IS FURTHER ORDERED THAT**, pursuant to Section 1.80 of the Commission's rules,[116] within thirty (30) days of the release date of this Notice of Apparent Liability for Forfeiture, TerraCom, Inc. and YourTel America, Inc. **SHALL PAY** the full amount of the proposed forfeiture for which they are jointly and severally liable, or each **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture.

57. *Payment Instructions*. Payment of the forfeiture must be made by check or similar instrument, wire transfer, or credit card, and must include the NAL/Account Number and FRN referenced above. TerraCom, Inc. and YourTel America, Inc. shall send electronic notification of payment to Johnny Drake at johnny.drake@fcc.gov on the date said payment is made. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.[117] When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in block number 24A (payment type code). Below are additional instructions the Companies should follow based on the form of payment they select:

· Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank - Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

· Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.

· Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

***17** 58. Any request for full payment over time under an installment plan should be sent to: Chief Financial Officer—Financial Operations, Federal Communications Commission, 445 12th Street, SW, Room 1-A625, Washington, DC

20554.[118] If the Companies have questions regarding payment procedures, they should contact the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

59. *Response Instructions*. The response, if any, must be mailed both to the Office of the Secretary, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554, ATTN: Enforcement Bureau—Telecommunications Consumers Division, and to Richard A. Hindman, Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554, and must include the NAL/Acct. No. referenced in the caption.

60. If the Companies choose to file a response seeking reduction of the proposed forfeiture on the basis of mitigation of harms caused by the apparently unlawful conduct described herein, the response must include (1) specific representations and warranties describing in detail such mitigation measures, (2) a signed declaration in compliance with Section 1.16 of the Commission's rules,[119] and (3) a request for reduction in forfeiture. The Commission may consider reducing the forfeiture if the Companies demonstrate that they have done or have entered into binding contracts to do one or more of the following:
· notified all affected consumers that their proprietary information was compromised;

· provided free credit monitoring services to all affected consumers (and will continue to provide such service for ten years in the future);

· assessed the scope of financial, reputational, or other harm that resulted from the apparently unlawful conduct and has made appropriate restitution to all affected consumers (including, but not limited to, providing restitution to consumers whose identities may have been stolen and/or credit rating harmed after the apparently unlawful conduct took place);

· provided a hotline and website where affected consumers may contact the Companies to report instances of identity theft or other harm in order to receive credit monitoring and other assistance from the Companies;

· appointed a Chief Privacy Officer as a permanent management position to oversee notification to affected consumers and administration of credit monitoring and other remediation measures;

· conducted training of all employees of the Companies concerning restitution to consumers, data security, and privacy protection policies;

· adopted industry best practices for data security and handling of confidential information as established by reputable organizations such as the National Institute of Standards and Technology;

· conducted independent third-party security audits of all online systems and systems that store proprietary information.

***18** The Commission may consider any or all mitigation efforts declared by the Companies when evaluating a request for reduction in forfeiture. Any such reductions in forfeiture shall be at the discretion of the Commission, and may not be calculated on a dollar-for-dollar basis.[120]

61. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits: (1) federal tax returns for the most recent three-year period; (2) financial statements prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status. Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation submitted.

62. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture shall be sent by Certified Mail Return Receipt Requested and First Class Mail to TerraCom, Inc. and YourTel America, Inc., Attn: Douglas D. Orvis, II, Esq., Bingham McCutchen LLP, 2020 K Street, NW, Washington, D.C. 20006-1806.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch

Secretary

STATEMENT OF CHAIRMAN TOM WHEELER

Re: TerraCom, Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No. EB-TCD-13-00009175

Today, the Commission is proposing a $10 million fine against two companies that failed to adequately secure the personal information of their customers. These companies have a duty under the Communications Act to protect the confidentiality of their customers' personal information. As the nation's expert agency on communications networks, the Commission cannot — and will not — stand idly by when a service provider's lax data security practices expose the personal information of hundreds of thousands of the most vulnerable Americans to identity theft and fraud.

Let's be clear about the facts: The companies in question collected sensitive information from low-income consumers to establish their eligibility for the Lifeline program. This collection is consistent with our rules, and the companies promised in their privacy policies to safeguard this information. But rather than safeguarding the information, the companies outsourced this responsibility to a vendor that collected and stored customers' Social Security numbers, names, addresses, driver's licenses, and other sensitive information on unprotected Internet servers.

In other words, the most sensitive, personal information of up to 305,000 Americans was available to anyone with an Internet connection anywhere in the world. We do not need detailed ex ante rules and regulations to know that this is simply unacceptable. Failure to take reasonable steps to secure consumer information is a clear breach of a carrier's duty to protect the confidentiality of the customer information they collect and an "unjust and unreasonable practice" — both violations of the companies' statutory obligations under the Communications Act.

Consumers entrust their most personal, confidential, and sensitive information to our communications networks and service providers every day. The Commission has a responsibility under the Communications Act to ensure that those service providers and network operators take reasonable steps to honor that public trust, and to protect consumers from harm caused by violations of the Communications Act. That is exactly what we are doing today.

STATEMENT OF COMMISSIONER MIGNON CLYBURN

Re: TerraCom, Inc. and YourTel America, Inc., Apparent Liability for Forfeiture, File No. EB-TCD-13-00009175

The single most critical piece of one's personal information is the nine-digit number assigned to you at birth. That social security number is your first and continuous link to wages, earnings and benefits, and stays with you for eternity. Headlines reporting significant data breaches are all too common. Once a breach occurs, there is often a long road for consumers to regain control of their personal information. Thus, it is imperative that companies in possession of our proprietary data take all appropriate measures to make sure it is not compromised.

The Commission has a clear role to ensure that providers protect sensitive information. In fact, Section 222 of the Communications Act imposes a "duty" on carriers to "protect the confidentiality of proprietary information." I find this case to be particularly egregious. These companies failed to protect the proprietary information entrusted to them. I fully support this action and sincerely hope it sends a clear signal that providers must ensure that consumers' sensitive information is protected.

DISSENTING STATEMENT OF COMMISSIONER AJIT PAI

Re: TerraCom, Inc. and YourTel America, Inc., Apparent Liability for Forfeiture, File No. EB-TCD-13-00009175

A core principle of the American legal system is due process. The government cannot sanction you for violating the law unless it has told you what the law is.[1]

In the regulatory context, due process is protected, in part, through the fair warning rule. Specifically, the D.C. Circuit has stated that "[i]n the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what

is expected of it—an agency may not deprive a party of property."[2] Thus, an agency cannot at once invent and enforce a legal obligation.

Yet this is precisely what has happened here. In this case, there is no pre-existing legal obligation to protect personally identifiable information (also known as PII) or notify customers of a PII data breach to enforce. The Commission has never interpreted the Communications Act to impose an enforceable duty on carriers to "employ reasonable data security practices to protect" PII.[3] The Commission has never expounded a duty that carriers notify all consumers of a data breach of PII. The Commission has never adopted rules regarding the misappropriation, breach, or unlawful disclosure of PII.[4] The Commission never identifies in the entire Notice of Apparent Liability a single rule that has been violated.[5]

Nevertheless, the Commission asserts that these companies violated novel legal interpretations and never-adopted rules. And it seeks to impose a substantial financial penalty. In so doing, the Commission runs afoul of the fair warning rule. I cannot support such "sentence first, verdict afterward" decision-making.

To the extent that the circumstances giving rise to today's item merited the Commission's attention, there was a better (and lawful) path forward. We could have opened a notice-and-comment rulemaking.[6] This process would have given the public an opportunity to speak. And in turn, the agency would have had a chance to formulate clear, well-considered rules—rules we then could have enforced against anyone who violated them. Instead, the Commission proposes a forfeiture today that, if actually imposed, has little chance of surviving judicial review.

One more thing. The Commission asserts that the base forfeiture for these violations is nine billion dollars—that's $9,000,000,000—which is by far the biggest in our history.[7] It strains credulity to think that Congress intended such massive potential liability for "telecommunications carriers" but not retailers or banks or insurance companies or tech companies or cable operators or any of the myriad other businesses that possess consumers' PII. Nor can I understand how such liability can be squared with the Enforcement Bureau's recent consent decrees with these companies. Under those consent decrees, the companies paid the Treasury $440,000 and $160,000 for flouting our *actual* rules and draining the Universal Service Fund by seeking Lifeline support multiple times for the same customer.

Consumer protection is a critical component of the agency's charge to promote the public interest. But any enforcement action we take in that regard must comport with the law. For the reasons stated above, I dissent.

DISSENTING STATEMENT OF COMMISSIONER MICHAEL O'REILLY

Re: TerraCom, Inc. and YourTel America, Inc., Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175
Companies that collect personal information about their customers have a responsibility to take reasonable measures to protect that information. Most companies take that obligation extremely seriously because it's in their best interests. So I was disturbed to learn that YourTel and TerraCom had allowed sensitive information about their universal service Lifeline subscribers to be stored in such a way that it could be accessed over the Internet through simple queries. I am also troubled that the companies did not appear to do anything to monitor the activities of their vendor to ensure that it was taking all necessary steps to protect this information. This is unacceptable for many reasons.

As unfortunate as this case may be, however, I find major flaws with the item proposed. First, I'm not convinced that the FCC has authority to act. In my previous employment, I worked extensively on privacy matters, and I am familiar with privacy laws across federal agencies. I also was there for the creation of section 222 of the Act, and it is my firm belief that it was never intended to address the security of data on the Internet. I also do not believe that section 201(b) covers this conduct. Second, even if the FCC did have authority to act, I am not persuaded that it is appropriate for the agency to proceed, in this first instance, through an enforcement action because the agency has not provided fair notice that there could be liability for such conduct. The Commission should have sought comment on these issues to determine the authority for and scope of any data security rules for common carriers. Therefore, I must respectfully dissent from this Notice of Apparent Liability for Forfeiture.

I am noticing a disturbing trend at the Commission where, in the absence of clear statutory authority, the Commission suddenly imbues an innocuous provision of the Act with tremendous significance in order to meet its policy outcome. Section 706 was one such example. Today it's section 222(a).

Section 222(a), however, cannot be interpreted in a vacuum. There is a history here, and it is worth retelling because it is relevant not only to the Commission's authority to act, but also to whether parties would have fair notice of what conduct is barred by the provision.

Those that have been following common carrier law long enough will recall that CPNI rules pre-date the Telecommunications Act of 1996. In the *Computer II*, *Computer III*, *GTE ONA*, and *BOC CPE Relief* proceedings, the Commission established rules concerning the use of CPNI in the enhanced services operations of AT&T, the BOCs, and GTE, and the CPE operations of AT&T and the BOCs. The Commission adopted these rules (along with other nonstructural safeguards) because the Commission was concerned that the carriers could use CPNI obtained from their provision of regulated services to gain an anticompetitive advantage in the unregulated CPE and enhanced services markets.[8] It also determined that the CPNI requirements were necessary to protect legitimate customer expectations of confidentiality regarding individually identifiable information.[9]

With this history in mind, and with the further understanding that one of the goals of the 1996 Act was to open local markets to competition from new telecommunications carriers, the structure and purpose of section 222 becomes evident.

Section 222(a) begins with a duty on every telecommunications carrier to protect the confidentiality of proprietary information. That is, the purpose of section 222(a) was to extend CPNI rules to *all* telecommunications carriers, not just AT&T, the BOCs, and GTE. This was understood by the Commission at the time it was implementing the 1996 Act.[10] Then, sections 222(b) and (c) go on to codify certain restrictions to address the two concerns that led the Commission to adopt CPNI rules in the first place: to protect other carriers from anticompetitive practices; and to protect the privacy expectations of consumers.

Critically, the general duty in section 222(a) was intended to be read in conjunction with, not separate from, the specific limitations in sections 222(b) and (c). And that is how the Commission viewed the provisions.[11] Namely, section 222(a) sets forth who has the basic duty to protect the proprietary information of other telecommunications carriers, equipment manufacturers, and customers, while sections 222(b) and (c) detail when and how that duty is to be exercised. Section 222(b) requires that carriers may only use proprietary information of other carriers for the purpose of providing telecommunications and may not use it for their own marketing efforts. Section 222(c) specifies under what circumstances the proprietary information of customers (also known as CPNI) may be disclosed.

I do not see persuasive evidence that section 222(a) was intended to confer authority that was independent of the carrier information and CPNI provisions. Indeed, on multiple occasions, the Commission has made statements like "[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI."[12] That is because the Commission viewed them as co-extensive.[13] In fact, it is very telling that the Commission has never before attempted to interpret 222(a) independent of CPNI. What is more, the House Conference Report on the 1996 Act notes, "[i]n general, the new section 222 strives to balance both competitive and consumer privacy interests *with respect to CPNI*."[14]

Moreover, the fact that section 222(a) uses a broader term "proprietary information" is not dispositive in this instance. Separate from my working experiences with this provision, given the three-part structure of section 222, the statute includes a term in 222(a) that encompasses both the carrier information at issue in 222(b) and the customer information at issue in 222(c).

Furthermore, I find the reliance on the section heading in this case as a source of authority just plain laughable. If the Commission can invent new authority based on the "Privacy of Customer Information" heading of section 222, I can only imagine what it could do with the heading of section 215: """"Transactions Relating to Services, Equipment, *And So Forth*".[15] I suspect that those in the Commission that are asked to defend the Commission's work would also agree that section headings are of little to no value.

I do not agree that section 201(b), which dates even further back to 1934, can be read to cover data protection, and I strongly disagree with the assertion in footnote 79 that the Commission has authority to enforce unlawful practices related to cybersecurity. Moreover, if data protection falls within the ambit of 201(b), then I can only imagine what else might be a practice "in connection with" a communications service. What is the limiting principle? Perhaps recognizing that it is on

shaky legal ground, the NAL at least declines to propose a forfeiture for the failure to employ just or reasonable data security practices or to notify all consumers affected by the breach.

Yet even if the Commission did have authority under section 222(a) and/or section 201(b), and I do not believe that it does, I would still have serious concerns that the Commission did not provide fair notice that the companies could be liable under those sections for this conduct. In other words, it appears the Commission is short circuiting the procedural requirements of law.

I acknowledge that the Commission has asserted in the past that it may announce new interpretations or policies in the context of an adjudication. However, "[a] fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required."[16] Accordingly, "[a] conviction or punishment fails to comply with due process if the statute or regulation under which it is obtained 'fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement."DD'[17] Moreover, "[i]n the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability."[18]

As the FCC itself has explained, "fair notice of the obligation being imposed on a regulatee" means that "'by reviewing the regulations and other public statements issued by the agency a regulated party acting in good faith would be able to identify, with ascertainable certainty, the standards with which the agency expects parties to conform before imposing civil liability."DD'[19] However, there are no regulations *at all* on section 222(a), and I am not aware of any statements that say or even hint that 222(a) and/or 201(b) covers this conduct. If there were, I would have expected them to be cited in this NAL. At most, and this is being more than generous, a very creative practitioner might have been able to imagine a scenario under which misrepresenting data security practices could fall within section 201(b). But that's it. For these reasons, and for the reasons discussed above, I do not think that the companies had fair notice and, therefore, the Commission should not propose a forfeiture. I would not be surprised to see this issue litigated at some point.

In fact, a series of agency actions (and inaction) made it *less likely* that the companies would have had fair notice. In 2007, the Commission sought comment on, among other things, requiring carriers to physically safeguard the security and confidentiality of CPNI.[20] This included questions on whether to adopt rules governing the physical transfer of CPNI among companies or to any other third party authorized to access or maintain CPNI, including a carrier's joint venture partners and independent contractors. Since the Commission included reference to this proceeding in the NAL, it certainly knows that it never acted on that part of the further notice.[21] In fact, commenters generally opposed further requirements and noted that the chief concern was access to CPNI by pretexters over the phone, not hackers seeking to gain unlawful access to carriers' CPNI databases.[22] So the issue appeared to have died. Moreover, when the Commission did act on another part of the 2007 further notice regarding data on mobile devices, it did so only after the relevant Bureaus sought further comment to refresh the record, including on whether the Commission should act by declaratory ruling, which it ultimately did. Therefore, it would have been reasonable for a regulated entity acting in good faith to believe that, at most, the Commission might act on physical safeguards, but only with respect to CPNI, and only after seeking further comment.

In sum, while I am troubled that sensitive information about Lifeline subscribers was exposed to the public, I cannot support an NAL that exceeds our authority and comes without fair notice to the companies involved. I respectfully dissent.

Footnotes

1 Lifeline service is a retail voice telephony service that telecommunications carriers provide to qualifying low- income consumers for a reduced charge. 47 C.F.R. § 54.407(b). *See also Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6662-67, paras. 11-18 (2012) (*Lifeline Reform Order*); 47 C.F.R. §§ 54.400-54.422.

2 Carriers providing Lifeline service are called "eligible telecommunications carriers," or ETCs, and are reimbursed by the Universal Service Fund for the subsidized amount of the voice service they provide to qualified consumers. 47 C.F.R. § 54.407(b). *See also*

Lifeline Reform Order, 27 FCC Rcd at 6662-67, paras. 11-18; 47 C.F.R. §§ 54.400-54.422.

3 TerraCom provides wireless Lifeline service in Arkansas, Arizona, Colorado, Indiana, Iowa, Louisiana, Maryland, Minnesota, Nebraska, Nevada, Oklahoma, Texas, West Virginia, and Wisconsin.

4 YourTel provides wireless Lifeline service in Illinois, Kansas, Maine, Missouri, Oklahoma, Pennsylvania, Rhode Island, and Washington.

5 TerraCom's and YourTel's Chief Operating Officer (COO) is Dale Schmick.

6 BrightStar Global Solutions, LLC is an Oklahoma limited liability company located at 1101 Territories Dr., Edmond, OK 73034. TerraCom describes BrightStar as "***." *See* Letter from Mark C. Del Bianco, Law Office of Mark C. Del Bianco, Attorney for TerraCom and YourTel, to Steven Ruckman, Esq., Assistant Attorney General, Maryland Office of the Attorney General, (June 14, 2013) (on file in EB-TCD-13-00009175) (Maryland AG Letter of Jun. 14, 2013).

7 According to the respective 499s of TerraCom and YourTel, the Companies share the same corporate headquarters address at 401 E. Memorial, Suite 400, Oklahoma City, OK 73114. However, according to YourTel's 2013-2014 Biennial Registration Report with the Missouri Secretary of State, the company's principal place of business or corporate headquarters is 2800 E. 18th Street, Kansas City, MO 64127. *See* YourTel America, Inc. 2013-2014 Biennial Registration Report (Mar. 20, 2013), *available at* Missouri Sec. of State, Online UCC Filing, https:// bsd.sos.mo.gov/BusinessEntity/BusinessEntityDetail.aspx?page=beSearch&ID=356173.

8 *See* 47 C.F.R. § 54.410; *see also* E-mail and attachment from Matt Connolly, Manager, Regulatory Affairs, YourTel America, Inc., to Donna Cyrus, Senior Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (July 17, 2013, 17:02 EDT) (on file in EB-TCD-13-00009175) (TerraCom/YourTel LOI Response).

9 *See* Letter of Intent From Call Centers India DBA Vcare Corporation to BrightStar Global Solutions, LLC (Jul. 10, 2012) (on file in EB-TCD-13-00009175) (Vcare Agreement). ***, Vcare provided a variety of services purchased by the Companies *** to enable their provision of Lifeline services, including, among other things, front end website and backend application flow and processing, customer account activations, support for lifeline enrollments, including processing customer applications, certain integration and gateway services, and call center services. *See* Vcare Agreement at 1-3; *see also JLee-Cease-and-Desist-Ltr*, torekeland.com, *available at* https://torekeland.com/wp-content/uploads/2013/05/JLee-Cease-and-Desist-Ltr.pdf (last visited Oct. 17, 2014).

10 The Companies were not specific about the exact date in September 2012 when they began storing PI on Vcare's servers, so for purposes of this Notice of Apparent Liability for Forfeiture, we will attribute this date to September 30, 2012. *See* E-mail from Douglas D. Orvis II, Bingham, Counsel to TerraCom and YourTel, to Donna Cyrus, Senior Attorney Advisor, Telecommunications Consumers Division, Enforcement Bureau, FCC (Jan. 24, 2014, 15:09 EDT) (on file in EB-TCD-13-00009175) (January 24, 2014, E-mail).

11 *See* Letter from Douglas D. Orvis II, Bingham, Counsel to TerraCom and YourTel, to Kimberly Wild, Deputy Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, (Nov. 19, 2013) (on file in EB-TCD-13-00009175)

(TerraCom/YourTel November 19, 2013, Supplemental LOI Response).

12 The records of 343 individuals were also accessed by unknown parties during this time. *See* TerraCom/YourTel November 19, 2013, Supplemental LOI Response. Additional, undetermined access to these records may have occurred since September 2012, "when VCare [sic] became the third party verification company for TerraCom and YourTel." *See* January 24, 2014, E-mail.

13 *Isaac Wolf Accesses Lifeline Files*, NewsNet5 Cleveland (May 19, 2013), *available at* http://www.newsnet5.com/news/local-news/special-reports/privacy-on-the-line-security-lapse-exposes-some-lifeline-phone-customers-to-id-theft-risk (last visited September 4, 2014).

14 *Id.*

15 E-mail from Isaac Wolf, Scripps Howard News Service, to Dale Schmick, COO, TerraCom and YourTel (Apr. 26, 2013, 11:17 EDT) (on file in EB-TCD-13-00009175), *available at* http://media.thedenverchannel.com/documents/Scripps+email+requesting+interview.pdf.

16 Letter from Jonathan D. Lee, Principal, JD Lee Consulting, and Counsel, TerraCom, Inc. and YourTel America, Inc., to William Appleton, Senior Vice President/General Counsel, The E.W. Scripps Company, *available at* media.thedenverchannel.com/documents/Response+from+Jonathan+Lee.pdf (Apr. 30, 2013) (Scripps Cease and Desist Letter) (on file in EB-TCD-13-00009175).

17 *Id.*

18 *See* E-mail and attachments from Mark Del Bianco. Esq.. Law Office of Mark C. Del Bianco. Attorney for TerraCom and YourTel. to Donna Cyrus. Senior Attorney Advisor. Telecommunications Consumers Division, FCC Enforcement Bureau (May 7. 2013, 23:32 EDT) (on file in EB-TCD-13-00009175) (May 7, 2013, E-mail).

19 *Id.*

20 *Id.*

21 Isaac Wolf. *Privacy on the Line: Security lapse exposes some Lifeline phone customers to ID theft risk*. Scripps News (May 20, 2013), *available at* http://www.kirh.com/news/local-news/investigations/privacy-on-the-liiie-securitv-lapse-exposes-some-lifeline-phone-customers-to-id-theft-risk: *see also* May 7, 2013. E-mail (the Companies stated that their investigation "revealed that the records of approximately 343 individuals were accessed one or two at a time from IP addresses whose owners we cannot confirm at this time.").

22 *See* Letter from Jonathan D. Lee, Esq., Principal. JD Lee Consulting. Counsel for TerraCom and YourTel. to Radhika Karmarkar,

Deputy Division Chief. Telecommunications Access Policy Division. FCC Wireline Competition Bureau (May 17. 2013) (on file in EB-TCD-13-00009175) (May 17. 2013, Letter).

23 *See* Letter from Richard A. Hindman, Chief. Telecommunications Consumers Division. FCC Enforcement Bureau, to Mark C. Del Bianco. Esq.. and Jonathan D. Lee, Esq.. Counsel for TerraCom and YourTel (June 17, 2013) (on file in EB-TCD-13-00009175) (LOI).

24 *See* TerraCom/YourTel LOI Response. The LOI was addressed to both Companies and required each entity to answer questions with respect to that entity's operations. The Companies filed a joint response to the Bureau's inquiries on behalf of both companies, but they indicated that TerraCom and YourTel are unaffiliated corporations. Accordingly, to the extent the answers submitted by the Companies identify a single company, we attribute that answer to the identified company; when the responses do not specify either TerraCom or YourTel individually, we attribute that answer to both Companies. Moreover, in their joint letters to the Wireline Competition Bureau and in their initial responses to the Enforcement Bureau's inquiries, the Companies referred to each other jointly and identified themselves as affiliates.

25 47 U.S.C. § 222(a).

26 47 U.S.C. § 201(b).

27 *See* TerraCom/YourTel LOI Response at 6, stating "Vcare provides the entrance portal through which applicant order information is collected and delivered for processing and storage on Vcare owned servers." *See also JLee-Cease-and-Desist-Ltr*, torekeland.com, *available at* https://torekeland.com/wp-content/uploads/2013/05/JLee-Cease- and-Desist-Ltr.pdf (last visited Oct. 17, 2014).

28 *See* TerraCom Privacy Policy, terracomwireless.com, https:// web.archive.org/web/20110924070048/http://www.terracomwireless.com/privacy/ (archived Sept. 24, 2011) (accessed by searching for TerraCom, Inc. Privacy Policy in the Internet Archive) (on file in EB-TCD-13-00009175); YourTel Privacy Policy, yourtelwireless.com, https:// web.archive.org/web/20110521001951/http://www.yourtelwireless.com/privacy/ (archived May 21, 2011) (accessed by searching for YourTel America, Inc. Privacy Policy in the Internet Archive) (on file in EB-TCD-13-00009175) (archived copies of the privacy policies of TerraCom and YourTel prior to September 2012). *See also* TerraCom Privacy Policy, www.terracomwireless.com/privacy.php (last visited Sept. 4, 2014), YourTel Privacy Policy, www.yourtelwireless.com/privacy.php (last visited Sept. 4, 2014) (current privacy policies of the Companies, respectively).

29 *See* 47 U.S.C. § 222(a).

30 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007).

31 *Id.* at 6959-60, para. 65.

32 Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996 Act) (codified at 47 U.S.C. §§ 151 *et seq.*).

33 *See, e.g., supra* note 30.

34 *See* 47 U.S.C. § 396(l)(4)(C) ("The Corporation shall make available for public inspection the final report required by the Corporation on an annual basis from each recipient of funds under subsection (k)(3)(A)(iii)(III) of this section, excluding proprietary, confidential, or privileged information.").

35 *See* 47 U.S.C. § 273(d)(2). This prohibition against unauthorized use or release of proprietary information continues "even after such [standards-setting or certification] entity ceases to be so engaged [by the equipment manufacturer]." *Id.*

36 *See also, e.g.*, 47 U.S.C. § 272(d)(3)(C) (in the context of joint federal/state biennial audits of Bell Operating Company affiliates, requiring State commissions to "implement appropriate procedures to ensure the protection of any proprietary information submitted to it" as part of the audits); 47 U.S.C. § 274(b)(9) (in the context of rules applicable to BOCs and BOC affiliates with respect to joint ventures for the provision of electronic publishing services, requiring "reasonable safeguards to protect any proprietary information" contained in certain reports made available for public inspection).

37 *See* 47 U.S.C. § 222(c) (defining telecommunications carriers' obligations with respect to CPNI); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 28 FCC Rcd 9609, 9618 ¶ 27 ("We also note that subsection (a)'s obligation to protect customer information is not limited to CPNI that the carrier has obtained or received.").

38 *See* National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, SP 800-122, *available at* http://csrc nist.gov/publications/nistpubs/800-122/sp800-122.pdf (last accessed Sep. 11, 2014); *see also* GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information* (May 2008), *available at* http://www.gao.gov/new.items/d08536.pdf.

39 *Lifeline Reform Order*, 27 FCC Rcd at 6745, para. 207.

40 *Id.*

41 TerraCom/YourTel LOI Response at 3; *see also Phone Carriers Expose Low-Income Applicants to Risk of ID Theft*, thedenverchannel.com, *available at* http://www.thedenverchannel.com/news/privacy-on-the-line/phone-carriers-expose-low-income-applicants-to-risk-of-id-theft (last visited Oct. 17, 2014).

42 *Id.*

43 *See* TerraCom/YourTel November 5, 2013, Clarification Response at 2, stating, "The Company also objects to the categorization of these persons as "customers", as it assumes, without proper foundation, that the applicants identified in the databases of the

Company are all enrolled customers. That is not correct." According to the evidence, the Companies believed that only 20,150 of approximately 151,000 records downloaded by Scripps belonged to applicants and not customers. *See* E-mail from Salil Gupta, Vcare, to Dale Schmick, COO, TerraCom/YourTel (May 8, 2013, 16:18 EDT) (on file in EB-TCD-13-00009175).

44 In this regard, Section 54.410 of our rules bars the Companies from activating a consumer's Lifeline service "unless and until it has ... [c] onfirmed that the consumer is a qualifying low-income consumer ... [and] [c] ompleted the eligibility determination ...." 47 C.F.R. § 54.410(a)(1)—(2).

45 Black's Law Dictionary defines "customer" to include "[a] buyer, purchaser, consumer or patron," while Random House defines "customer" as "a patron, buyer, or shopper." Customer, Black's Law Dictionary (5th ed. 1979); customer, The Random House College Dictionary (1973).

46 *See supra* paras. 14-20. *See also Lifeline and Link Up Reform and Modernization*, Notice of Proposed Rulemaking, 26 FCC Rcd 2770 para. 57, n.97 (2011).

47 *See supra* note 28.

48 *See* Appendix, examples of the Lifeline Certification Form used by each Company.

49 In addition, the term "customer" includes both current and former applicants and subscribers.

50 47 U.S.C. § 222(a).

51 47 U.S.C. § 222(b).

52 47 U.S.C. § 222(c).

53 Both subsections (a) and (b) protect the confidentiality of carrier information. *Compare* 47 U.S.C. § 222(a) *with* 47 U.S.C. § 222(b) (subsection (a) protects "other telecommunication carriers" and includes within the term "customer" carriers that resell telecommunications services). Similarly, both subsections (a) and (c) protect "customer" information—with subsection (c) limited in scope to protecting CPNI, specifically. *Compare* 47 U.S.C. § 222(a) *with* 47 U.S.C. § 222(c) (subsection (a) protects """proprietary information of ... customers" and subsection (c) protects """customer proprietary network information").

54 Our interpretation of "customer" in this way is consistent with established principles of statutory construction. *See, e.g., Sacramento Nav. Co. v. Salz*, 273 U.S. 326, 330 (1927) (".... words are ... to be taken in the sense which will best manifest the legislative intent"). In this case, the Companies' argument that "customer" does not include applicants seeking to become subscribers of the Companies' services is an overly mechanical reading of the statute that would defeat the intent of Congress to protect consumers' personal information from public exposure. *See Lawson v. Suwannee Fruit & Steamship Co.*, 336 U.S. 198, 201 (1949) (proper to give construction to avoid overly narrow reading of statutory terms, even defined terms, that would lead to

results Congress did not intend). Moreover, identical words used in different parts of the statute, or even within the same part of a statute, may be read flexibly in order to best reflect Congressional intent. *See Environmental Defense v. Duke Energy Corp.*, 549 U.S. 561, 574 (2007) (*Environmental Defense*) ("We ... understand that most words have different shades of meaning and consequently may be variously construed, not only when they occur in different statutes, but when used more than once in the same statute or even in the same section.") (internal citations omitted).

55 47 U.S.C. § 222(c).

56 47 C.F.R. § 64.2003(f).

57 *See Environmental Defense*, 549 U.S. at 574 (holding that identical words within a statute may take on different meanings, even when the words share a common, general definition, and stating that "each section [of the regulation] must be analyzed to determine whether the context gives the term a further meaning that would resolve the issue in dispute ....").

58 *See* report from Sensei Enterprises, Inc., to Andy Roth, Dentons, Counsel for TerraCom and YourTel (December 13, 2013) (on file in EB-TCD-13-00009175) (Sensei Forensic Report)*; see also infra* note 67.

59 Bureau Staff contacted the site and requested removal of the archived website pages, and notified counsel for TerraCom when the website agreed to do so. *See* Email from Kristi Thompson, Deputy Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Douglas D. Orvis II, Bingham, Counsel to TerraCom and YourTel (Jul. 1, 2014, 16:06 EDT) (on file in EB-TCD-13-00009175).

60 *See* E-mail from Michael C. Maschke, Chief Information Officer, Sensei Enterprises, Inc., to Dale Schmick, COO, TerraCom and YourTel (May 14, 2013, 13:31 EDT) (on file in EB-TCD-13-00009175); *see also Crawling & Indexing*, Google, *available at* http:// www.google.com/insidesearch/howsearchworks/crawling-indexing html (last visited Oct. 17, 2014).

61 47 U.S.C. § 201(b).

62 *See* TerraCom/YourTel LOI Response at 3; *see a/so Investigative Journalists Threatened with Felony for Exposing Security Flaw*, rt.com, *available at* http://rt.com/usayhack-teiTacom-securiry-scripps-596/ (last visited Oct. 17.2014).

63 *See* Maryland AG Letter of Jun. 14, 2013. at 2 (stating that the parties ***.

64 *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd 6927 at 6946.

65 The single act of placing a consumer's name in a URL may, under certain circumstances, be a breach of a carrier's duty under Section 222(a) of the Act. but when the name is linked to other proprietary information belonging to the named person (as is the

case here), it is *clearly* a failure to "protect" that information and. therefore, a violation.

66 *See* Sensei Forensic Report.

67 *See Isaac Wolf accesses Lifeline files*, Naples Daily News. May 19. 2013, http://www.naplesnews.com/videos/detail/isaac-wolf-accesses-files-online-lifeline/ (last visited Jun. 26, 2014) (video of Scripps reporter Isaac Wolf demonstrating how to access TerraCom Lifeline application materials via Google searches).

68 The Companies reported that the security breach occurred between March 24, 2013 and April 26, 2013. It is now apparent, however, that the Companies' problem of inadequate security extends well beyond these dates, to September 2012 when Vcare became the Companies' third party data processor and began storing the applicant files in publicly accessible folders. *See* January. 24.2014. E-mail. Thus, for at least seven months, the personal information contained in the Lifeline enrollment applications and proof documents were accessible by search engines.

69 In addition to this estimate of 128.066 provided by the Companies, the Sensei Forensic Report reports that a total of *** were made by ***. Scripps also reports that figure as high as 170,000. *See* Ellen Weiss. *Scripps Investigation into Security' Risks Draws Scrutiny*, Scripps Howard News Service (May 15. 2013). *available at* http://www.abcactionnews.com/news/local-news/i-team-investigates/kjrh_scripps-investigation-mto-security-risks-draws-scrutiny1368649588977.

70 E-mail from Michael Maschke. Chief Information Officer. Sensei. to Dale Schmick. YourTel (May 14, 2013).

71 TerraCom/YourTel LOI Response. Ex. 1.

72 Sensei Forensic Report at 3.

73 *See, e.g.*, Erik Olsen, *Losing Face: Identity Thieves Steal More Than Money*, ABC News, *available at* erikolsen.com/writing/ABCarticles/ABCNEWS.com_ID_ theft.htm (last visited Sept. 4, 2014) (identifying Eastern Europe and Southeast Asia as hotspots for identity theft, because "the level of education and technical sophistication is high, and [] tracking down and prosecuting criminals can be very tricky.").

74 While we find that the Companies apparently violated Section 201(b) in this section, because this is the first case in which we make such a finding, we decline to exercise our discretion to propose a forfeiture for such violation at this time. However, we caution other carriers that the Commission is committed to aggressive enforcement of unlawful practices related to cyber security and data protection.

75 *See* archived and current TerraCom privacy policies, *supra* note 28.

76 ***Id.***

77 *See supra* para. 29.

78 The Companies claim that ***" TerraCom/YourTel LOI Response at 7.

79 *See* attachment to May 7, 2013, E-mail, Factual Submission for TCD Staff.

80 TerraCom/YourTel LOI Response at 6-7 (identifying the security measures currently in place, and those in place at the time Scripps accessed customer proprietary information).

81 *See STi Telecom Inc.*, Notice of Apparent Liability for Forfeiture. 26 FCC Rcd 12808. 12812 para. 10 (2011) (disclosures must be in clear and unambiguous language to ensure that they are effective.). *See also Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers*, Policy Statement, 15 FCC Rcd 8654, 8655 (2000) (*Joint FCC/FTC Policy Statement*), stating that "Legalistic disclaimers too complex for consumers to understand may not cure otherwise deceptive messages or practices"; *id.* at 8663 (noting that prominence, proximity, and placement of disclosure in comparison to advertising representation affect effectiveness of disclosure).

82 *See STi Telecom Inc.*, 26 FCC Rcd 12808; *Locus Telecommunications, Inc.*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12818 (2011)

83 The FCC has indicated that a marketing act or practice by a carrier that would constitute an unfair or deceptive act or practice under the FTC Act likewise constitutes an unjust and unreasonable act under Section 201(b) of the Communications Act. *See* Joint FCC/FTC Policy Statement, 15 FCC Rcd at 8655; *Business Discount Plan, Inc.*, Order of Forfeiture, 15 FCC Rcd 14461 at 14468-69 paras. 15-16 (2000) (finding that "deceptive telemarketing practices constitute 'unjust and unreasonable' practices within the meaning of section 201(b)"), *recon. denied in relevant part*, Order on Reconsideration, 15 FCC Rcd 24396 at 24399, para. 8 (2000) (finding that section 201(b) grants the Commission "a more general authority to address such practices as they might arise in a changing telecommunications marketplace"); *Locus Telecommunications, Inc.*, 26 FCC Rcd at 12820, para. 7. The same principle applies here. *See, e.g., Eli Lilli & Co.*, 133 F.T.C. 763, 767 (2002) (alleging that a failure to maintain appropriate security measures was an unfair or deceptive act or practice).

84 January 24, 2014, E-mail. In addition, the Companies posted a notice about the breach on their websites between May 2013 and November 2013. *Id.*

85 *Id.*

86 *See id.*; *see also infra* note 108.

87 May 7, 2013, E-mail.

88 The Companies admit that the "number [of persons whose information was accessed] cannot be determined with absolute certainty." but that their "best estimate" is 128,066. TerraCom/YourTel November 19, 2013, Supplemental LOI Response at 2 (clarification of Question 1.a. LOI answer).

89 May 7, 2013, E-mail; *see also* TerraCom/YourTel LOI Response at 3.

90 TerraCom/YourTel November 19. 2013. Supplemental LOI Response at 2 (clarification of Question 1.a. LOI answer).

91 Sensei Forensic Report at 3, 5.

92 *Id* at 4.

93 TerraCom/YourTel LOI Response. Exhibit 1. IP Identity List.

94 *See id.* at 5. The Companies state that "the personal information of a small number of subscribers or potential subscribers was accessible by unauthorized individuals via a Google search ... Given the low number and the pattern of record-by-record access, we believe that most, if not all, of these records were accessed by sales agents or other company personnel who are authorized to have access and who simply accessed the records from a home computer." *Id.*

95 Both applications were publically available on www.archive.org, a non-profit Internet library that uses web crawlers to access and save publically available internet pages. Prior to release of this NAL, the Bureau reached out to the Internet Archive requesting that the two applications be removed. Staff notified counsel for the Companies of these additional breaches. Copies of the web pages containing these applications are on file with Staff.

96 As of the release date of this NAL, the Company has provided the Commission of no updates that would show that it has completed notifying each such consumer.

97 Because this is the first time we declare a carrier's practices related to its failure to adequately notify consumers in connection with a security breach unjust and unreasonable in apparent violation of Section 201(b), we do not propose to assess a forfeiture for the apparent violations here. However, through our action today, carriers are now on notice that in the future we fully intend to assess forfeitures for such violations, taking into account the factors identified above.

98 47 U.S.C. § 503(b)(1)(B); *see also* 47 C.F.R. § 1.80(a)(2).

99 The maximum forfeiture for a continuing violation by a common carrier at the time the violations took place was $1,500,000. *See Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Forfeiture Maxima to Reflect Inflation*, Order, 23 FCC Rcd 9845 (2008). In 2013, the maximum forfeiture amount was increased to $1,575,000. *See Amendment Of Section 1.80(B) Of*

The Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation, Order, DA 13-1615, 78 FR 49371 (Rel. Aug. 1, 2013).

100 *Southern California Broadcasting Co.*, Memorandum Opinion and Order, 6 FCC Rcd 4387, 4388, para. 5 (1991).

101 *See* 47 U.S.C. § 503(b)(2)(E); *see also The Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Commission's Rules*, Report and Order, 12 FCC Rcd 17087, 17100-01, para. 27 (1997) (*Forfeiture Policy Statement*).

102 47 C.F.R. § 1.80(b)(8), Note to paragraph (b)(8).

103 *Id.*

104 *See, e.g., Nationwide Telecom, Inc.*, Order of Forfeiture, 26 FCC Rcd 2440 (2011); *Diamond Phone, Inc.*, Order of Forfeiture, 26 FCC Rcd 2451 (2011); *USA Teleport, Inc.*, Order of Forfeiture, 26 FCC Rcd 2456 (2011); *Jahan Telecommunication, LLC*, Order of Forfeiture, 27 FCC Rcd 6230 (2012); *88 Telecom Corporation*, Order of Forfeiture, 26 FCC Rcd 7913 (2011); *DigitGlobal Communications, Inc.*, Order of Forfeiture, 26 FCC Rcd 8400 (2011).

105 *See Business Discount Plan, Inc.*, 15 FCC Rcd 14461 at14471-72; *NOS Communications, Inc. and Affinity Network Corporation*, Notice of Apparent Liability for Forfeiture, 16 FCC Rcd 8133 at 8141-42 (2001)(NOS); *Locus Telecommunications, Inc.*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12818 at 12820-23 (2011); *Simple Network, Inc.*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 16669 at 16675 (2011); *STI Telecom Inc.* (Formerly Epana Networks, Inc.), Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12808 at 12810-15 (2011); *Touch-Tel USA LLC*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12836 at 12842-43 (2011); *Lyca Tel, LLC*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12827 at 12832-34 (2011); *NobelTel LLC*, Notice of Apparent Liability for Forfeiture, 27 FCC Rcd 11760 at 11765-68 (2012).

106 *See* January 24, 2014, E-mail.

107 *Id.* The Companies state that they "have not been provided with information detailing the number of files stored on VCare's [sic] servers during the period that some applicant information may have been potentially accessible."

108 Representatives of the Companies recently alleged in a meeting with Bureau staff that the number of customers and applicants may be less than the 305,065 figure previously submitted into the record by the Companies because some submissions were apparently duplicates. The actual number of affected consumers does not change the forfeiture calculation in this case. *See infra* note109.

109 *See NOS*, 16 FCC Rcd at 8141("Each rate sheet sent to consumers constitutes a separate violation of section 201(b)"); *see also supra* note99.

110 The applicable dates of the apparent violations related to Section 222(a) of the Act within the statute of limitations in this case are

February 4, 2013, to April 26, 2013.

111 In light of the number of violations in this case, the proposed forfeiture is well within the limits established in Section 503 of the Act. We also note that even if we were to subtract the mere applicants (that is, consumers who applied for Lifeline service from the Companies but never became subscribers) from the 305,065 affected consumers, our forfeiture calculations would still support the proposed penalty for Section 222(a) violations. Moreover, we note that each record that the Companies failed to protect separately constitutes an unjust and unreasonable act or practice prohibited by Section 201(b) of the Act for which we could assess an additional penalty of $40,000 per record.

112 *See NOS*, 16 FCC Rcd at 8141-42.

113 *See Business Discount Plan, Inc.*, 15 FCC Rcd 14461 at 14471-72; *NOS*, 16 FCC Rcd at 8141-42; *Locus Telecommunications, Inc.*, 26 FCC Rcd at 12820-23; *Simple Network, Inc.*, 26 FCC Rcd at 16675; *STI Telecom Inc.*, 26 FCC Rcd at 12810-15; *Touch-Tel USA LLC*, 26 FCC Rcd at 12842-43; *Lyca Tel, LLC*, 26 FCC Rcd at 12832-34; *NobelTel LLC*, 27 FCC Rcd at 11765-68.

114 *See supra* note 28.

115 *See supra* notes 74, 97.

116 47 C.F.R. § 1.80.

117 An FCC Form 159 and detailed instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

118 *See* 47 C.F.R. § 1.1914.

119 *See* 47 C.F.R. § 1.16.

120 *See* 47 U.S.C. § 503(b)(2)(E) (authorizing the Commission to determine the amount of forfeitures by taking into account such factors "as justice may require.").

1 *Mullane v. Central Hanover Tr. Co.*, 336 U.S. 306, 313 (1950) ("Many controversies have raged about the cryptic and abstract words of the Due Process Clause but there can be no doubt that at a minimum they require that deprivation of life, liberty or property by adjudication be preceded by notice and opportunity for hearing appropriate to the nature of the case."); *Calder v. Bull*, 3 U.S. 386, 390 (1798) (describing an *ex post facto* law as one that """that makes an action, done before the passing of the law, and which was innocent when done, criminal; and punishes such action"); *see also Bouie v. City of Columbia*, 378 U.S. 347, 350-54 (1964) ("There can be no doubt that a deprivation of the right of fair warning can result not only from vague statutory language but also from an unforeseeable and retroactive judicial expansion of narrow and precise statutory language.").

2 *General Electric Co. v. U.S. Environmental Protection Agency*, 53 F.3d 1324, 1328 (D.C. Cir. 1995); *see also United States v. Chrysler*, 158 F.3d 1350, 1354-55 (D.C. Cir. 1998) (discussing the "well-established rule in administrative law that the application of a rule may be successfully challenged if it does not give fair warning that the allegedly violative conduct was prohibited"); *Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir.1987) ("Traditional concepts of due process incorporated into administrative law preclude an agency from penalizing a private party for violating a rule without first providing adequate notice of the substance of the rule."); *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C.Cir.1986) (""[T]he due process clause prevents ... the application of a regulation that fails to give fair warning of the conduct it prohibits or requires.").

3 *TerraCom Order* at para. 2.

4 The closest we've come was seven years ago when we adopted protections for another type of confidential information, customer proprietary network information (CPNI). *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007). Nobody thinks those rules extend to PII.

5 None of this should be surprising given the lead role the Federal Trade Commission has taken in recent years regarding the misappropriation, breach, and unlawful disclosure of PII.

6 5 U.S.C. § 553.

7 *TerraCom Order* at para. 52. Although the FCC decides in its grace that a lower figure is "sufficient" in these particular circumstances, *id.*, it also notes that the figure could actually be billions more. *Id.* at note 111.

8 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12515, para. 4 (1996) (*CPNI NPRM*).

9 *Id.*

10 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, para. 194 (1998) (*CPNI Second Order and FNPRM*) ("We recognize, however, that our new CPNI scheme will impose some additional burdens on carriers, particularly carriers not previously subject to our *Computer III* CPNI requirements. We believe, however, that these requirements are not unduly burdensome. All carriers must expend some resources to protect certain information of their customers. Indeed, section 222(a) specifically imposes a protection duty; '[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carries, equipment manufacturers, and customers."DD' (quoting 47 U.S.C. § 222(a)).

11 *Id.* paras. 204-207 (reading section 222(a) in conjunction with 222(b) and 222(c)).

12 *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6931, para. 3 (2007); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1784, para. 4 (2006) (same); *CPNI Second Order and FNPRM*, 13 FCC Rcd, 8061, para. 208 ("In particular, we seek comment on whether the duty in section 222(a) upon all telecommunications carriers to protect the confidentiality of customers' CPNI, or any other provision, permits and/or requires [the Commission] to prohibit the foreign storage or access to domestic CPNI.").

13 *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609, 9617, para. 24 (2013) ("Although it is certainly true that *some* of the information that carriers have collected and stored on mobile devices is not CPNI, it is equally clear that some of it is. In any event, if the information a carrier collects in the future does not meet the statutory definition, then section 222 will not apply. To reiterate, the Commission is clarifying only that information that meets the definition of CPNI is subject to section 222, just as the same information would be subject to section 222 if it were stored elsewhere on a carrier's network.") (internal citations omitted); *see id.* at 9618, para. 27 (section 222(a) helps define where but not what is covered).

14 H.R. Rep. No. 104-458, at 205 (1996) (Conf. Rep.) (emphasis added).

15 47 U.S.C. § 215 (emphasis added).

16 *F.C.C. v. Fox Television Stations, Inc.*, 132 S.Ct. 2307, 2317 (2012) (citing *Connally v. General Constr. Co.*, 269 U.S. 385, 391 (1926)).

17 *Id.* (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)).

18 *Trinity Broadcasting of Florida, Inc., v. FCC*, 211 F.3d 618, 628 (D.C. Cir. 2000) (quoting *General Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995)).

19 *Infinity Broadcasting Corporation of Florida*, File No. EB-04-TP-478, Order on Review, 24 FCC Rcd 4270, 4275, para. 17 (2009) (*quoting Trinity*, 211 F.3d at 628).

20 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6961, para. 70 (2007).

21 While the Commission has previously pursued enforcement actions despite having open rulemaking proceedings, I am concerned that open proceedings may provide companies with a false sense of security. This makes it all the more important that the Commission close open rulemaking proceedings by a date certain or as soon as it determines that it will not act on the open issues.

22 *See, e.g.*, Comments of Verizon, CC Docket No. 96-115, WC Docket No. 04-36, at 15-17 (filed July 9, 2007); Comments of the Rural Cellular Association, CC Docket No. 96-115, WC Docket No. 04-36, at 4-5 (filed July 9, 2007); Comments of the National Cable & Telecommunications Association, CC Docket No. 96-115, WC Docket No. 04-36, at 2 (filed July 9, 2007); Comments of COMPTEL, CC Docket No. 96-115, WC Docket No. 04-36, at 2- 3 (filed July 9, 2007); *but see* Consumer Coalition Comments, CC Docket No. 96-115, WC Docket No. 04-36, at 9- 12 (filed July 9, 2007) (requesting that the FCC require carriers to encrypt stored CPNI and limit employee access to CPNI).

23 *Mullane v. Central Hanover Tr. Co.*, 336 U.S. 306, 313 (1950) ("Many controversies have raged about the cryptic and abstract words of the Due Process Clause but there can be no doubt that at a minimum they require that deprivation of life, liberty or property by adjudication be preceded by notice and opportunity for hearing appropriate to the nature of the case."); *Calder v. Bull*, 3 U.S. 386, 390 (1798) (describing an *ex post facto* law as one that """"that makes an action, done before the passing of the law, and which was innocent when done, criminal; and punishes such action"); *see also Bouie v. City of Columbia*, 378 U.S. 347, 350-54 (1964) ("There can be no doubt that a deprivation of the right of fair warning can result not only from vague statutory language but also from an unforeseeable and retroactive judicial expansion of narrow and precise statutory language.").

24 *General Electric Co. v. U.S. Environmental Protection Agency*, 53 F.3d 1324, 1328 (D.C. Cir. 1995); *see also United States v. Chrysler*, 158 F.3d 1350, 1354-55 (D.C. Cir. 1998) (discussing the "well-established rule in administrative law that the application of a rule may be successfully challenged if it does not give fair warning that the allegedly violative conduct was prohibited"); *Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir.1987) ("Traditional concepts of due process incorporated into administrative law preclude an agency from penalizing a private party for violating a rule without first providing adequate notice of the substance of the rule."); *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986) ("[T]he due process clause prevents ... the application of a regulation that fails to give fair warning of the conduct it prohibits or requires.").

25 *TerraCom Order* at para. 2.

26 The closest we've come was seven years ago when we adopted protections for another type of confidential information, customer proprietary network information (CPNI). *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007). Nobody thinks those rules extend to PII.

27 None of this should be surprising given the lead role the Federal Trade Commission has taken in recent years regarding the misappropriation, breach, and unlawful disclosure of PII.

28 5 U.S.C. § 553.

29 *TerraCom Order* at para. 52. Although the FCC decides in its grace that a lower figure is "sufficient" in these particular circumstances, *id.*, it also notes that the figure could actually be billions more. *Id.* at note 111.

30 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12515, para. 4 (1996) (*CPNI NPRM*).

31 *Id.*

32 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, para. 194 (1998)(*CPNI Second Order and FNPRM*) ("We recognize, however, that our new CPNI scheme will impose some additional burdens on carriers, particularly carriers not previously subject to our *Computer III* CPNI requirements. We believe, however, that these requirements are not unduly burdensome. All carriers must expend some resources to protect certain information of their customers. Indeed, section 222(a) specifically imposes a protection duty; '[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carries, equipment manufacturers, and customers."DD' (quoting 47 U.S.C. § 222(a)).

33 *Id.* paras. 204-207(reading section 222(a) in conjunction with 222(b) and 222(c)).

34 *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6931, para. 3 (2007)*; Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1784, para. 4 (2006) (same); *CPNI Second Order and FNPRM*, 13 FCC Rcd, 8061, para. 208 ("In particular, we seek comment on whether the duty in section 222(a) upon all telecommunications carriers to protect the confidentiality of customers' CPNI, or any other provision, permits and/or requires [the Commission] to prohibit the foreign storage or access to domestic CPNI.").

35 *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609, 9617, para. 24 (2013) ("Although it is certainly true that *some* of the information that carriers have collected and stored on mobile devices is not CPNI, it is equally clear that some of it is. In any event, if the information a carrier collects in the future does not meet the statutory definition, then section 222 will not apply. To reiterate, the Commission is clarifying only that information that meets the definition of CPNI is subject to section 222, just as the same information would be subject to section 222 if it were stored elsewhere on a carrier's network.") (internal citations omitted); *see id.* at 9618, para. 27 (section 222(a) helps define where but not what is covered).

36 H.R. Rep. No. 104-458, at 205 (1996) (Conf. Rep.) (emphasis added).

37 47 U.S.C. § 215 (emphasis added).

38 *F.C.C. v. Fox Television Stations, Inc.*, 132 S.Ct. 2307, 2317 (2012) (citing *Connally v. General Constr. Co.*, 269 U.S. 385, 391 (1926)).

39 *Id.* (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)).

40 *Trinity Broadcasting of Florida, Inc., v. FCC*, 211 F.3d 618, 628 (D.C. Cir. 2000) (quoting *General Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995)).

41 *Infinity Broadcasting Corporation of Florida*, File No. EB-04-TP-478, Order on Review, 24 FCC Rcd 4270, 4275, para. 17 (2009) (*quoting Trinity*, 211 F.3d at 628).

42 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6961, para. 70 (2007).

43 While the Commission has previously pursued enforcement actions despite having open rulemaking proceedings, I am concerned that open proceedings may provide companies with a false sense of security. This makes it all the more important that the Commission close open rulemaking proceedings by a date certain or as soon as it determines that it will not act on the open issues.

44 *See, e.g.*, Comments of Verizon, CC Docket No. 96-115, WC Docket No. 04-36, at 15-17 (filed July 9, 2007); Comments of the Rural Cellular Association, CC Docket No. 96-115, WC Docket No. 04-36, at 4-5 (filed July 9, 2007); Comments of the National Cable & Telecommunications Association, CC Docket No. 96-115, WC Docket No. 04-36, at 2 (filed July 9, 2007); Comments of COMPTEL, CC Docket No. 96-115, WC Docket No. 04-36, at 2-3 (filed July 9, 2007); *but see* Consumer Coalition Comments, CC Docket No. 96-115, WC Docket No. 04-36, at 9-12 (filed July 9, 2007) (requesting that the FCC require carriers to encrypt stored CPNI and limit employee access to CPNI).

29 FCC Rcd. 13325 (F.C.C.), 29 F.C.C.R. 13325, 61 Communications Reg. (P&F) 652, 2014 WL 5439575

30 FCC Rcd. 2808 (F.C.C.), 30 F.C.C.R. 2808, 62 Communications Reg. (P&F) 526, 2015 WL 1577197

Federal Communications Commission (F.C.C.)
Order

IN THE MATTER OF AT&T SERVICES, INC.

File No.: EB-TCD-14-00016243
Acct. No.: 201532170010
FRN: 0005193701
DA 15-399
Released: April 8, 2015
Adopted: April 8, 2015

**1 *2808 By the Chief, Enforcement Bureau:

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission) has entered into a **Consent Decree** to resolve its investigation into whether **AT**&**T** Services, Inc. (**AT**&**T** or Company) failed to properly protect the confidentiality of almost 280,000 customers' proprietary information, including sensitive personal information such as customers' names and at least the last four digits of their Social Security numbers, as well as account-related data known as customer proprietary network information (CPNI), in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines. At least two employees believed to have engaged in the unauthorized access confessed that they sold the information obtained from the breaches to a third party, known to them as "El Pelon." The breaches resulted in the personal information of 51,422 AT&T customers' information being used to place 290,803 handset unlock requests through AT&T's online customer unlock request portal. The investigation also examined whether AT&T promptly notified law enforcement authorities of the security breaches involving its customers' CPNI.

2. The failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act. These laws ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information. The Commission has made clear that it expects telecommunications carriers such as AT&T to take ""every reasonable precaution" to protect their customers' data, and that it is committed to protecting the personal information of American consumers from misappropriation, breach, and unlawful disclosure. In addition, the laws that require prompt disclosure of data breaches to law enforcement authorities, and subsequently to consumers, aid in the pursuit and apprehension of bad actors and provide valuable information that helps affected consumers be proactive in protecting themselves in the aftermath of a data breach. To settle this matter, AT&T will pay a civil penalty of $25,000,000 and develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into AT&T's business practices to protect consumers against similar data breaches in the future. In particular, AT&T will be required to improve its privacy and data security practices by appointing a senior compliance manager who is privacy certified, conducting a privacy risk assessment, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company's privacy policies and the applicable privacy legal authorities.

**2 3. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest would be served by adopting the Consent Decree and terminating the referenced investigation regarding AT&T's compliance with 201(b) and 222 of the Communications Act *2809 of 1934, as amended (Communications Act or Act),[1] and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules[2] in connection with a data breach.

4. In the absence of material new evidence relating to this matter, we conclude that our investigation raises no substantial or material questions of fact as to whether AT&T possesses the basic qualifications, including those related to character, to hold or obtain any Commission license or authorization.

5. Accordingly, **IT IS ORDERED** that, pursuant to Section 4(i) of the Act[3] and the authority delegated by Sections 0.111 and 0.311 of the Rules[4] the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

6. **IT IS FURTHER ORDERED** that the above-captioned matter **IS TERMINATED**.

7. **IT IS FURTHER ORDERED** that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Mr. James Talbot and Ms. Jackie Flemming, AT&T Services, 1120 20th St. NW, Suite 1000, Washington, DC 20036.

FEDERAL COMMUNICATIONS COMMISSION

Travis LeBlanc
Chief
Enforcement Bureau

***2810 CONSENT DECREE**
1. The Enforcement Bureau of the Federal Communications Commission and **AT&T** Services, Inc. (**AT&T** or Company), by their authorized representatives, hereby enter into this **Consent Decree** for the purpose of terminating the Enforcement Bureau's investigation into whether **AT&T** violated Sections 201(b) and 222[1] of the Communications Act of 1934, as amended (Communications Act or Act),[2] and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules[3] in connection with a data breach.

I. DEFINITIONS
2. For the purposes of this Consent Decree, the following definitions shall apply:
(a) "Act" means the Communications Act of 1934, as amended.

(b) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(c) "Affected Customer" means any AT&T customer whose account was accessed without the customer's authorization by an employee of a call center in Colombia or the Philippines for the purpose of obtaining unlock codes.

****3** (d) "AT&T" or "Company" means AT&T Services, Inc., and its affiliates, subsidiaries, predecessors-in-interest, and successors-in-interest.

(e) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(f) "Commission" and "FCC" mean the Federal Communications Commission and all of its bureaus and offices.

(g) "Call Center" means call centers operated by AT&T Mobility or its contractor(s) that provide mobility customer service or wireless sales service for AT&T Mobility consumer customers.

(h) "Communications Laws" means, collectively, the Act, the Rules, and the published and promulgated orders and decisions of the Commission to which AT&T is subject by virtue of its business activities.

***2811** (i) "Compliance Plan" means the compliance obligations, program, and procedures described in this Consent Decree at paragraph 18.

(j) "Covered Employees" means all employees and agents of AT&T who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of Personal Information or Customer Proprietary Network Information at Call Centers managed and operated by AT&T Mobility. Covered Employees do not include Covered Vendor Employees.

(k) "Covered Vendor Employees" means all employees and agents of Vendors who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of Personal Information or CPNI at Vendor Call Centers that provide customer service and wireless sales services for AT&T Mobility customers.

(l) "Customer Proprietary Network Information" and "CPNI" shall have the meaning set forth at Section 222(h)(1) of the Act.

(m) "CPNI Rules" means the rules set forth at 47 C.F.R. § 64.2001 *et seq.* and any amendments or additions to those rules subsequent to the Effective Date.

(n) "Data Breach" means access to a customer's account without authorization for the purpose of obtaining the customer's name, cellular telephone number, and last four digits of the customer's Social Security number to be used to obtain an unlock code.

(o) "Effective Date" means the date by which both the Bureau and **AT&T** have signed the **Consent Decree**.

(p) "Investigation" means the investigation commenced by the Bureau in EB-TCD-14-00016243.

(q) "Operating Procedures" means the standard internal operating procedures and compliance policies established by AT&T to implement the Compliance Plan.

(r) "Parties" means AT&T and the Bureau, each of which is a "Party."

(s) "Personal Information" means either of the following: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver's license number or other government-issued identification card number; or (C) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

**4 (t) "Rules" means the Commission's regulations, found in Title 47 of the Code of Federal Regulations.

(u) "Vendor" means a third-party that operates and/or manages a Call Center on behalf of AT&T Mobility and provides customer service and wireless sales services for AT&T Mobility consumer customers.

***2812 II. BACKGROUND**

3. Section 222(c) of the Act, entitled "Confidentiality of Customer Proprietary Network Information," restricts carriers' use and disclosure of CPNI.[4] Section 222(c)(1) only permits a carrier to disclose, permit access to, or use a customer's individually identifiable CPNI to provide telecommunications services, or other services "necessary to, or used in," the carrier's telecommunications service, unless otherwise authorized by the customer or required by law.[5]

4. The Commission has adopted rules implementing Section 222(c)'s protections of CPNI. Section 64.2010(a) of the Commission's Rules requires that "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[6] Section 64.2011(b) requires a telecommunications carrier to notify designated law enforcement authorities of a "breach" of its customers' CPNI "[a]s soon as practicable, in no event later than seven (7) business days, after reasonable determination of the breach ...."[7] A "breach" occurs "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[8] A telecommunications carrier must provide notice of a breach to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through an online portal.[9]

5. Section 201(b) of the Act states, in part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge,

practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."[10] The Notice of Apparent Liability in *TerraCom* states that Section 201(b) applies to carriers' practices for protecting customers' PII and CPNI.[11]

6. AT&T is a telecommunications carrier that provides mobile voice and data services to customers throughout the United States, with its principal place of business in Dallas, Texas.[12] AT&T is the second largest wireless carrier in the United States, with over 100 million subscribers, earning $126.4 billion in revenue in 2012 and $128.8 billion in 2013.[13]

7. In May 2014, the Enforcement Bureau (Bureau) began investigating an internal Data Breach that occurred between November 2013 and April 2014 at a facility in Mexico under contract with ***2813** AT&T (the April 2014 Breach). The Bureau's investigation[14] into the April 2014 Breach was based on reports submitted by AT&T to the Commission's CPNI Data Breach Portal[15] and publicly available information.[16] AT&T informed the Bureau that it discovered that three employees of an AT&T Vendor that provided Spanish-language customer support services from an inbound Call Center located in Mexico (Mexico Call Center), had used login credentials to access customer accounts to obtain customer information—specifically, names and the last four digits of customers' Social Security numbers—that could then be used to submit online requests for cellular handset unlock codes.[17]

****5** 8. AT&T maintained and operated the systems the Mexico Call Center employees used to access AT&T customer records. These systems were governed by AT&T's data security measures.[18] In this case, those measures failed to prevent or timely detect a large and ongoing Data Breach. The April 2014 Breach lasted 168 days (from November 4, 2013, until April 21, 2014). During this period, the three Mexico Call Center employees accessed 68,701 customers' accounts, without authorization to obtain the above-referenced information required for unlock codes, which appeared on the same account page as these customers' CPNI.[19] Beginning in December 2013, more than 11,000 customer accounts were accessed each month until March 2014.[20] AT&T also determined that the personal information of 51,422 of these customers was used to place 290,803 handset unlock requests through AT&T's online customer unlock request portal.[21] Although CPNI appeared on the same page as the information required for unlock codes, AT&T found no evidence that the Mexico Call Center employees used or disclosed CPNI in connection with the data breach. In December 2012, an AT&T employee became suspicious that an employee at the Mexico Call Center was possibly providing customer information to unauthorized persons.[22] The Mexico Call Center employee was terminated by the Mexico Call Center for accessing customer accounts without leaving account notations.[23] In January 2013, AT&T discovered information ***2814** that another at the Mexico Call Center may have engaged in suspicious activities suggesting access to accounts for an improper purpose.[24] This employee left the Mexico Call Center voluntarily prior to the completion of AT&T's investigation.[25] AT&T did not classify the 2012 and 2013 incidents as CPNI breaches at the time that they occurred because AT&T did not conclude that the breaches included use or disclosure of CPNI. Following the April 2014 Breach, however, AT&T re-examined these incidents and reported them to the USSS and FBI via the CPNI breach reporting portal in September 2014.[26]

9. AT&T commenced its investigation of the April 2014 Breach on April 3, 2014, and notified members of its senior management of the investigation on April 4, 2014.[27] According to AT&T, "it was quickly apparent that the incident potentially involved a high volume of customer account access."[28] AT&T was aware from the outset of its investigation that the customer database that was accessed to perpetrate the suspected breach contained billing information and other CPNI.[29] On April 8, 2014, the Mexico Call Center, in consultation with AT&T, interviewed one of the employees suspected of engaging in the breach, concluded that the employee presented an "evasive attitude" during the interview, and, after conducting a polygraph examination of the employee, severed him from his job functions and began the process to terminate his employment.[30] By April 22, 2014, AT&T had received the imaged hard drives from computers believed to have been involved in the breach, and began its forensic analysis shortly thereafter.[31] On May 20, 2014, AT&T notified the USSS and the FBI of the incident.[32] As noted above, Section 64.2011(b) requires a carrier to notify law enforcement of a CPNI breach "[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach ...."[33] AT&T reported completing notification to customers affected by the breach on July 3, 2014.[34]

****6** 10. AT&T informed the Bureau that it terminated its use of the Mexico Call Center on September 28, 2014.[35]

11. In March 2015, AT&T disclosed to the Bureau that it was investigating additional potential Data Breaches in Colombia and the Philippines. AT&T informed the Bureau that its ***2815** investigation was ongoing but that thus far it had discovered that call center employees in Bogota, Colombia and the Philippines had accessed customer accounts in order to obtain unlock codes for AT&T mobile phones. In Bogota, until May 27, 2014, full Social Security numbers were accessible in the ordinary

course of business to three of the managers whose login credentials were used in these activities. After May 27, 2014, AT&T implemented measures to mask full Social Security numbers for AT&T Mobility Call Center managers. AT&T has found no evidence that these or any other managers in Colombia or the Philippines acquired or used the full Social Security numbers of any Affected Customers. In some cases, certain CPNI relating to bill amounts and rate plans were visible at the time of the unauthorized activity, but AT&T's investigation also found no evidence that this information was used. The unauthorized access ceased in the Bogota, Colombia facility in July 2014. In December 2014, AT&T changed its unlock policy and ceased requiring information from customer records before providing an unlock code. This change eliminated the incentive for Covered Employees or Covered Vendor Employees to engage in the activities described above. AT&T informed the Bureau that based on its investigation to date, it had identified approximately 211,000 customer accounts that were accessed in connection with the unlock code activities in the Colombian and Philippines facilities, but that its ongoing investigation could reveal additional instances of such activities. AT&T informed the Bureau that it is in the process of developing new monitoring procedures to identify suspicious account access by call center representatives.

12. The Parties negotiated the following terms and conditions of settlement and hereby enter into this Consent Decree as provided below.

III. TERMS OF AGREEMENT

13. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order.

14. **Jurisdiction**. AT&T agrees that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree.

15. **Effective Date; Violations**. The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

16. **Termination of Investigation**. In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigation and its investigation into matters described in paragraph 11. In consideration for the termination of the Investigation, AT&T agrees to the terms, conditions, and procedures contained herein. The Bureau further agrees that, in the absence of new material evidence relating to the Investigation, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute any new proceeding, formal or informal, or take any action against AT&T concerning the matters that were the subject of the Investigation, including the matters described in paragraphs 7 through 10, and its investigation into matters described in paragraph 11. The Bureau also agrees that, in the absence of new material evidence relating to the Investigation described in paragraphs 7-10, the investigation into matters described in paragraph 11 and in the absence of any misrepresentation in paragraph 19(a), it will not use the facts developed in the Investigation or its investigation into matters described in paragraph 11 through the Effective Date, or the existence of this Consent Decree, to institute any proceeding, formal or informal, or take any action against AT&T with respect to basic qualifications, including its character qualifications, to be a Commission licensee or hold Commission licenses or authorizations. For purposes of this paragraph, additional instances of unauthorized access to a customer's account in Colombia or the Philippines for the apparent purpose of obtaining an unlock code do not constitute new material evidence. For the purpose of this **Consent Decree** only, **AT&T** does not contest that its actions that were the subject of the Investigation violated Section 222(c) of the Act, and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules. It is the intent of the Parties that this Consent Decree shall not be used as evidence or precedent in any action or ***2816** proceeding, except in an action to enforce the Consent Decree.

****7** 17. **Compliance Officer**. Within thirty (30) calendar days after the Effective Date, AT&T shall designate a senior corporate manager with the requisite corporate and organizational authority to serve as a Compliance Officer and to discharge the duties set forth below. The person designated as the Compliance Officer shall be responsible for developing, implementing, and administering the Compliance Plan and ensuring that AT&T complies with the terms and conditions of the Compliance Plan and this Consent Decree. In addition to the general knowledge of the Communications Laws necessary to discharge his or her duties under this Consent Decree, the Compliance Officer shall have specific knowledge of the information security principles and practices necessary to implement the information security requirements of this Consent Decree, and the specific requirements of Section 222 of the Act, and the CPNI Rules, before assuming his/her duties. The Compliance Officer or managers reporting to the Compliance Officer with responsibilities related to this Consent Decree

shall be privacy certified by an industry certifying organization and keep current through appropriate continuing privacy education courses.

18. **Compliance Plan**. For purposes of settling the matters set forth herein, AT&T agrees that it shall, within ninety (90) calendar days after the Effective Date, develop and implement a Compliance Plan designed to ensure future compliance with the Communications Laws and with the terms and conditions of this **Consent Decree**. **AT&T** will implement, at a minimum, the following procedures:
(a) **Risk Assessment**. Within ninety (90) calendar days after the Effective Date, AT&T shall complete a risk assessment reasonably designed to identify internal risks of unauthorized access, use, or disclosure of Personal Information and CPNI by Covered Employees and Covered Vendor Employees (Risk Assessment). The Risk Assessment must evaluate the sufficiency of existing policies, procedures, and other safeguards in place to control the risk of such unauthorized access, use, or disclosures.

(b) **Information Security Program**. Within ninety (90) calendar days after the Effective Date, AT&T shall have in place and thereafter maintain an information security program reasonably designed to protect CPNI and Personal Information from unauthorized access, use, or disclosure by Covered Employees and Covered Vendor Employees (Information Security Program). AT&T shall ensure that the Information Security Program is fully documented in writing (including, as appropriate, within the Operating Procedures/Compliance Manual described below) and includes: (i) administrative, technical, and physical safeguards reasonably designed to protect the security and confidentiality of Personal Information and CPNI; (ii) reasonable measures to protect Personal Information and CPNI maintained by or made available to Vendors, Covered Employees, and Covered Vendor Employees, including exercising due diligence in selecting Vendors, requiring Vendors by contract to implement and maintain administrative, technical, and physical safeguards for the protection of Personal Information and CPNI, and engaging in ongoing monitoring of Vendors' compliance with their security obligations and implementing measures to sanction Vendors that fail to comply with their security obligations (including, where appropriate, terminating AT&T's relationship with such Vendors); (iii) access controls reasonably designed to limit access to Personal Information and CPNI to authorized AT&T employees, agents, and Covered Vendor Employees; (iv) reasonable processes to assist AT&T in detecting and responding to suspicious or anomalous account activity, including whether by malware or otherwise, involving Covered Employees and Covered Vendor Employees: (v) a comprehensive breach response plan that will enable AT&T to fulfill its obligations under applicable laws, with regard to breach ***2817** notifications, including its obligations under paragraph 20 while that paragraph remains in effect.

****8** (c) **Ongoing Monitoring and Improvement**. AT&T shall monitor its Information Security Program on an ongoing basis to ensure that it is operating in a manner reasonably calculated to control the risks identified through the Risk Assessment, to identify and respond to emerging risks or threats, and to comply with the requirements of Section 222 of the Act, the CPNI Rules, and this Consent Decree. To the extent that such monitoring reveals that the program is deficient or no longer reasonably fulfills this purpose, AT&T shall implement additional safeguards to address these deficiencies and gaps. Such additional safeguards shall be implemented within a reasonable period of time, taking into account the seriousness of the deficiencies or gaps and the steps necessary to address them.

(d) **Compliance Review**. Within ninety (90) calendar days after the Effective Date, AT&T shall commence a formal internal review of its Information Security Program using procedures and standards generally accepted in the information privacy field. This formal internal review shall be directed by AT&T's Corporate Compliance Unit by professionals with the requisite privacy certifications necessary to review and assess information security programs. Such assessment shall be completed within one hundred and fifty (150) calendar days after the Effective Date, and AT&T shall submit a copy of the written assessment findings to the Commission within ten (10) calendar days of the assessment's completion.

(e) **Compliance Manual**. Within one hundred and twenty (120) calendar days after the Effective Date, the Compliance Officer shall develop and distribute a Compliance Manual to all Covered Employees and to all Vendors with instructions to Vendors to distribute a copy of the Compliance Manual to all Covered Vendor Employees within thirty (30) days and to certify that such distribution has been completed. If such certification is not provided, AT&T will pursue any remedy available to require distribution and certification, including, if necessary, termination of the relationship. Additionally, AT&T shall instruct all Vendors to deliver a Compliance Manual to all future Covered Vendor Employees within thirty (30) calendar days after such future Covered Vendor Employee assumes such position or responsibilities.

(f) The Compliance Manual shall explain the requirements of Sections 222 of the Act, the CPNI Rules, and this Consent Decree, and set forth the Operating Procedures that Covered Employees and Covered Vendor Employees shall follow to help ensure AT&T's compliance with the Act, Rules, and this **Consent Decree**. **AT&T** shall periodically review and revise the Compliance Manual and Operating Procedures as necessary to ensure that the information set forth therein remains current and accurate. AT&T shall distribute any revisions to the Compliance Manual to all Covered Employees and all Vendors within thirty (30) calendar days of making such revisions.

9 (g) **Compliance Training Program. AT&T shall establish and implement a Compliance Training Program on compliance with Section 222, the CPNI Rules, and the Operating Procedures. As part of the Compliance Training Program Covered Employees shall be advised of AT&T's reporting obligations under paragraph 20 of this Consent Decree and shall be instructed on how to disclose noncompliance with Section 222, the CPNI Rules and the Operating Procedures to the Compliance Officer or his designees. All Covered Employees shall be trained pursuant to the Compliance Training program within six (6) months after the Effective Date, and, any person who becomes a Covered Employee at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar *2818 days after the date such person becomes a Covered Employee. AT&T shall repeat compliance training on an annual basis, and shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness. AT&T shall request, and where permitted by contract require, all Vendors to provide the training to all Covered Vendor Employees within six (6) months after the Effective Date, except that any person who becomes a Covered Vendor Employee at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar days after the date such person becomes a Covered Vendor Employee. AT&T shall request, and where permitted by contract, require Vendors to repeat compliance training on an annual basis.

19. **Terms Specific to Call Centers in Colombia and the Philippines**.
(a) AT&T represents and warrants that it engaged independent third parties to investigate the activities in Bogota, Colombia and to assist with employee interviews in connection with AT&T's investigation of call centers in the Philippines. AT&T further represents and warrants that it has no evidence and no reason to believe that any CPNI or any Personal Information was obtained or used during the course of the activities described in paragraphs 7-11, AT&T further represents and warrants that, effective December 11, 2014, it changed its device unlock policy and no longer requires information contained in AT&T customer records in order to obtain an unlock code, thereby eliminating the incentive for the activities described in paragraphs 7-11. After reasonable diligence, and based on information currently available, including AT&T's change in its unlock policy, AT&T believes that the activities described in paragraph 11 have ceased. AT&T further represents and warrants that it has reported to the Bureau all known instances in which it has reasonably concluded that a Data Breach occurred in Colombia and Philippines call centers. AT&T further represents and warrants that it is continuing to investigate call centers in Colombia and the Philippines for Data Breaches.

**10 (b) Within thirty (30) calendar days of the Effective Date, AT&T shall:
i. Begin a process to provide each Affected Customer written notice that his or her account, including Personal Information and/or CPNI, had been accessed by persons without authorization in violation of AT&T's privacy and security policies and include an offer of one year of complimentary credit monitoring services through a nationally recognized credit monitoring service, such as CSID Protector. The complimentary credit monitoring services offered to each Affected Customer shall include, at a minimum, single bureau credit report and monitoring; court record monitoring and public records searches; non-credit loan searches; identity theft insurance at no cost to Affected Customers; and full service identity theft restoration services. Each written notice provided to Affected Customers shall include the toll-free telephone numbers and web addresses of the major credit reporting agencies. AT&T shall complete such notification within 60 days.

ii. AT&T shall provide a toll-free number where Affected Customers may contact AT&T with questions about the impact of these activities, if any, on their account information.

*2819 iii. Subparagraphs 19(b)(i)-(ii) shall also apply to Affected Customers who are identified after the Effective Date and AT&T shall provide the notice required pursuant to subparagraph 19(b) to such customers within thirty (30) calendar days of AT&T's discovery that such customers' accounts were illegally accessed.

20. **Reporting Noncompliance and Data Breaches**. AT&T shall report any noncompliance with the terms and conditions of this Consent Decree within fifteen (15) calendar days after discovery of such noncompliance. Such reports shall include a detailed explanation of: (i) each known instance of noncompliance; (ii) the steps that AT&T has taken or will take to remedy such noncompliance; (iii) the schedule on which such remedial actions will be taken; and (iv) steps that AT&T has taken or will take to prevent the recurrence of any such noncompliance. AT&T shall also report to the FCC any breaches of Personal Information or CPNI involving any Covered Employees or Covered Vendor Employees that AT&T is required by any federal or state law to report to any Federal or state entity or any individual. Reports shall be submitted no later than seven (7) business days after completion of the notification required by federal or state authorities. Such reports shall include (i) the date the breach was reported, (ii) the applicable Federal and state authorities to whom the breach was reported, (iii) copies of the reports AT&T submitted to the applicable state authorities, and (iv) the reference number generated by the central reporting facility for CPNI reports made pursuant to 47 C.F.R. § 64.2011(b). All reports of noncompliance shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4C-224, Washington, DC 20554, with copies submitted electronically to David.Valdez@fcc.gov and Michael.Epshteyn@fcc.gov. The foregoing reporting requirement does not affect AT&T's obligations to report data breaches to other regulatory authorities in accordance with applicable law.

11 21. **Compliance Reports. AT&T shall file compliance reports with the Commission six (6) months after the Effective Date, twelve (12) months after the Effective Date, twenty-four (24) months after the Effective Date, and thirty-six (36) months after the Effective Date.
(a) Each Compliance Report shall include a detailed description of AT&T's efforts during the relevant period to comply with the terms and conditions of this Consent Decree. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of AT&T, stating that the Compliance Officer has personal knowledge that AT&T: (i) has established and implemented the Compliance Plan; (ii) has utilized the Operating Procedures since the implementation of the Compliance Plan; and (iii) is not aware of any instances of noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in paragraph 20 of this Consent Decree.

(b) The Compliance Officer's certification shall be accompanied by a statement explaining the basis for such certification and shall comply with Section 1.16 of the Rules and be subscribed to as true under penalty of perjury in substantially the form set forth therein.[36]

(c) If the Compliance Officer cannot provide the requisite certification, the Compliance Officer, as an agent of and on behalf of AT&T, shall provide the Commission with a detailed explanation of the reason(s) why and describe fully: (i) each instance of noncompliance; (ii) the steps that AT&T has taken or will take to remedy such noncompliance, including the schedule on which proposed remedial actions will be taken; and (iii) the steps that AT&T has taken or will take to prevent the recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

*2820 (d) All Compliance Reports shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4C-224, Washington, DC 20554, with a copy submitted electronically to David.Valdez@fcc.gov and Michael.Epshteyn@fcc.gov.

22. **Termination Date**. With the exception of paragraphs 18(b)-(c), the requirements set forth in paragraphs 17 through 21 of this Consent Decree shall expire thirty-six (36) months after the Effective Date. The requirements set forth in paragraphs 18(b)-(c) shall expire seven (7) years after the Effective Date.

23. **Section 208 Complaints; Subsequent Investigations**. Nothing in this Consent Decree shall prevent the Commission or its delegated authority from adjudicating complaints filed pursuant to Section 208 of the Act[37] against AT&T or its affiliates for alleged violations of the Act, or for any other type of alleged misconduct, regardless of when such misconduct took place. The Commission's adjudication of any such complaint will be based solely on the record developed in that proceeding. Except as expressly provided in this Consent Decree, this Consent Decree shall not prevent the Commission from

investigating new evidence of noncompliance by AT&T with the Communications Laws.

12 24. **Civil Penalty. AT&T will pay a civil penalty to the United States Treasury in the amount of $ 25 million ($25,000,000) within thirty (30) calendar days after the Effective Date. AT&T shall send electronic notification of payment to Johnny Drake, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission at Johnny.Drake@fcc.gov on the date said payment is made. The payment must be made by check or similar instrument, wire transfer, or credit card, and must include the Account Number and FRN referenced above. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.[38] When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in block number 24A (payment type code). Below are additional instructions that should be followed based on the form of payment selected:
· Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank — Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

· Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.

· Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank — Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

Questions regarding payment procedures should be addressed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES @fcc.gov.

*2821 25. **Waivers**. As of the Effective Date, AT&T waives any and all rights it may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this **Consent Decree** and the Adopting Order. **AT&T** shall retain the right to challenge Commission interpretation of the **Consent** Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the **Consent Decree** or the Adopting Order, neither **AT&T** nor the Commission shall contest the validity of the **Consent Decree** or the Adopting Order, and **AT&T** shall waive any statutory right to a trial *de novo*. AT&T hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act[39] relating to the matters addressed in this Consent Decree.

13 26. **Severability. The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

27. **Invalidity**. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

28. **Subsequent Rule or Order**. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or Order adopted by the Commission (except an Order specifically intended to revise the terms of this **Consent Decree** to which **AT&T** does not expressly **consent**) that provision will be superseded by such Rule or Order.

29. **Successors and Assigns**. **AT&T** agrees that the provisions of this **Consent Decree** shall be binding on its successors, assigns, and transferees.

30. **Final Settlement**. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigation.

31. **Modifications**. Except as provided in paragraph 27, this Consent Decree cannot be modified without the advance written consent of both Parties.

32. **Paragraph Headings**. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

33. **Authorized Representative**. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

***2822** 34. **Counterparts**. This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

___

Travis LeBlanc, Chief

Enforcement Bureau

___

Date

For: AT&T Services, Inc.

___

Debbie Storey

Executive Vice President — Mobility Customer Service

AT&T Services, Inc.

___

Date

Footnotes

1 *See* 47 U.S.C. §§ 201, 222.

2 *See* 47 C.F.R. §§ 64.2010(a), 64.2011(b).

3 47 U.S.C. § 154(i).

4 47 C.F.R §§ 0.111, 0.311.

1 47 U.S.C. §§ 201(b), 222.

2 47 U.S.C. § 151 *et seq.*

3 47 C.F.R. §§ 64.2010(a), 64.2011(b).

4 *See* 47 U.S.C. § 222(c).

5 *Id.* at § 222(c)(1).

6 47 C.F.R. § 64.2010(a).

7 47 C.F.R. § 64.2011(b).

8 47 C.F.R. § 64.2011(e).

9 47 C.F.R. § 64.2011(b). The Commission maintains a link to the portal at http://www.fcc.gov/eb/cpni. Telecommunications carriers are required to report CPNI data breaches via the online portal accessible through that site. The data reported through the FCC portal is collected by U.S. Secret Service and the Federal Bureau of Investigation.

10 47 U.S.C. § 201(b).

11 *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13335-36, paras. 31-32 (2014).

12 AT&T is an interexchange carrier (499 Filer ID Number: 806172). New Cingular Wireless Services, Inc. CONSOLIDATED, is listed as providing Cellular/PCS/SMR services and doing business as AT&T Mobility (499 Filer ID Number: 821002). AT&T's principal place of business is located at 208 S. Akard Street, Dallas, TX 75202. Randall Stephenson is the Chief Executive Officer.

13 *See AT&T's 2013 Annual Report*, http://www.att.com/Investor/ATT_ Annual/2013/financial_highlights.html (lasted visited Jan. 20, 2015).

14 The Bureau issued two Letters of Inquiry (LOIs) to AT&T, seeking information about the April 2014 Breach, other reported security breaches, and AT&T's data security practices generally. *See* Letter from Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Jackie Flemming, AT&T Services, Inc. (June 30, 2014) (on file in

EB-TCD-14-00016243); *see also* Letter from Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Jackie Flemming, AT&T Services, Inc. (November 7, 2014) (on file in EB-TCD-14-00016243). AT&T responded to the LOI on July 29, 2014. *See* Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (July 29, 2014) (on file in EB-TCD-14-00016243) (LOI Response). AT&T submitted a response to the Supplemental LOI on December 8, 2014. *See* Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Dec. 8, 2014) (on file in EB-TCD-14-00016243) (Supplemental LOI Response).

15 *See supra* note 9.

16 AT&T reported the April 2014 Breach to the California Attorney General. *See* Submitted Breach Notification Sample, State of California Department of Justice, Office of the Attorney General, http:// oag.ca.gov/ecrime/databreach/reports/sb24-45415 (lasted visited Dec. 19, 2014); *see also* Martyn Williams, *AT&T says customer data accessed to unlock smartphones*, ITworld (June 12, 2014), http:// www.itworld.com/article/2695622/security/at-t-says-customer-data-accessed-to-unlock-smartphones.html (last visited Jan. 29, 2015).

17 *See* LOI Response at 19.

18 *See* Supplemental LOI Response at 6.

19 *See* LOI Response at 5-6, 20.

20 *See* LOI Response at 5.

21 *See* LOI Response at 21.

22 *See* Supplemental LOI Response at 8-9.

23 *See* Supplemental LOI at 9.

24 *Id.*

25 *Id.*

26 *See* Supplemental LOI Response at 8-9. In December 2014, AT&T identified additional customer accounts that appeared to have been accessed by these employees in 2012. AT&T treated these incidents as CPNI breaches and reported them via the online

portal. *See* Supplemental LOI Response at 9-10.

27 *See* LOI Response at 6.

28 LOI Response at 15.

29 *See* LOI Response at 1.

30 *See* LOI Response at 17.

31 *See* LOI Response at 17.

32 *See* LOI Response at 20.

33 47 C.F.R. § 64.2011(b).

34 *See* LOI Response at 7. AT&T determined that approximately 156 prepaid customers, however, did not have valid physical addresses or email addresses and those customers were notified via SMS message on July 10, 2014.

35 *See* Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Jan. 23, 2015) (on file in EB-TCD-14-00016243); *see also* e-mail from James Talbot, Attorney, AT&T Services, Inc., to Rosemary Cabral, Attorney-Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Jan. 27, 2015, 15:42 EDT).

36 *See* 47 C.F.R. § 1.16.

37 47 U.S.C. § 208.

38 An FCC Form 159 and detailed instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

39 *See* 5 U.S.C. § 504; 47 C.F.R. §§ 1.1501-1.1530.

30 FCC Rcd. 2808 (F.C.C.), 30 F.C.C.R. 2808, 62 Communications Reg. (P&F) 526, 2015 WL 1577197

End of Document

30 FCC Rcd. 7075 (F.C.C.), 30 F.C.C.R. 7075, 62 Communications Reg. (P&F) 1618, 2015 WL 4159266

Federal Communications Commission (F.C.C.)
Order

IN THE MATTER OF TERRACOM, INC., AND YOURTEL AMERICA, INC.

File Nos.: EB-TCD-13-00009175, EB-IHD-13-00010677
NAL/Acct. No.: 201432170015
FRN: 0010103745 and 0008410409
DA 15-776
Released: July 9, 2015
Adopted: July 9, 2015

**1 *7075 By the Chief, Enforcement Bureau:

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission has entered into a Consent Decree resolving its investigation into whether TerraCom, Inc. (TerraCom), and YourTel America, Inc. (YourTel) (collectively, the Companies) failed to protect the confidentiality of proprietary information that they received from customers applying to demonstrate eligibility for their low-income Lifeline phone services, including sensitive personal information such as names, addresses, dates of birth, full or partial Social Security numbers, and driver's licenses. The Companies' vendor stored the proprietary information of more than 300,000 customers in clear, readable text on servers that were accessible over the Internet, and the data was not password protected or encrypted. The Companies' failure to provide reasonable protection resulted in a data breach which exposed their customer's personal information to unauthorized individuals. After learning that a news reporter had discovered the breach and was preparing to publish an article, TerraCom and YourTel notified the Bureau of the breach.

2. The failure to reasonably secure customers' proprietary information violates a carrier's duty under the Communications Act and also constitutes an unjust and unreasonable practice in violation of the Act. These duties ensure that consumers can trust that carriers have taken appropriate steps to prevent unauthorized persons from accessing, viewing or misusing their personal information. The Commission has made clear that it expects telecommunications carriers such as TerraCom and YourTel to take "every reasonable precaution" to protect their customers' data, and that it is committed to protecting the personal information of American consumers from misappropriation, breach, and unlawful disclosure.

3. The Consent Decree also resolves the Bureau's investigation into whether YourTel violated the Commission's rules by failing to timely de-enroll ineligible subscribers from its Lifeline service after the Universal Service Administrative Company instructed it to do so. The Commission's rules and orders governing Lifeline specify that eligible telecommunications carriers are permitted to receive universal service support reimbursement only for each qualifying low-income consumer they serve. Eligibility and de-enrollment rules ensure that universal service support is not directed towards consumers who may be ineligible for Lifeline, thereby protecting the integrity of this important Universal Service Fund program.

4. To settle this matter, TerraCom and YourTel will pay a civil penalty of $3,500,000, for which they are jointly and severally liable, and will develop and implement a compliance plan to ensure appropriate procedures are incorporated into the Companies' business practices to protect consumers against similar data breaches in the future. In particular, TerraCom and YourTel will be required to improve their privacy and data security practices by: (i) designating a senior corporate manager who is a certified privacy professional; (ii) conducting a privacy risk assessment; (iii) implementing a written information security program; (iv) maintaining reasonable oversight of third party vendors; (v) **7076 implementing a data breach response plan; and (vi) providing privacy and security awareness training to employees. Additionally, YourTel will be required to implement a compliance plan to improve its compliance with the Lifeline eligibility and de-enrollment rules. TerraCom and YourTel will also file regular compliance reports with the FCC.

**2 5. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest

would be served by adopting the Consent Decree and terminating the referenced investigation regarding TerraCom's and YourTel's compliance with 201(b) and 222(a) of the Communications Act of 1934, as amended (Act),[1] as well as the referenced investigation regarding whether YourTel violated Sections 54.405, 54.407, and 54.409 of the Commission's rules and its orders governing the provision of Lifeline service to low-income consumers.[2]

6. In the absence of material new evidence relating to this matter, we do not set for hearing the question of TerraCom's or YourTel's basic qualifications to hold or obtain any Commission license or authorization.[3]

7. Accordingly, **IT IS ORDERED** that, pursuant to Sections 4(i) and 503(b) of the Act[4] and the authority delegated by Sections 0.111 and 0.311 of the Rules,[5] the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

8. **IT IS FURTHER ORDERED** that the above-captioned investigations **ARE TERMINATED**.

9. **IT IS FURTHER ORDERED** that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Dale Schmick, Chief Operating Officer, TerraCom, Inc., 401 E. Memorial, Ste 400, Oklahoma City, OK 73114-2282, to Dale Schmick, Chief Operating Officer, YourTel America, Inc., 2800 E. 18th Street, Kansas City, MO 64127-2610, and to Peter Karanjia, Esq., Davis Wright Tremaine LLP, 1919 Pennsylvania Avenue, NW, Suite 800, Washington, DC 20006.

FEDERAL COMMUNICATIONS COMMISSION

Travis LeBlanc
Chief
Enforcement Bureau

EB IHD 13-00010677[1]

***7077 CONSENT DECREE**

1. The Enforcement Bureau of the Federal Communications Commission, TerraCom, Inc. (TerraCom), and YourTel America, Inc. (YourTel), by their authorized representatives, hereby enter into this Consent Decree for the purpose of terminating the Enforcement Bureau's investigation into whether TerraCom and YourTel violated Sections 201(b) and 222(a) of the Communications Act of 1934, as amended,[2] and whether YourTel violated Sections 54.405, 54.407, and 54.409 of the Commission's rules and its orders governing the provision of Lifeline service to low-income customers.[3]

I. DEFINITIONS

****3** 2. For the purposes of this Consent Decree, the following definitions shall apply:

(a) "Act" means the Communications Act of 1934, as amended.[4]

(b) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(c) "Affected Customer" means any Customer whose PI was potentially accessible to unauthorized third parties in connection with the data breach that was the subject of the Investigation.[5]

(d) "Affiliate" shall have the same meaning defined in Section 153(2) of the Communications Act, 47 U.S.C. § 153(2).

***7078** (e) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(f) "Commission" and "FCC" mean the Federal Communications Commission and all of its bureaus and offices.

(g) "Communications Laws" means, collectively, the Act, the Rules, and the published and promulgated orders and decisions of the Commission to which TerraCom and YourTel are subject by virtue of their business activities.

(h) "Compliance Plan for Sections 201(b) and 222(a) of the Act" means the compliance obligations, programs, and procedures described in this Consent Decree at paragraph 22.

(i) "Compliance Plan for Lifeline Eligibility and De-Enrollment Rules" means the compliance obligations, programs, and procedures described in this Consent Decree at paragraph 23.

(j) "Compliance Plans" as used in this Consent Decree means the Compliance Plan for Sections 201(b) and 222(a) of the Act and the Compliance Plan for Lifeline Eligibility and De-Enrollment Rules.

(k) "Compliance Training Program for Sections 201(b) and 222(a) of the Act" means the workforce training program described in this Consent Decree at paragraph 22(j).

(l) "Compliance Training Program for Lifeline Eligibility and De-Enrollment Rules" means the workforce training program described in this Consent Decree at paragraph 23(c).

(m) "Covered Employees" means all employees of each of TerraCom and YourTel who perform, supervise, oversee, or manage the performance of, duties that relate to TerraCom's or YourTel's responsibilities under the Communications Laws, including, with respect to the Compliance Plans described herein, Sections 201(b) and 222(a) of the Act and the Lifeline Eligibility and De-Enrollment Rules, respectively.

(n) "Covered Third Party" means any Person that performs services involving the collection, transmission, retrieval, processing, or storage of PI, or any duties that relate to the Lifeline Eligibility and De-Enrollment Rules, pursuant to a contractual relationship or agreement with TerraCom, YourTel, or any Person that they own or control.

(o) "Covered Third Party Employees" means all employees of any Covered Third Party who perform, supervise, oversee, or manage the performance of, duties that relate to TerraCom's or YourTel's responsibilities under the Communications Laws, including Sections 201(b) and 222(a) of the Act and the Lifeline Eligibility and De-Enrollment Rules.

**4 (p) "Customer" means any current or former subscriber of and/or applicant for TerraCom's or YourTel's Lifeline services or any other service subject to the Communications Laws.

(q) "Effective Date" means the date by which the Bureau and TerraCom and YourTel have signed the Consent Decree.

(r) "ETC" means an eligible telecommunications carrier designated under, or operating pursuant to, Section 214(e) of the Communications Act, as amended, 47 U.S.C. § 214(e), as eligible to offer and receive support for one or more services that are *7079 supported by federal universal service support mechanisms pursuant to Section 254(e) of the Act, 47 U.S.C. § 254(e).

(s) "Investigation" means the investigation commenced by the Bureau in File No. EB-TCD-13-00009175 regarding whether TerraCom and YourTel violated Sections 201(b) and 222(a) of the Act, and the investigation commenced by the Bureau in File No. EB-IHD-13-00010677 regarding whether YourTel violated the Lifeline Eligibility and De-Enrollment Rules.

(t) "Lifeline Eligibility and De-Enrollment Rules" means Sections 54.405, 54.407, and 54.409 of the Rules, 47 C.F.R. §§ 54.405, 54.407, 54.409; *Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656 (2012) (*Lifeline Reform Order*); and *Lifeline and Link Up Reform and Modernization*, Report and Order, 26 FCC Rcd 9022 (2011) (*Lifeline Duplicates Order*).

(u) "Operating Procedures" means the standard internal operating procedures and compliance policies established by TerraCom and YourTel to implement the Compliance Plans.

(v) "Parties" means TerraCom, YourTel, and the Bureau, each of which is a "Party."

(w) "Person" shall have the same meaning defined in Section 153(39) of the Communications Act, 47 U.S.C. § 153(39).

(x) "Proprietary Information" or "PI" means all types of Customer information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy; including but not limited to such confidential information as privileged information, trade secrets, and personally identifiable information—information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PI includes, but is not limited to, information such as a consumer's (i) first and last name; (ii) home or other physical address; (iii) email address or other online contact information, such as an instant messaging screen name that reveals an individual's email address; (iv) telephone number; (v) Social Security Number, tax identification number, passport number, driver's license number, or any other government-issued identification number that is unique to an individual; (vi) account numbers, credit card numbers, and any information combined that would allow access to the consumer's accounts; (vii) Uniform Resource Locator ("URL") or Internet Protocol ("IP") address or host name that identifies an individual; or (viii) any combination of the above.

**5 (y) "Rules" means the Commission's regulations found in Title 47 of the Code of Federal Regulations.

(z) "TerraCom" means TerraCom, Inc., its Affiliates, subsidiaries, predecessors-in-interest, and successors-in-interest.

(aa) "USAC" means the Universal Service Administrative Company.

(bb) "YourTel" means YourTel America, Inc., its Affiliates, subsidiaries, predecessors-in-interest, and successors-in-interest.

II. BACKGROUND

A. Sections 201(b) and 222(a) of the Communications Act

3. Section 222(a) of the Act, entitled "Privacy of Customer Information," imposes a duty on every telecommunications carrier "to protect the confidentiality of proprietary information of, and relating *7080 to ... customers.""[6] The Commission has made clear that Section 222(a) requires carriers to "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information"[7] and that it was "committing to taking resolute enforcement action to ensure that the goals of [S]ection 222 are achieved."[8] In the *TerraCom/YourTel NAL*, the Commission found that, pursuant to Section 222(a), the term " proprietary information" broadly encompasses all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy.[9] The Commission found that "proprietaryinformation" broadly encompasses such confidential information as privileged information, trade secrets, and personally identifiable information—information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.[10]

4. Section 201(b) of the Act states, in pertinent part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [[interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."[11] The Commission has interpreted Section 201(b) to apply to carriers' practices for protecting PI.[12] Specifically, in the *TerraCom/YourTel NAL*, the Commission found that Section 201(b) requires companies to employ just and reasonable data security practices to protect consumers' PI against unauthorized access, use, or disclosure.

5. TerraCom and YourTel are common carriers providing telecommunications services as Eligible Telecommunications Carriers (ETCs) participating in the federal Universal Service Fund (USF or Fund) Lifeline program.[13] TerraCom and YourTel have certain common shareholders, share key management employees,[14] and are joint owners of a third company, BrightStar Global Solutions, LLC,[15] but are separate corporate entities headquartered in Oklahoma and Missouri, respectively.

**6 6. In connection with evaluating Customers' eligibility for Lifeline services, TerraCom and YourTel collected a variety of sensitive information and documents.[16] Customers were required to *7081 submit, among other things, their name, address, date of birth, full or partial social security number, and copies of their driver's license or state ID card.[17] TerraCom and YourTel also collected additional information from Customers, such as one or more of the following: proof of participation in

the Supplemental Nutrition Assistance Program; annual statement of government benefits; prior year's state, federal or Tribal tax return; paycheck stubs; Social Security benefit statements; Veterans Administration benefit statements; retirement or pension information; Unemployment or Workers' Compensation benefit statements; Federal or Tribal notice letters of participation in General Assistance; divorce decrees or child support awards; or other official documents establishing the applicant's income level or participation in a relevant program.[18]

7. Customers submitted their information to TerraCom and YourTel via electronic application forms, and supplemented their applications with scanned images of the supporting documentation described in paragraph 6. TerraCom and YourTel state that they relied on a third-party vendor to securely store this information in a manner that would be accessible only to authorized persons (including representatives of YourTel and TerraCom). TerraCom and YourTel further state that although the third-party vendor implemented various security measures to protect Customers' sensitive information, including using firewalls and encrypting a database containing Customer names, it inadvertently failed to implement password protection for some of the stored data while updating its servers. Accordingly, as described in the *TerraCom/YourTel NAL*, the PI of more than 300,000 Customers was accessible over the public Internet.[19] Specifically, this information was stored in clear, readable text on servers that were accessible over the Internet, and the data was not password protected or encrypted. Further, in storing the Lifeline Customers' information and documents, certain of the URLs used by the vendor contained the names of the Customers in plain text.

8. On May 7, 2013, TerraCom and YourTel contacted the Bureau and reported a data breach. On June 17, 2013, the Bureau initiated an investigation into the compromised PI and the associated data breach. On October 24, 2014, the Commission released the *TerraCom/YourTel NAL*, charging each of TerraCom and YourTel with violating:
(a) Section 222(a) of the Act by failing to protect the confidentiality of PI that Customers provided to demonstrate eligibility for Lifeline services;

(b) Section 201(b) of the Act by engaging in unjust and unreasonable practices by failing to employ reasonable data security practices to protect Customers' PI;

(c) Section 201(b) of the Act by representing in their privacy policies that they protected Customers' PI, when in fact they did not; and

****7** (d) Section 201(b) of the Act by engaging in unjust and unreasonable practices by failing to notify all Customers whose PI could have been breached by TerraCom's or YourTel's inadequate data security practices.

B. Lifeline Eligibility and De-Enrollment Rules

9. Lifeline is a USF program that helps ensure that qualifying consumers have the opportunities and security that phone service brings, including being able to connect to jobs, family members, and emergency services.[20] ETCs designated pursuant to the Act provide Lifeline service to consumers.[21] ***7082** Under the Lifeline program rules, ETCs provide discounted service to qualifying consumers and may seek and receive reimbursement from the USF for the revenue they forgo as a result of the discount.[22]

10. The Commission's Lifeline rules establish explicit requirements that an ETC must meet to receive federal Lifeline support.[23] Section 54.407(a) of the Commission's rules requires that Lifeline support "shall be provided directly to an eligible telecommunications carrier, based on the number of actual qualifying low-income consumers it serves."[24] Pursuant to Section 54.407(b), an ETC may receive Lifeline support only for "each qualifying low-income consumer served."[25] A low-income consumer is ""qualifying" only if he or she meets the eligibility criteria set forth in Section 54.409, including the requirement that he or she "must not already be receiving a Lifeline service."[26]

11. An ETC providing qualifying low-income customers with Lifeline discounts files, on a periodic basis, FCC Form 497 with USAC to request reimbursement for providing service at the discounted rates. An ETC's FCC Form 497 documents the number of qualifying low-income customers served and the total amount of Lifeline support claimed by the ETC during the specified time period. Section 54.407(d) provides that an ETC may receive reimbursement from the Fund only if it certifies as part of its reimbursement request that it is in compliance with the Lifeline rules.[27] An ETC may revise its Form 497 data

within 12 months after the data are submitted.[28]

12. If USAC determines that an ETC is providing Lifeline-discounted service to a subscriber who is also receiving service from another ETC, USAC notifies the subscriber in writing, giving him or her an ***7083** opportunity to select a single Lifeline service provider; if the subscriber does not make a selection, USAC designates a single ETC to serve as the subscriber's default Lifeline carrier. USAC then notifies the other ETC(s) in writing and directs them to de-enroll subscribers already receiving Lifeline service. USAC includes a spreadsheet with its notification identifying the subscribers each ETC must de-enroll. Pursuant to Section 54.405(e)(2), the ETC must de-enroll the subscriber within five business days of the notification letter.[29]

****8** 13. YourTel provides wireless Lifeline telephone service as an ETC in the following eight states: Illinois, Kansas, Maine, Missouri, Oklahoma, Pennsylvania, Rhode Island, and Washington.[30] YourTel offers wireless service to consumers by using a combination of its own facilities, leased wireline facilities, and the wholesale wireless services of Sprint Spectrum, LLC, and Cellco Partnership d/b/a Verizon Wireless.[31] YourTel also provides wireline Lifeline service in Illinois, Kansas, Missouri, and Oklahoma.[32]

14. On October 12, 2012, USAC directed YourTel to de-enroll a group of its Lifeline subscribers in Illinois.[33] Subsequently, USAC examined YourTel's Illinois subscriber data for November 2012 and found that YourTel had failed to de-enroll some of those subscribers. USAC referred the matter to the Bureau, which initiated an investigation by issuing a Letter of Inquiry (*LOI*) to YourTel on July 11, 2013.[34] YourTel responded to the *LOI* on August 12, 2013.[35] In its response, YourTel admitted that it did not timely de-enroll the subscribers due to a "system error."[36] According to YourTel, the underlying carrier whose service YourTel resold did not convert all of the subscribers to non-Lifeline plans within the requisite time period.[37] USAC confirmed that YourTel subsequently revised its Forms 497 to reimburse the USF for the improperly disbursed funds.

15. The Parties negotiated the following terms and conditions of settlement and hereby enter into this Consent Decree as provided below.

***7084 III. TERMS OF AGREEMENT**

16. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order without change, addition, deletion, or modification.

17. **Jurisdiction**. TerraCom and YourTel each agree that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree.

18. **Effective Date**. The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

19. **Termination of Investigation**. In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigation. In consideration for the termination of the Investigation, TerraCom and YourTel each agree to the terms, conditions, and procedures contained herein. The Bureau further agrees that, in the absence of new material evidence, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute, on its own motion, any new proceeding, formal or informal, or take any action on its own motion against TerraCom or YourTel concerning the matters that were the subject of the Investigation. The Bureau also agrees that, in the absence of new material evidence, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute on its own motion any proceeding, formal or informal, or to set to hearing the question of TerraCom's or YourTel's basic qualifications to be a Commission licensee or hold Commission licenses or authorizations.[38]

****9** 20. **Admissions of Liability**. TerraCom and YourTel each admit for the purpose of this Consent Decree and for Commission civil enforcement purposes, and in express reliance on the provisions of paragraph 19 herein, that their actions that were the subject of the Investigation violated Sections 201(b) and 222(a) of the Act. Additionally, YourTel admits for the purpose of this Consent Decree and for Commission civil enforcement purposes, and in express reliance on the provisions of paragraph 19 herein, that its actions that were the subject of the Investigation violated Sections 54.405, 54.407, and 54.409 of

the Rules, 47 C.F.R. §§ 54.405, 54.407, and 54.409, and the Commission's *Lifeline Reform Order*, 27 FCC Rcd 6656, and *Lifeline Duplicates Order*, 26 FCC Rcd 9022. The Parties agree that this Consent Decree is a compromise settlement and it is their intent that the Consent Decree shall not be used as evidence or precedent in any action, litigation, investigation, or proceeding, except an action to enforce this Consent Decree.

21. **Compliance Officer**. Within thirty (30) calendar days after the Effective Date, TerraCom and YourTel each shall designate a senior corporate manager with the requisite corporate and organizational authority to serve as a Compliance Officer and to discharge the duties set forth below. The person designated as the Compliance Officer shall be responsible for developing, implementing, and administering the Compliance Plans, including the Information Security Program (as defined in paragraph 22(b)) required under the Compliance Plans, and ensuring that TerraCom and YourTel comply with the terms and conditions of the Compliance Plans and this Consent Decree. In addition to the general knowledge of the Communications Laws necessary to discharge his or her duties under this Consent Decree, the Compliance Officer shall have specific knowledge of the information security principles and practices necessary to implement the information security requirements of this Consent Decree, and the specific requirements of Sections 222(a) and 201(b) of the Act and the Lifeline Eligibility and De-Enrollment Rules, prior to assuming his/her duties. The Compliance Officer shall promptly and without ***7085** unreasonable delay become privacy certified by an industry certifying organization and keep current through appropriate continuing privacy education courses.

22. **Compliance Plan for Sections 201(b) and 222(a) of the Act**. For purposes of settling the matters set forth herein with respect to Sections 201(b) and 222(a) of the Act, TerraCom and YourTel each agree that it shall, within ninety (90) calendar days after the Effective Date, develop and implement a Compliance Plan designed to ensure future compliance with the Communications Laws, including Sections 201(b) and 222(a) of the Act, and with the terms and conditions of this Consent Decree. Such Compliance Plan must include the following components:
****10** (a) **Risk Assessment**. Within thirty (30) calendar days after the Effective Date, TerraCom and YourTel each shall conduct a comprehensive and thorough risk assessment to identify internal and external risks to the security, confidentiality, and integrity of PI collected or maintained by or on behalf of TerraCom and YourTel that could result in unauthorized access, disclosure, misuse, destruction, or compromise of such information (Risk Assessment). The Risk Assessment must evaluate the likelihood and potential impact of these threats and the sufficiency of existing policies, procedures, and other safeguards in place to control risks.

(b) **Information Security Program**. Within sixty (60) calendar days after the Effective Date, TerraCom and YourTel each shall develop and implement a reasonable and comprehensive information security program to protect the security, confidentiality, and integrity of PI collected or maintained by or on behalf of TerraCom and YourTel (Information Security Program). TerraCom and YourTel each shall ensure that such Information Security Program is fully documented in writing (including, as appropriate, within the Operating Procedures and Compliance Manual described below) and includes:
i. Administrative, technical, and physical safeguards that are reasonable in light of TerraCom's and YourTel's size and complexity, the nature and scope of TerraCom's and YourTel's activities, the sensitivity of the PI collected or maintained by or on behalf of TerraCom and YourTel, and the risks identified through the Risk Assessment;

ii. Reasonable measures to protect PI collected or maintained by Covered Third Parties, including exercising due diligence in selecting Covered Third Parties, requiring Covered Third Parties by contract to implement and maintain reasonable and comprehensive safeguards for the protection of PI, engaging in the ongoing monitoring of Covered Third Parties' compliance with their security obligations, and implementing measures to sanction Covered Third Parties that fail to comply with their security obligations (including, where appropriate, terminating TerraCom and/or YourTel's relationship with such Covered Third Parties); and

iii. Policies and procedures to properly identify the nature and extent of PI collected or maintained by or on behalf of TerraCom and YourTel, collect the minimum amount of PI necessary to verify eligibility for the Lifeline program, collect and maintain PI in a manner that is secure, retain PI and Lifeline verification information and documents for no longer than strictly necessary to verify eligibility for the Lifeline program and comply with applicable law, and properly and securely dispose of PI.

In addition, TerraCom and YourTel each shall:

i. Monitor and evaluate their Information Security Programs, on an ongoing (but no less than quarterly) basis, to control the risks identified through the Risk Assessment, to evaluate the effectiveness of the Information Security ***7086** Program's key controls, systems and procedures, and to ensure compliance with Sections 201(b) and 222(a) of the Act and this Consent Decree;

****11** ii. Adjust and update their Information Security Programs pursuant to the results of the monitoring and evaluation described above, any material changes to any operations or business arrangements, any relevant changes in technology or to internal or external threats to PI, any changes in Covered Third Parties, or any other circumstances TerraCom or YourTel knows or has reason to know may have a material impact on the effectiveness of the Information Security Program; and

iii. Engage a qualified, objective, and independent third party auditing firm to review and audit their Information Security Programs using procedures and standards generally accepted in the profession. Such audit shall be completed within ninety (90) calendar days after the Effective Date, and TerraCom and YourTel shall submit copies of the audit reports to the Commission within ten (10) calendar days after their completion.

(c) **Third Party Oversight**. Within thirty (30) calendar days after the Effective Date, each of TerraCom and YourTel shall require all existing Covered Third Parties, by contract or amendment to an existing agreement, to protect PI by establishing and maintaining reasonable administrative, technical and physical safeguards that are no less stringent than the requirements to which TerraCom and YourTel are subject to pursuant to this Consent Decree, and shall include such requirements in agreements with future Covered Third Parties. Such agreements shall also include strict restrictions on the Covered Third Parties' further disclosure of PI, requirements for notifications of breaches of Covered Third Party systems that may result in unauthorized use or disclosure of PI, and other reasonable security controls. Each of TerraCom and YourTel shall monitor and verify, on an ongoing (but no less than quarterly) basis, that its Covered Third Parties comply with the terms of this paragraph.

(d) **Incident Response Plan**. Within thirty (30) calendar days after the Effective Date, TerraCom and YourTel each shall implement and maintain a reasonable and comprehensive security incident response plan to enable TerraCom and YourTel to detect, respond to, and, where appropriate, provide timely notification, in accordance with applicable law and the requirements of paragraph 24 below, to all Customers (at the Customer's last known address and pursuant to TerraCom's and YourTel's reasonable efforts to locate the Customer) and relevant governmental authorities of data breaches involving PI.

(e) **Representations to Customers**. Immediately upon the Effective Date and on an ongoing basis thereafter, TerraCom and YourTel each shall not misrepresent, expressly or by implication, in privacy policies, statements on websites, subscriber agreements, or other communications or representations made to Customers, the extent to which TerraCom and YourTel or their Covered Third Parties protect PI. Each of TerraCom and YourTel shall ensure that privacy policies and statements on each of TerraCom's and YourTel's websites regarding Customer privacy and the security of Customers' PI accurately reflect each of TerraCom's and YourTel's data security and privacy practices, and are updated routinely to reflect any material changes.

****12** (f) **Remediation Measures**. Within sixty (60) calendar days after the Effective Date, unless otherwise indicated, TerraCom and YourTel each shall:
***7087** i. Offer to provide one year of complimentary credit monitoring services to all Affected Customers through a nationally recognized credit monitoring service, the availability of which must be described in the notice discussed below; and

ii. Identify each Affected Customer and ensure that each Affected Customer has been notified (at the Affected Customer's last known address and pursuant to TerraCom's and YourTel's reasonable efforts to locate the Affected Customer) that his or her PI was compromised. The notification to each Affected Customer must include:
a. A general description of the manner in which the Affected Customer's PI was compromised;

b. A general description for all Affected Customers of the type of PI that was compromised;

c. The toll-free telephone numbers and addresses of the major credit reporting agencies;

d. Information regarding the complimentary credit monitoring services available to Affected Customers;

e. A toll-free hotline and website where Affected Customers may contact each of TerraCom and YourTel to inquire about their compromised PI, and receive reasonable and comprehensive counseling on responding to and mitigating credit harm incidences, including identity theft; and

f. Reasonable and comprehensive information regarding free and/or readily available credit protection options including obtaining free annual credit reports, placing fraud alerts on credit files, requesting security freezes, contacting financial institutions, and any other such free and/or readily available credit protections.

To the extent an Affected Customer was previously sent a notice that does not meet the requirements set forth above, TerraCom and YourTel shall provide such Affected Customer with an updated notice that satisfies the above requirements.

(g) **Notice of Consent Decree**. Within thirty (30) calendar days after the Effective Date, TerraCom and YourTel each shall deliver a copy of this Consent Decree to all existing Covered Employees, and shall also deliver a copy of this Consent Decree to all future Covered Employees within thirty (30) calendar days after the person assumes such position or responsibilities.

(h) **Operating Procedures**. Within sixty (60) calendar days after the Effective Date, TerraCom and YourTel each shall establish Operating Procedures that all Covered Employees must follow to help ensure each of TerraCom's and YourTel's compliance with this Consent Decree, including the policies and procedures adopted pursuant to subparts (a)-(f) of this paragraph, and Sections 201(b) and 222(a) of the Act. Each of TerraCom and YourTel shall also develop a compliance checklist that describes the steps that a Covered Employee must follow to ensure compliance with this Consent Decree, and Sections 201(b) and 222(a) of the Act.

****13** (i) **Compliance Manual**. Within sixty (60) calendar days after the Effective Date, TerraCom and YourTel each shall develop, use, and maintain a Compliance Manual (which may be in hard copy and/or electronic format), and distribute the same to all Covered Employees and Covered Third Parties. For any person who becomes a ***7088** Covered Employee or Covered Third Party more than sixty (60) calendar days after the Effective Date, TerraCom and YourTel shall distribute the Compliance Manual to that person within thirty (30) calendar days after the date such person becomes a Covered Employee or Covered Third Party, and prior to such person engaging with Customers with respect to TerraCom's or YourTel's services. Within the same period, TerraCom and YourTel shall further direct all Covered Third Parties to disseminate a copy of the Compliance Manual to each Covered Third Party Employee.
i. The Compliance Manual shall set forth and explain the requirements of Sections 201(b) and 222(a) of the Act and this Consent Decree, and shall instruct Covered Employees and Covered Third Party Employees to consult and follow the Operating Procedures to ensure TerraCom's and YourTel's compliance with the Communications Laws and this Consent Decree, including the policies and procedures adopted pursuant to subparts (a)-(f) of this paragraph.

ii. The Compliance Manual shall require Covered Employees and Covered Third Party Employees to contact their supervisor or the Compliance Officer with any questions or concerns that arise with respect to TerraCom's or YourTel's obligations under or compliance with the Communications Laws and this Consent Decree, and require any supervisor who receives such information from a Covered Employee or Covered Third Party Employee to promptly notify the Compliance Officer. Each of TerraCom and YourTel shall provide, and shall direct Covered Third Parties to provide, a hotline or other appropriate mechanism for anonymous reporting of any noncompliance.

iii. TerraCom and YourTel each shall periodically review and revise the Compliance Manual to ensure that the information set forth therein remains current and complete.

iv. TerraCom and YourTel shall (individually or collectively) distribute any revisions of the Compliance Manual to all Covered Employees and Covered Third Parties within thirty (30) calendar days after any revisions have been made by TerraCom or YourTel. These revisions may be in electronic format.

(j) **Compliance Training Program for Sections 201(b) and 222(a) of the Act**. Within sixty (60) calendar days after the Effective Date, TerraCom and YourTel each shall establish, implement, and maintain a compliance training program to ensure compliance with Sections 201(b) and 222(a) of the Act and this Consent Decree:
i. The Compliance Training Program shall include reasonable and comprehensive privacy and security awareness training for all Covered Employees, Covered Third Parties, and Covered Third Party Employees. The program shall include instruction on TerraCom's and YourTel's obligations, policies, and procedures for protecting PI pursuant to Section 201(b), 222(a), and this Consent Decree, including identifying and collecting PI from Customers, recognizing security threats and suspicious activity that may indicate that PI has been compromised, the timely reporting of data breaches, and other reasonable and appropriate training regarding the protection of PI. Each of TerraCom and YourTel shall cause all Covered Employees whose job functions relate to the implementation of the remediation measures described in paragraph 22(f) to receive training regarding ***7089** such remediation measures, as described below. In addition, each of TerraCom and YourTel shall direct all Covered Third Parties to ensure that their Covered Third Party Employees receive training in accordance with the Compliance Training Program. For purposes of complying with the provisions of this paragraph, TerraCom and YourTel are permitted to themselves provide the training or use a third party to provide the training described herein;

****14** ii. As part of the Compliance Training Program, TerraCom and YourTel shall ensure that each Covered Employee is advised of TerraCom's and YourTel's obligations to report any noncompliance with Sections 201(b) and 222(a) of the Act and this Consent Decree, and is instructed on how to disclose noncompliance to the Compliance Officer, including instructions on how to anonymously report such noncompliance. TerraCom and YourTel shall further direct all Covered Third Parties to disseminate the same instructions to each Covered Third Party Employee.

iii. TerraCom and YourTel shall ensure that the training for Covered Employees is conducted pursuant to the Compliance Training Program within sixty (60) calendar days after the Effective Date, except that any person who becomes a Covered Employee at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar days after the date such person becomes a Covered Employee. Each of TerraCom and YourTel shall document their Covered Employees' completion of the training. TerraCom and YourTel shall further direct and contractually require that all Covered Third Parties conduct the same type of training for each of their Covered Third Party Employees within the same period, and that completion of training is documented.

iv. Within sixty (60) calendar days after the Effective Date, neither TerraCom nor YourTel shall allow any Covered Employee to interact with any Customer about TerraCom's or YourTel's service until the Covered Employee has been trained and has received a copy of the Compliance Manual. Beginning within ninety (90) calendar days after the Effective date, TerraCom and YourTel shall further direct all Covered Third Parties to ensure that their Covered Third Party Employees shall not interact with any Customer about TerraCom's or YourTel's service until their Covered Third Party Employees have been trained and have received copies of the Compliance Manual; and

v. TerraCom and YourTel shall ensure that the Compliance Training Program is conducted at least annually and shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness.

23. **Compliance Plan for Lifeline Eligibility and De-Enrollment Rules**. For purposes of settling the matters set forth herein with respect to the Lifeline Eligibility and De-Enrollment Rules, YourTel agrees that it shall, within sixty (60) calendar days after the Effective Date, develop and implement a Compliance Plan designed to ensure future compliance with the Communications Laws, including the Lifeline Eligibility and De-Enrollment Rules, and with the terms and conditions of this Consent Decree. With respect to the Lifeline Eligibility and De-Enrollment Rules, YourTel will implement, at a minimum, the following procedures:
***7090** (a) **Operating Procedures**. Within thirty (30) calendar days after the Effective Date, YourTel shall establish Operating Procedures that all Covered Employees must follow to help ensure YourTel's compliance with the Lifeline

Eligibility and De-Enrollment Rules. YourTel's Operating Procedures shall include internal procedures and policies specifically designed to ensure that YourTel timely de-enrolls customers determined to be ineligible for the program, and avoids improperly claiming ineligible customers for Lifeline support. YourTel shall also develop a compliance checklist that describes the steps that a Covered Employee must follow to ensure compliance with the Lifeline Eligibility and De-Enrollment Rules. The Operating Procedures and compliance checklist shall include internal procedures and policies specifically designed to ensure compliance with the following requirements:
**15 i. Upon notification by USAC that a subscriber is receiving Lifeline service from another ETC or that more than one member of a subscriber's household is receiving Lifeline service and therefore that the subscriber should be de-enrolled from participation in YourTel's Lifeline program, YourTel must de-enroll the subscriber from program participation within five (5) business days pursuant to Section 54.405(e)(2).

ii. YourTel shall not claim Lifeline reimbursement for any subscriber identified by USAC to be de-enrolled pursuant to Section 54.405(e)(2) more than five (5) business days following USAC notification pursuant to that rule section.

iii. For purposes of the Form 497 claim process and prior to submitting a Form 497 claim for reimbursement following any subscriber de-enrollments performed pursuant to Section 54.405(e)(2): YourTel must confirm the specified ineligible subscribers are not included in any claim for reimbursement following the date of de-enrollment or more than five (5) business days following USAC notification; and YourTel will adopt procedures that provide for routine checks that such de-enrollments are timely performed, and describe these checks in its Compliance Reports.

iv. To the extent YourTel uses a Covered Third Party for verifying, maintaining, or updating subscriber information, providing records management and storage, or processing enrollments or de-enrollments, YourTel will establish oversight procedures, including regular compliance checks, to ensure compliance with the Lifeline Eligibility and De-Enrollment Rules and the terms of this Consent Decree. YourTel will describe these compliance checks in its Compliance Reports.

(b) **Compliance Manual**. Within sixty (60) calendar days after the Effective Date, YourTel shall develop, use, and maintain a Compliance Manual (which may be in hard copy and/or electronic format), and distribute the same to all Covered Employees and Covered Third Parties. For any person who becomes a Covered Employee or Covered Third Party more than sixty (60) calendar days after the Effective Date, YourTel shall distribute the Compliance Manual to that person within thirty (30) calendar days after the date such person becomes a Covered Employee or Covered Third Party, and prior to such person engaging with Customers with respect to YourTel's services. Within the same period, YourTel shall further direct all Covered Third Parties to disseminate a copy of the Compliance Manual to each Covered Third Party Employee.
i. The Compliance Manual shall set forth and explain the requirements of the Lifeline Eligibility and De-Enrollment Rules and this Consent Decree, and shall instruct Covered Employees and Covered Third Party Employees to consult and follow the Operating Procedures to ensure YourTel's compliance with the Communications Laws and this Consent Decree.

**16 *7091 ii. The Compliance Manual shall require Covered Employees and Covered Third Party Employees to contact their supervisor or the Compliance Officer with any questions or concerns that arise with respect to YourTel's obligations under or compliance with the Communications Laws and this Consent Decree, and require any supervisor who receives such information from a Covered Employee or Covered Third Party Employee to promptly notify the Compliance Officer.

iii. YourTel shall periodically review and revise the Compliance Manual to ensure that the information set forth therein remains current and complete.

iv. YourTel shall distribute any revisions of the Compliance Manual to all Covered Employees and Covered Third Parties within thirty (30) calendar days after any revisions have been made by YourTel. Like the Compliance Manual, these revisions may be in electronic format.

(c) **Compliance Training Program for Lifeline Eligibility and De-Enrollment Rules**. YourTel shall establish and implement a Compliance Training Program on compliance with the Lifeline Eligibility and De-Enrollment Rules and the Operating Procedures. As part of the Compliance Training Program, Covered Employees and Covered Third Parties shall be advised of YourTel's obligation to report any noncompliance with the Lifeline Eligibility and De-Enrollment Rules under

paragraph 24 of this Consent Decree and shall be instructed on how to disclose noncompliance to the Compliance Officer. All Covered Employees and Covered Third Parties shall be trained pursuant to the Compliance Training Program within sixty (60) calendar days after the Effective Date, except that any person who becomes a Covered Employee or Covered Third Party at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar days after the date such person becomes a Covered Employee or Covered Third Party. YourTel shall repeat compliance training on an annual basis, and shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness.

24. **Reporting Noncompliance**. Each of TerraCom and YourTel (collectively or individually) shall report any noncompliance with Sections 201(b) and 222(a)-(c) of the Act, the Commission's CPNI rules,[39] the terms and conditions of this Consent Decree, and, for YourTel, the Lifeline Eligibility and De-Enrollment Rules, within fifteen (15) calendar days after discovery of such noncompliance. Such reports shall include a detailed explanation of: (i) each instance of noncompliance; (ii) the steps that each of TerraCom and YourTel have taken or will take to remedy such noncompliance; (iii) the schedule on which such remedial actions will be taken; and (iv) the steps that each of TerraCom and YourTel have taken or will take to prevent the recurrence of any such noncompliance. Each of TerraCom and YourTel shall also report any breaches of PI or CPNI as soon as practicable, but no later than seven (7) business days after reasonable determination of the breach. Such reports shall include, to the extent known, a detailed explanation of: (i) the nature of the breach; (ii) the date of the breach; (iii) the date of discovery of the breach; (iv) the type of PI or CPNI involved in the breach; (v) the number of individuals affected by the breach; and (vi) the steps that each of TerraCom and YourTel have taken or will take to remedy the breach and prevent its recurrence. All reports of noncompliance or PI/CPNI breaches shall be submitted to (1) the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4C-224, Washington, DC ***7092** 20554, with a copy submitted electronically to David.Valdez@fcc.gov, Michael.Epshteyn@fcc.gov, and Shante.Willis@fcc.gov, and (2) the Chief, Investigations and Hearings Division, Federal Communications Commission, 445 12th Street., SW, Rm. 4-C224, Washington, DC 20554, with a copy submitted electronically to Jeffrey.Gee@fcc.gov, Kalun.Lee@fcc.gov, and Mindy.Littell @fcc.gov.

****17** 25. **Compliance Reports**. Each of TerraCom and YourTel shall file compliance reports with the Commission ninety (90) days after the Effective Date, six (6) months after the Effective Date, twelve (12) months after the Effective Date, twenty-four (24) months after the Effective Date, and thirty-six (36) months after the Effective Date.
(a) Each Compliance Report shall include a detailed description of TerraCom's and YourTel's efforts during the relevant period to comply with the terms and conditions of this Consent Decree and Sections 201(b) and 222(a) of the Act and, for YourTel, compliance with the Lifeline Eligibility and De-Enrollment Rules. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of each of TerraCom and YourTel, stating that the Compliance Officer has personal knowledge that TerraCom and YourTel: (i) have established and implemented the Compliance Plans required by paragraphs 22 and 23; (ii) have utilized the applicable Operating Procedures since the implementation of the Compliance Plans; and (iii) are not aware of any instances of noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in paragraph 24 of this Consent Decree.

(b) The Compliance Officer's certification shall be accompanied by a statement explaining the basis for such certification and shall comply with Section 1.16 of the Rules and be subscribed to as true under penalty of perjury in substantially the form set forth therein.[40]

(c) If the Compliance Officer cannot provide the requisite certification, the Compliance Officer, as an agent of and on behalf of each of TerraCom and YourTel, shall provide the Commission with a detailed explanation of the reason(s) why and describe fully: (i) each instance of noncompliance; (ii) the steps each of TerraCom and YourTel have taken or will take to remedy such noncompliance, including the schedule on which proposed remedial actions will be taken; and (iii) the steps that each of TerraCom and YourTel have taken or will take to prevent the recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

(d) Each Compliance Report shall also include a detailed description of any new or additional telecommunications companies owned, in whole or in part, by any of the present or past owners, shareholders, officers, or directors of TerraCom and YourTel. The Compliance Report shall also include a description of any additional telecommunications companies managed

by the companies that manage TerraCom and YourTel.

(e) All Compliance Reports shall be submitted to (1) the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4-C224, Washington, DC 20554, with copies submitted electronically to David.Valdez@fcc.gov, Michael.Epshteyn@fcc.gov, and Shante.Willis@fcc.gov, and (2) the Chief, Investigations and Hearings Division, ***7093** Federal Communications Commission, 445 12th Street., SW, Rm. 4-C224, Washington, DC 20554, with a copy submitted electronically to Jeffrey.Gee@fcc.gov, Kalun.Lee@fcc.gov, and Mindy.Littell@fcc.gov.

****18** 26. **Termination Date**. Unless stated otherwise, the obligations set forth in paragraphs 22(f)-(j), 23, 24, and 25 of this Consent Decree shall expire thirty-six (36) months after the Effective Date. The obligations set forth in paragraph 21 shall remain in effect during the entire period that each of TerraCom and YourTel collects PI from or about Customers. The remaining obligations set forth in paragraph 22 shall expire eight (8) years after the Effective Date.

27. **Section 208 Complaints; Subsequent Investigations**. Nothing in this Consent Decree shall prevent the Commission or its delegated authority from adjudicating complaints filed pursuant to Section 208 of the Act[41] against TerraCom, YourTel, or their Affiliates for alleged violations of the Act, or for any other type of alleged misconduct, regardless of when such misconduct took place. The Commission's adjudication of any such complaint will be based solely on the record developed in that proceeding. Except as expressly provided in this Consent Decree, this Consent Decree shall not prevent the Commission from investigating new evidence of noncompliance by TerraCom or YourTel with the Communications Laws.

28. **Civil Penalty**. TerraCom and YourTel shall pay a civil penalty to the United States Treasury in the amount of three million five hundred thousand dollars ($3,500,000), for which they are jointly and severally liable (Civil Penalty). TerraCom and YourTel each specifically consent to, the Commission's offset of the Civil Penalty against any USF support owed to TerraCom and/or YourTel until the Civil Penalty is paid in full. TerraCom and YourTel each agree that (i) the Commission, through the Bureau, may direct the USF administrator to effectuate the offset against all USF support owed to TerraCom and/or YourTel and to send all such USF support, to the U.S. Treasury and (ii) TerraCom and Yourtel will immediately send written affirmation to the USAC of their consent to offset until the Civil Penalty is paid in full. TerraCom and YourTel shall send electronic notification of payment to Johnny Drake, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission at Johnny.Drake@fcc.gov, and Mindy Littell, Investigations and Hearings Division, Federal Communications Commission at Mindy.Littell@fcc.gov, on the date said payment is made. The payment must be made by check or similar instrument, wire transfer, or credit card, and must include the NAL Account Number and FRN referenced above. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.[42] When completing the FCC Form 159, enter the NAL Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in block number 24A (payment type code). Below are additional instructions that should be followed based on the form of payment selected:
· Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank — Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

****19** · Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure ***7094** appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.

· Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank — Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

Questions regarding payment procedures should be addressed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES @fcc.gov.

29. **Waivers**. As of the Effective Date, TerraCom and YourTel each waive any and all rights they may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this Consent Decree and the Adopting Order. TerraCom and YourTel shall retain the right to challenge Commission interpretation of the Consent Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the Consent Decree or the Adopting Order, neither TerraCom, YourTel, nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and TerraCom and YourTel each shall waive any statutory right to a trial *de novo*. TerraCom and YourTel each hereby agree to waive any claims they may otherwise have under the Equal Access to Justice Act[43] relating to the matters addressed in this Consent Decree.

30. **Severability**. The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

31. **Invalidity**. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

32. **Subsequent Rule or Order**. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or Order adopted by the Commission (except an Order specifically intended to revise the terms of this Consent Decree to which TerraCom or YourTel, as applicable, do not expressly consent) that provision will be superseded by such Rule or Order.

20 33. **Successors and Assigns. TerraCom and YourTel each agree that the provisions of this Consent Decree shall be binding on their successors, assigns, and transferees.

34. **Final Settlement**. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigation.

35. **Modifications**. This Consent Decree cannot be modified without the advance written consent of all Parties.

36. **Paragraph Headings**. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

*7095 37. **Authorized Representative**. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

38. **Counterparts**. This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

For: Federal Communications Commission

_____

Travis LeBlanc, Chief

Enforcement Bureau

_____

Date

For: TerraCom, Inc.

_____

Dale Schmick, Chief Operating Officer

_____

Date

For: YourTel America, Inc.

_____

Dale Schmick, Chief Operating Officer

_____

Date

Footnotes

1 *See* 47 U.S.C. §§ 201, 222(a).

2 47 C.F.R. §§ 54.405, 54.407, and 54.409; *Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656 (2012); *Lifeline and Link Up Reform and Modernization*, Report and Order, 26 FCC Rcd 9022 (2011).

3 *See* 47 C.F.R. § 1.93(b).

4 47 U.S.C. §§ 154(i), 503(b).

5 47 C.F.R §§ 0.111, 0.311.

1 The investigation of YourTel initiated under File No. EB-13-IH-0931 was subsequently assigned to File No. EB-IHD-13-00010677.

2 47 U.S.C. §§ 201(b), 222(a).

3 47 C.F.R. §§ 54.405, 54.407, and 54.409; *Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656 (2012) (*Lifeline Reform Order*); *Lifeline and Link Up Reform and Modernization*, Report and Order, 26 FCC Rcd 9022, 9022-23, para. 1 (2011) (*Lifeline Duplicates Order*).

4 47 U.S.C. § 151 *et seq.*

5 *See TerraCom, Inc., and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13342, para. 50 (Oct. 24, 2014) (*TerraCom/YourTel NAL*).

6 *See* 47 U.S.C. § 222(a).

7 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007); *see also Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling and Order, FCC 15-24, 2015 WL 1120110, at *140, para. 462 (Mar. 12, 2015).

8 *Id.* at 6959-60, para. 65.

9 *TerraCom/YourTel NAL*, 29 FCC Rcd at 13330-31, paras. 14-16.

10 *Id.* at 13331, para. 17.

11 47 U.S.C. § 201(b).

12 *TerraCom/YourTel NAL*, 29 FCC Rcd at 13335-36, paras. 31-32.

13 Lifeline service is a retail voice telephony service that telecommunications carriers provide to qualifying low-income consumers for a reduced charge. 47 C.F.R. § 54.407(b). *See also Lifeline Reform Order*, 27 FCC Rcd at 6662-67, paras. 11-18; 47 C.F.R. §§ 54.400-54.422.

14 TerraCom's and YourTel's Chief Operating Officer is Dale Schmick.

15 BrightStar Global Solutions, LLC, is an Oklahoma limited liability company located at 1101 Territories Dr., Edmond, OK 73034. *See* Letter from Mark C. Del Bianco, Law Office of Mark C. Del Bianco, Attorney for TerraCom and YourTel, to Steven Ruckman, Esq., Assistant Attorney General, Maryland Office of the Attorney General (June 14, 2013) (on file in EB-TCD-13-00009175).

16 *See TerraCom/YourTel NAL*, 29 FCC Rcd at 13326, para. 4.

17 *Id.*

18 *Id.*

19 *Id.* at 13329-30, para. 12.

20 *See Lifeline Reform Order*, 27 FCC Rcd at 6662-67, paras. 11-18; 47 C.F.R. §§ 54.400-54.422.

21 47 U.S.C. § 254(e) (providing that "only an eligible telecommunications carrier designated under section 214(e) of this title shall be eligible to receive specific Federal universal service support"); 47 U.S.C. § 214(e) (prescribing the method by which carriers are designated as ETCs).

22 47 C.F.R. § 54.403(a). An ETC may receive $9.25 per month for each qualifying low-income consumer receiving Lifeline service, and up to an additional $25 per month if the qualifying low-income consumer resides on Tribal lands. *See id.* Lifeline provides a single discounted wireline or wireless phone service to each qualifying low-income consumer's household. *See* 47 C.F.R. § 54.401; *see also* 47 C.F.R. § 54.400(h) (defining "household" as "any individual or group of individuals who are living together at the same address as one economic unit"); *Lifeline Reform Order*, 27 FCC Rcd at 6760, para. 241 (noting that the costs of wireless handsets are not supported by the Lifeline program).

23 *See* 47 C.F.R. §§ 54.400-54.422.

24 47 C.F.R. § 54.407(a).

25 47 C.F.R. § 54.407(b). In 2011, the Commission took action designed to address potential waste, fraud, and abuse in the Lifeline program by preventing duplicate payments for multiple Lifeline-supported services to the same individual. *See Lifeline and Link Up Reform and Modernization*, Report and Order, 26 FCC Rcd 9022, 9022-23, para. 1 (2011) (*Lifeline Duplicates Order*); *see also Lifeline and Link Up Reform and Modernization*, Order, 28 FCC Rcd 9057 (Wir. Comp. Bur. 2013) (codifying the Commission's requirement that ETCs verify a subscriber's eligibility before activating service). Specifically, the Commission amended Sections 54.401 and 54.405 of the rules to codify the restriction that an eligible low-income consumer cannot receive more than one Lifeline-supported service at a time. *See Lifeline Duplicates Order*, 26 FCC Rcd at 9026, para. 7. In the *Lifeline Reform Order*, this codified restriction was moved from Section 54.401(a) to revised Section 54.409(c). *See Lifeline Reform Order*, 7 FCC Rcd at 6689, para. 74, n.192. The Commission reiterated this limitation in the *Lifeline Reform Order*. *See Lifeline Reform Order*, 27 FCC Rcd at 6689, para. 74; 47 C.F.R. § 54.405.

26 47 C.F.R. § 54.409(c); *see also id.* § 54.400(a) (defining ""qualifying low income subscriber").

27 *See* 47 C.F.R. § 54.407(d).

28 *See Lifeline Reform Order*, 27 FCC Rcd at 6788, para. 305. Subsequent form revisions, however, do not vitiate violations of an

ETC's duty to verify the eligibility of the subscribers that are reflected on any of its previously filed Form 497s.

29 *See* 47 C.F.R. § 54.405(e)(2).

30 *See* Ill. Commerce Comm'n, Docket No. 09-0605 (granted March 24, 2010); Kan. Corp. Comm'n, Docket No. 09-TPCT-596-ETC (granted June 10, 2009); Me. P.U.C., Docket No. 2011-160 (granted Sept. 14, 2011); Mo. Pub. Serv. Comm'n, File No. CO-2009-0257 (granted March 21, 2009); Okla. Corp. Comm'n, Cause No. PUD-201100013, Order No. 588339 (granted Aug. 18, 2011); Pa. P.U.C., Docket No. P-2011-2226044 (granted Oct. 14, 2011); R.I. P.U.C., Docket No. 4293 (granted July 26, 2011); Wash. Util. & Transp. Comm'n, Docket No. UT-110423, Order 01 (granted June 16, 2011).

31 *See* Third Revised Compliance Plan of YourTel America, Inc., WC Docket Nos. 09-197 and 11-42, at 4 (filed June 19, 2012).

32 *See* Ill. Commerce Comm'n, Docket No. 09-0605 (granted March 24, 2010); Kan. Corp. Comm'n, Docket No. 03-TPCT-355-ETC (granted Feb. 27, 2003); Mo. Pub. Serv. Comm'n, Case No. CN-2007-0218 (ordered Jan. 17, 2007); Okla. Corp. Comm'n, Cause No. PUD 200300532, Order No. 484228 (granted Dec. 19, 2003).

33 *See* Letter from USAC to Ron Medlin, YourTel (dated Oct. 12, 2012) (*De-Enrollment Letter*).

34 *See* Letter from Pamela S. Kane, Deputy Chief, Investigations and Hearings Division, FCC Enforcement Bureau, to Dale Schmick, YourTel (July 11, 2013) (on file in EB-IHD-13-00010677) (*LOI*).

35 *See* Letter from Douglas D. Orvis, Counsel for YourTel, to Marlene Dortch, Secretary, FCC (Aug. 12, 2013) (on file in EB-IHD-13-00010677) (*LOI Response*).

36 *Id.*

37 *See LOI Response* at Response to Question 24.

38 *See* 47 C.F.R. § 1.93(b).

39 *See* 47 C.F.R. § 64.2001-2011; *see also* 47 U.S.C. § 222(h)(1)(defining Customer Proprietary Network Information or CPNI).

40 *See* 47 C.F.R. § 1.16.

41 47 U.S.C. § 208.

42 An FCC Form 159 and detailed instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

43 *See* 5 U.S.C. § 504; 47 C.F.R. §§ 1.1501-1.1530.

30 FCC Rcd. 7075 (F.C.C.), 30 F.C.C.R. 7075, 62 Communications Reg. (P&F) 1618, 2015 WL 4159266

End of Document

30 FCC Rcd. 12302 (F.C.C.), 30 F.C.C.R. 12302, 63 Communications Reg. (P&F) 1064, 2015 WL 6779864

Federal Communications Commission (F.C.C.)
Order

IN THE MATTER OF COX COMMUNICATIONS, INC.

File No.: EB-IHD-14-00017829
Acct. No.: 201632080001
FRN: 0001834696
DA 15-1241
Released: November 5, 2015
Adopted: November 5, 2015

1 *12302 By the Chief, Enforcement Bureau:

1. Consumers of cable and satellite services are entitled to have their personal information protected. The Communications Act already imposes heightened obligations on cable and satellite operators to protect the personally identifiable information of their subscribers, and to take such actions as are necessary to prevent unauthorized access to this information. Inadequate security of subscribers' personal information can result in real world consequences for those customers, who are put at risk of financial and digital identity theft. In the wrong hands, a customer's sensitive personal information could also be used to take control of a customer's real accounts, to change the passwords on those accounts, to expose the customer's personal information on the web, and to harass or embarrass the customer through social media. Today, the Enforcement Bureau (Bureau) of the Federal Communications Commission has entered into a Consent Decree to resolve its investigation into whether Cox Communications, Inc. (Cox), failed to properly protect the confidentiality of its customers' proprietary information (PI), proprietary network information (CPNI), and personally identifiable information, and whether Cox failed to promptly notify law enforcement authorities of security breaches involving CPNI, as required by Commission rules (Rules).

2. Cox's electronic data systems were breached in August 2014 when a third party used a common social engineering ploy known as pretexting. Specifically, the third party pretended to be from Cox's information technology department and gained access to data systems containing Cox customer information by convincing a Cox customer service representative and a Cox contractor to enter their respective account IDs and passwords into a fake website, which the third party controlled. The relevant data systems did not have technical safeguards, such as multi-factor authentication, to prevent the compromised credentials from being used to access the PI and CPNI of Cox's customers. Thus, the third party was able to make use of the credentials to view personal data of Cox's current and former customers, including sensitive personal information such as name, home address, email address, phone number, partial Social Security Number, partial driver's license number, and telephone customers' account-related data. This third-party hacker then posted some of the personal information of at least eight of the affected customers on social media sites, changed the passwords of at least 28 of the affected customers, and shared customer personal information with another alleged hacker. Cox did not report the breaches through the Commission's breach-reporting portal.

2 3. Congress and the Commission have made clear that cable operators such as Cox must "take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[1] Furthermore, telecommunications carriers such as Cox must take ***12303 "every reasonable precaution"[2] to protect their customers' data. In addition, the law requires carriers to promptly disclose CPNI breaches via our reporting portal within seven (7) business days after reasonable determination of a breach to facilitate the investigations of the FBI and the United States Secret Service.[3]

4. To settle this matter, Cox will pay a civil penalty of $595,000 and develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into Cox's business practices to protect consumers against similar data breaches in the future. In particular, Cox will be required to improve its privacy and data security practices by: (i) designating a senior corporate manager who is a certified privacy professional; (ii) conducting privacy risk assessments; (iii)

implementing a written information security program; (iv) maintaining reasonable oversight of third party vendors, to include implementing multi-factor authentication; (v) implementing a more robust data breach response plan; and (vi) providing privacy and security awareness training to employees and third-party vendors. Cox will also identify all affected consumers, notify them of the breach, provide them with free credit monitoring, and file regular compliance reports with the FCC.

5. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest would be served by adopting the Consent Decree and terminating the referenced investigation regarding Cox's compliance with Sections 201(b), and 222(a) and (c), and 631(c) of the Communications Act of 1934, as amended (Act), as well as Sections 64.2010(a) and 64.2011(b) of the Rules.[4]

6. In the absence of material new evidence relating to this matter, we do not set for hearing the question of Cox's basic qualifications to hold or obtain any Commission license or authorization.[5]

7. Accordingly, **IT IS ORDERED** that, pursuant to Section 4(i) of the Act[6] and the authority delegated by Sections 0.111 and 0.311 of the Rules,[7] the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

8. **IT IS FURTHER ORDERED** that the above-captioned matter **IS TERMINATED**.

***12304** 9. **IT IS FURTHER ORDERED** that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Barry Ohlsohn, Esq., Vice President, Regulatory Affairs, Cox Enterprises, Inc., 975 F Street, NW, Suite 300, Washington, DC 20004, and to counsel David H. Solomon, Esq., and J. Wade Lindsay, Esq., Wilkinson Barker Knauer, LLP, 1800 M Street, N.W., Suite 800N, Washington, D.C. 20036.

FEDERAL COMMUNICATIONS COMMISSION

****3** Travis LeBlanc
Chief
Enforcement Bureau

***12305 CONSENT DECREE**

1. The Enforcement Bureau of the Federal Communications Commission and Cox Communications, Inc. (Cox), by their authorized representatives, hereby enter into this Consent Decree for the purpose of terminating the Enforcement Bureau's investigation into whether Cox violated Sections 201(b) and 222(a) and (c), and 631 of the Communications Act of 1934, as amended, and Sections 64.2010(a) and 64.2011(b) of the Commission's rules.[1]

I. DEFINITIONS

2. For the purposes of this Consent Decree, the following definitions shall apply:
(a) "Act" means the Communications Act of 1934, as amended.[2]

(b) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(c) "Affected Customer" means any Customer whose PI and/or CPNI was viewed by unauthorized third parties in connection with the August 7, 2014, data breach.

****4** (d) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(e) "Commission" and "FCC" mean the Federal Communications Commission and all of its bureaus and offices.

(f) "Communications Laws" means, collectively, the Act, the Rules, and the published and promulgated orders and decisions of the Commission to which Cox is subject by virtue of its business activities.

(g) "Compliance Officer" means the individual designated in paragraph 16 of this Consent Decree as the person responsible for administration of the Compliance Plan.

(h) "Compliance Plan" means the compliance obligations, programs, and procedures described in this Consent Decree at paragraph 17.

(i) "Covered Employees" means all employees of Cox assigned to call centers that provide customer service or sales service for Cox Customers managed and operated by Cox, Cox field technicians, and Cox information technology Help Desk employees, who perform or directly supervise, oversee, or manage the performance of, duties that involve access to, use, or disclosure of PI and/or CPNI. Covered Employees do not include Covered Third Party Employees.

(j) "Covered Third Party" means any third-party that, on behalf of Cox, operates and/or manages a call center that provides customer service or sales service for Cox, ***12306** provides field technician services, or provides information technology Help Desk services.

(k) "Covered Third Party Employees" means all employees of Covered Third Parties assigned to call centers that provide customer service to Cox Customers, field technicians, and information technology Help Desk employees, who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of PI and/or CPNI of Cox Customers.

(l) "Cox" means Cox Communications, Inc., its wholly owned subsidiaries that own and operate cable systems that provide video, broadband, or telecommunications services in the United States and successors-in-interest.

(m) "Customer" means any current and/or former subscriber of any Cox service, which service is subject to the Communications Laws. "Customer" shall include any applicant for any Cox service to the extent that Cox, or any Covered Third Party collects and stores PI and/or CPNI regarding the applicant on behalf of Cox, in any Cox or Covered Third Party electronic data systems.

(n) "Customer Proprietary Network Information" or "CPNI" shall have the meaning set forth at 47 U.S.C. § 222(h).

(o) "Effective Date" means the date by which the Bureau and Cox have signed the Consent Decree.

(p) "Investigation" means the investigation commenced by the Bureau in File No. EB-IHD-14-00017829 regarding whether Cox violated the Privacy Laws in 2014.[3]

****5** (q) "Operating Procedures" means the standard internal operating procedures and compliance policies established by Cox to implement the Compliance Plan.

(r) "Parties" means Cox and the Bureau, each of which is a "Party."

(s) "Personal Information" or "PI" means either of the following: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver's license number or other government-issued identification card number; or (C) account number, credit or debit ***12307** card number, in combination with any required security code, access code, PIN, or password that would permit access to an individual's financial account; or (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(t) "Privacy Laws" means Sections 47 U.S.C. §§ 201(b), 222, and 551, and 47 C.F.R §§ 64.2001-2011, insofar as they relate to the security, confidentiality, and integrity of PI and/or CPNI.

(u) "Rules" means the Commission's regulations found in Title 47 of the Code of Federal Regulations.

II. BACKGROUND

3. Section 631(c) of the Act provides that, with certain exceptions, a cable operator "shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[4]

4. Section 222 of the Act is entitled "Privacy of customer information."[5] Section 222(a), entitled "In general," provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to ... customers."[6] The Commission has interpreted Section 222(a) as applying to customer ""proprietary information" that does not fit within the statutory definition of CPNI.[7] The Commission has stated that proprietary information broadly encompasses all types of information that should not be exposed widely to the public, whether that information is sensitive for economic or personal privacy reasons,[8] and that this includes privileged information, trade secrets, and personally identifiable information.[9]

5. Section 222(c) of the Act imposes certain restrictions on telecommunications carriers to protect the confidentiality of their customers' CPNI.[10] Section 64.2010(a) of the Rules establishes protections for CPNI by requiring carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.[11] Section 64.2011(b) requires carriers to provide notification of a CPNI breach via the FCC portal "[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach."[12]

**6 6. Section 201(b) of the Act states, in pertinent part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service *12308 [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful.""[13] The Commission has interpreted Section 201(b) to apply to carriers' data-security practices for protecting proprietary information.[14] In that regard, the Commission has interpreted Section 201(b) to require companies to employ just and reasonable data security practices to protect consumers' proprietary information.[15]

7. Cox provides digital cable television services, broadband Internet access service, telecommunications services, and home automation services in the United States. Cox is the third largest cable company in the United States, serving approximately six million residential and commercial customers,[16] and is the seventh largest landline telephone provider in the United States.[17]

8. The Bureau's review of the record shows that Cox's systems were breached on or about August 7, 2014, by a hacker using the alias "EvilJordie," a member of the hacker group known as the Lizard Squad.[18] This individual apparently used a social engineering method known as pretexting[19] to gain access to Cox electronic data systems containing customer information. Specifically, EvilJordie pretended to be from Cox's information technology department and convinced a contractor to enter her account ID and password into a fake, or "phishing," website on or about August 7, 2014.[20] According to Cox, the phony phishing website appeared to be a Cox website but, in fact, was controlled by "EvilJordie."[21] Around the same time, the access credentials of a Cox Tech Support representative were also compromised by means of a social engineering effort that prompted the representative to enter his access credentials into the same phishing website. Cox states that it believes that ""EvilJordie" shared the compromised credentials with "chF."[22]

9. As a result of these actions, the hackers had access to Cox electronic data systems that included some PI of *** active Customers and some PI and CPNI of *** telephone *12309 Customers.[23] The record reflects that from August 7, 2014, through August 14, 2014, the hackers viewed some PI of 54 current Affected Customers, seven former Affected Customers, and likely viewed some CPNI of at least one, but possibly up to four, of these Affected Customers.[24] The hackers posted some information of eight of the Affected Customers on social media sites; they also changed the passwords of 28 of the Affected Customers' whose PI was viewed.[25] Of the current Affected Customers whose information was viewed, 20 subscribed to telephone service at the time of the breach.[26]

**7 10. Cox asserts that it learned of the August 7th breach on August 12, 2014, when a Cox employee in San Diego received an email from a Nevada Customer who complained of account information being posted on a social media site.[27] Cox's privacy team then engaged its customer safety team, which investigated the incident, identified the source of the breach, and disabled the compromised access credentials within two days of learning of the August 7th breach. At the time of the breach,

Cox employed multi-factor authentication for some employees and third party contractors with access to Cox electronic data systems, but not for the compromised employee or contractor. Cox's internal policies and training programs expressly prohibited Cox employees and third party contractors from disclosing access credentials to anyone and warned against pretexting attacks. On August 18, 2014, Cox directly contacted the FBI and cooperated in the subsequent investigation of the breach, which resulted in the arrest of "EvilJordie."[28] Cox did not disclose the CPNI breach via the FCC data breach reporting portal. Via a letter dated September 16, 2014, Cox notified all but two of current Affected Customers that their PI/CPNI had been compromised as a result of a Cox customer service representative sharing access credentials with an unknown individual and offered free credit monitoring services.[29] Cox took other remedial steps as a result of the incident.

11. The Bureau subsequently commenced an investigation that it states involved whether Cox: (i) failed to properly protect the confidentiality of Customers' personally identifiable information; (ii) failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI; (iii) failed to provide timely notification to law enforcement of a CPNI breach; and (iv) engaged in unjust and unreasonable practices by (a) failing to employ reasonable data security practices to protect proprietary information and CPNI, and failing to monitor for Customers' breached data online; and (b) failing to notify all potentially affected Customers of the breaches. The Parties negotiated the following terms and conditions of settlement and hereby enter into this Consent Decree as provided below.

III. TERMS OF AGREEMENT

12. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order without change, addition, deletion, or modification.

13. **Jurisdiction**. Cox agrees that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree.

***12310** 14. **Effective Date**. The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

****8** 15. **Termination of Investigation**. In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigation. In consideration for the termination of the Investigation, Cox agrees to the terms, conditions, and procedures contained herein. The Bureau further agrees that, in the absence of new material evidence, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute, on its own motion, any new proceeding, formal or informal, or take any action on its own motion against Cox concerning the matters that were the subject of the Investigation. The Bureau also agrees that, in the absence of new material evidence, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute on its own motion any proceeding, formal or informal, or to designate for hearing the question of Cox's basic qualifications to be a Commission licensee or hold Commission licenses or authorizations.[30]

16. **Compliance Officer**. Within thirty (30) calendar days after the Effective Date, Cox shall designate a senior corporate manager with the requisite corporate and organizational authority to serve as a Compliance Officer and to discharge the duties set forth below. The person designated as the Compliance Officer, together with the Chief Privacy Officer (who shall be privacy certified by an industry-certifying organization and who shall keep current through appropriate continuing privacy education courses) and Chief Information Security Officer, shall be responsible for developing, implementing, and administering the Compliance Plan, including the Information Security Program (as defined in paragraph 17(b)) required under the Compliance Plan, and ensuring that Cox complies with the terms and conditions of the Compliance Plan and this Consent Decree. In addition to the general knowledge of the Communications Laws necessary to discharge his or her duties under this Consent Decree, the Compliance Officer, Chief Information Security Officer, or managers reporting to either the Compliance Officer or Chief Information Security Officer with responsibilities related to this Consent Decree, shall have specific knowledge of the information security principles and practices necessary to implement the information security requirements of this Consent Decree, and the specific requirements of the Privacy Laws relevant to their duties, prior to assuming their duties.

17. **Compliance Plan**. For purposes of settling the matters set forth herein, Cox agrees that it shall, within one hundred

twenty (120) calendar days after the Effective Date, supplement its existing compliance policies and procedures regarding the Privacy Laws by developing and implementing a Compliance Plan designed to ensure future compliance with the Privacy Laws, and with the terms and conditions of this Consent Decree, which shall be implemented and operated in accordance with Cox's risk-based approach. Such Compliance Plan must include the following components:

9 (a) **Risk Assessment. Cox shall conduct a comprehensive and thorough risk assessment, conducted with reference to the NIST Cybersecurity Framework, to identify internal and external risks to the security, confidentiality, and integrity of PI/CPNI collected or maintained by Cox or Covered Third Parties that could result in unauthorized access, disclosure, misuse, destruction, or compromise of such information (Risk Assessment). The Risk Assessment, which shall be completed no later than December 31, 2016, must evaluate in writing the likelihood and potential impact of these threats and the sufficiency of existing policies, procedures, and other safeguards in place to control risks. Additional Risk Assessments shall be conducted at least biennially and Cox shall notify the Commission of completion of the Risk Assessments within thirty (30) calendar days via e-mail to the persons listed in paragraph 19(d).

*12311 (b) **Information Security Program**. Within one hundred fifty (150) calendar days after the Effective Date, Cox shall review and revise as appropriate its information security program to ensure that, using a risk-based approach, it has a reasonable and comprehensive security program to protect the security, confidentiality, and integrity of PI and CPNI collected and/or maintained by Cox or Covered Third Parties (Information Security Program). Cox shall ensure that such Information Security Program is documented in writing (including, as appropriate, within the Operating Procedures and Compliance Manual described below) and includes:

i. Administrative, technical, and physical safeguards that are reasonable in light of Cox's size and complexity, the nature and scope of Cox's activities, the sensitivity of the PI/CPNI collected or maintained by or on behalf of Cox, and the risks identified through risk assessments, including the use of multiple factor authentication or equivalent control(s) for Covered Employees' access to PI/CPNI;

ii. Reasonable measures to protect PI/CPNI collected or maintained by Covered Third Parties, including exercising due diligence in selecting Covered Third Parties, where reasonably feasible requiring Covered Third Parties by contract (upon execution of new agreements and renewal agreements) to implement and maintain reasonable and comprehensive safeguards of both the physical and electronic protection of PI/CPNI equivalent to the safeguards used by Covered Employees (e.g., with regard to multiple factor access/authentication or equivalent control(s) to Cox data systems/Customer information), engaging in appropriate verification of Covered Third Parties' compliance with their security obligations, and implementing appropriate measures to sanction Covered Third Parties that fail to comply with their security obligations (including, where appropriate, terminating Cox's relationship with such Covered Third Parties); and

iii. Policies and procedures to properly identify the nature and extent of CPNI and PI collected or maintained by Cox and Covered Third Parties, minimize the number of Employees who have access to PI and CPNI on a strictly need-to-know basis tied to job functions, collect the minimum amount of PI necessary to provision and provide services, and collect and maintain PI in a manner that is secure.

**10 In addition, and in accordance with its risk-based approach, Cox shall:

iv. Review and evaluate periodically the effectiveness of the Information Security Program's key controls, systems, and procedures particularly with regard to how such controls, systems, and procedures impact compliance with the Privacy Laws;

v. Monitor critical points within Cox's infrastructure containing PI and CPNI for security events. This process includes taking information feeds from industry sources and internal detection tools (e.g., antivirus) and correlating these information sources to alert Cox's security monitoring center when a potential event has occurred. The security monitoring team will take action on alerts as necessary;

vi. Adjust and update its Information Security Program as appropriate in light of limitations and deficiencies indicated by the reviews, evaluations, and monitoring described herein; and

*12312 vii. Conduct annual audits of selected call center systems and processes using procedures and standards generally

accepted in the profession, to ensure compliance with the Privacy Laws and this Consent Decree. The audits may be performed by Cox Enterprises Inc.'s Audit Services team (which operates separately from Cox) and which itself and through a co-sourcing relationship with a large global external audit firm, which Cox represents has the requisite knowledge and information-security related certifications including but not limited to: Certified Information Security Auditor; Certified Information Systems Security Professional; Certified Privacy Technologist; Certified Risk and Information Systems Control; Certified Fraud Examiner; and Certified Internal Auditor. Systems and processes shall be selected for audit based on Cox's risk evaluations and prioritization. Cox will notify the Commission of the completion of the audits within thirty (30) days via e-mail to the persons listed in paragraph 19(d).

viii. Conduct annual penetration testing of selected systems and processes related to payment cards and collection and storage of PI/CPNI. Systems and processes shall be selected for testing based on Cox's reasonable risk evaluations and prioritization.

ix. Develop an approach to internal threat monitoring that includes the detection of anomalous conduct by Covered Employees no later than December 31, 2016 and begin implementing such approach within one hundred twenty (120) days of that date.

(c) **Third Party Oversight**. Within one hundred twenty (120) calendar days after the completion of the Information Security Program, Cox shall implement the provisions of paragraph 17(b)(ii). In addition, Cox shall require all off-network access by Covered Third Parties with access to Cox customer PI/CPNI to be authenticated through an approved site-to-site virtual private network by December 31, 2016. Furthermore, by the first quarter of 2016, Cox shall conduct a formal assessment by a third party consulting firm to identify additional two-factor authentication opportunities, and by the end of the first quarter of 2016 shall complete the migration of all Covered Third Parties with access to Cox customer PI/CPNI leveraging remote access Citrix platforms to a two-factor authentication solution.

****11** (d) **Incident Response Plan**. Within one hundred and twenty (120) calendar days after the Effective Date, Cox shall review, revise and maintain its Incident Response Plan to ensure that it is reasonable, comprehensive, and enables Cox to detect, respond to, and provide timely notification, in accordance with the Privacy Laws, applicable law, and the requirements of subpart 17(e) below, to all relevant Customers and relevant governmental authorities of data breaches involving PI and CPNI. Such Incident Response Plan shall contain processes to (i) identify, (ii) investigate, (iii) mitigate, (iv) remediate, and (v) review information security incidents to identify root causes and to develop improved responses to security threats. Cox shall perform annual test exercises of the Incident Response Plan, and shall subject such plan to third-party review.

(e) **Breach Notification**. Within one hundred and twenty (120) calendar days after the Effective Date, and periodically thereafter, Cox shall review its breach notification practices to ensure that, to the extent they do not already so provide, in the event of an unauthorized breach of Customer PI/CPNI, Cox shall: (i) at least to the extent required by federal or state law, or guidance from law enforcement, notify all Customers (at the Customer's last known address and pursuant to Cox's reasonable ***12313** efforts to locate the Customer) whose unredacted and/ or unencrypted PI/CPNI information has been, or for which Cox knew, acquired by an unauthorized person; (ii) offer complimentary credit monitoring service for a minimum of one year to any Customer whose unredacted and/or unencrypted PI/CPNI is reasonably believed by Cox to have been acquired by an unauthorized person and if, consistent with industry practices, Cox reasonably believes involves a risk of identity theft; and (iii) conduct targeted monitoring of known websites for breach activity to identify potential Customer PI/CPNI data. Cox shall ensure that policies and statements on Cox's websites regarding the security of Customers' PI and CPNI accurately reflect Cox's data security practices, and are updated routinely to reflect any material changes.

(f) **Remediation Measures**. To the extent that Cox has not previously satisfied the requirements set forth below, within one hundred and twenty (120) calendar days after the Effective Date, unless otherwise indicated, Cox shall, with respect to the breach that was the subject of the Investigation:
i. Continue conducting targeted monitoring of known websites for breach activity to identify potential Affected Customer PI/CPNI data;

ii. Offer to provide one year of complimentary credit monitoring services to all Affected Customers through a nationally recognized credit monitoring service, the availability of which must be described in the notice discussed below; and

iii. Identify each Affected Customer and ensure that each Affected Customer has been notified (at the Customer's last known address and pursuant to Cox's reasonable efforts to locate the Customer) that his or her PI and/or CPNI was compromised. The notification to each Affected Customer must include:
**12 a. A general description of the manner in which the Affected Customer's PI/CPNI was compromised;

b. A general description for all Affected Customers of the type of PI/CPNI that was compromised;

c. The toll-free telephone numbers and addresses of the major credit reporting agencies;

d. Information regarding the complimentary credit monitoring services available to Affected Customers;

e. A toll-free hotline or website where Affected Customers may contact Cox to inquire about their compromised PI, and receive reasonable and comprehensive counseling on responding to and mitigating credit harm incidences, including identity theft; and

f. Reasonable and comprehensive information regarding free and/or readily available credit protection options including obtaining free annual credit reports, placing fraud alerts on credit files, requesting security freezes, contacting financial institutions, and any other such free and/or readily available credit protections.

(g) **Notice of Consent Decree**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall deliver a copy of this Consent Decree to all existing Covered Employees, and shall also deliver a copy of this Consent Decree to all future Covered Employees within sixty (60) calendar days after the person assumes such *12314 position or responsibilities. The Consent Decree can be delivered together with the Compliance Manual as provided in subpart 17(i) below.

(h) **Operating Procedures**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall establish Operating Procedures that all Covered Employees must follow to help ensure Cox's compliance with this Consent Decree, including the policies and procedures adopted pursuant to subparts (a)-(g) of this paragraph, and the Privacy Laws. Cox shall also develop a compliance checklist that describes the key steps that a Covered Employee must follow to ensure compliance with this Consent Decree and the Privacy Laws.

(i) **Compliance Manual**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall review, revise, use, and maintain a Compliance Manual (which may be in hard copy and/or electronic format). Within the same period, Cox shall distribute the Compliance Manual to all Covered Employees and to each Covered Third Party, requesting, and, where permitted by contract, requiring the Covered Third Party to distribute the Compliance Manual to each Covered Third Party Employee. For any person who becomes a Covered Employee more than one hundred twenty (120) calendar days after the Effective Date, Cox shall distribute the Compliance Manual to that person within sixty (60) calendar days after the date such person becomes a Covered Employee, and prior to such person engaging with Customers with respect to Cox's services. Further, Cox shall request, and where permitted by contract, require each Covered Third Party to distribute the Compliance Manual to each person who becomes a Covered Third Party Employee more than one hundred twenty (120) calendar days after the Effective Date within sixty (60) calendar days after such person becomes a Covered Third Party Employee, and prior to such person engaging with Customers with respect to Cox's services.
**13 i. The Compliance Manual shall set forth and explain the requirements of the Privacy Laws and this Consent Decree, and shall instruct Covered Employees to ensure Cox's compliance with the Privacy Laws and this Consent Decree, including the policies and procedures adopted pursuant to subparts (a)-(h) of this paragraph. Cox shall request, and where permitted by contract require, Covered Third Parties to direct Covered Third Party Employees to consult and follow the Operating Procedures.

ii. The Compliance Manual shall require Covered Employees to contact their supervisor or the Compliance Officer with any questions or concerns that arise with respect to Cox's obligations under or compliance with the Privacy Laws and this Consent Decree, and require any supervisor who receives such information from a Covered Employee or Covered Third

Party Employee to promptly notify the Compliance Officer. Cox shall request, and where permitted by contract require, Covered Third Parties to provide appropriate mechanisms for Covered Third Party Employees to contact their supervisor with any questions or concerns that arise with respect to their obligations under or compliance with the Privacy Laws and this Consent Decree, and for any such supervisor who receives such information from a Covered Third Party Employee to promptly notify the Compliance Officer. Cox shall provide and request, and, where permitted by contract, require Covered Third Parties to provide a hotline or other appropriate mechanism for anonymous reporting of any noncompliance.

***12315** iii. Cox shall review and revise the Compliance Manual to ensure that the information set forth therein remains current and complete.

iv. Cox shall distribute any revisions of the Compliance Manual to all Covered Employees and Covered Third Parties within sixty (60) calendar days after any revisions have been made by Cox. These revisions may be in electronic format.

(j) **Compliance Training Program**. Within six months after the Effective Date, Cox shall review, revise, implement, and maintain a compliance training program to ensure compliance with the Privacy Laws and this Consent Decree. In addition, Cox shall request, and where permitted by contract, require all Covered Third Parties to ensure that their Covered Third Party Employees receive training in accordance with the Compliance Training Program:
i. The Compliance Training Program shall include reasonable and comprehensive privacy and security awareness training for all Covered Employees. The program shall include instruction on Cox's obligations, policies, and procedures for protecting PI and CPNI pursuant to the Privacy Laws and this Consent Decree, including identifying and collecting PI from Customers, recognizing security threats and suspicious activity that may indicate that PI has been compromised, the timely reporting of data breaches, and other reasonable and appropriate training regarding the protection of PI and CPNI. Cox shall cause all Covered Employees whose job functions relate to the implementation of the remediation measures described in paragraph 17(f) to receive training regarding such remediation measures, as described below. For purposes of complying with the provisions of this paragraph, Cox is permitted to provide the training or use a third party to provide the training described herein.

****14** ii. As part of the Compliance Training Program, Cox shall ensure that each Covered Employee is advised of Cox's obligations to report any noncompliance with the Privacy Laws and this Consent Decree, and is instructed on how to disclose noncompliance to the Compliance Officer, including instructions on how to anonymously report such noncompliance. Cox shall request, and where permitted by contract, require, Covered Third Parties to disseminate the same instructions to each Covered Third Party Employee.

iii. Cox shall ensure that the training for Covered Employees is conducted pursuant to the Compliance Training Program within six (6) months after the Effective Date, except that any person who becomes a Covered Employee at any time after the initial Compliance Training Program shall be trained within sixty (60) calendar days after the date such person becomes a Covered Employee. Cox shall document its Covered Employees' completion of the training. Cox shall request, and where permitted by contract, require all Covered Third Parties to conduct the same type of training for each of their Covered Third Party Employees within the same period, and to document completion of that training.

iv. Within one hundred eighty (180) calendar days after the Effective Date, Cox shall not allow any Covered Employee to interact with any Customer about Cox's service until the Covered Employee has been ***12316** trained and has received a copy of the Compliance Manual. Beginning within one hundred eighty (180) calendar days after the Effective date, Cox shall further request, and where permitted by contract, require all Covered Third Parties to ensure that their Covered Third Party Employees shall not interact with any Customer about Cox's service until their Covered Third Party Employees have been trained consistent with this subparagraph 17(j); and

v. Cox shall ensure that the Compliance Training Program is conducted at least annually for Covered Employees. Cox shall request, and where permitted by contract, require Covered Third Parties to ensure that the Compliance Training Program is conducted at least annually for Covered Third Party Employees. Cox shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness.

18. **Reporting Noncompliance**. Cox shall report any material noncompliance with the Privacy Laws, and the terms and conditions of this Consent Decree, within fifteen (15) calendar days after discovery by the Compliance Officer, Chief Information Security Officer, or managers reporting to either the Compliance Officer or Chief Information Security Officer with responsibilities related to this Consent Decree, of such noncompliance. Such reports shall include a detailed explanation of: (i) each known instance of noncompliance; (ii) the steps that Cox has taken or will take to remedy such noncompliance; (iii) the schedule on which such remedial actions will be taken; and (iv) the steps that Cox has taken or will take to prevent the recurrence of any such noncompliance. Cox shall also report to the FCC any breaches of PI or CPNI involving any Covered Employees or Covered Third Party Employees that Cox is required by any federal or state law to report to any Federal or state entity or any individual. Reports shall be submitted no later than seven (7) business days after completion of the notification required by Federal or state authorities. Such reports shall include: (i) the date the breach was reported; (ii) the applicable Federal and state authorities to whom the breach was reported; (iii) copies of the reports Cox submitted to the applicable Federal and state authorities; and (iv) the reference number generated by the central reporting facility for CPNI reports made pursuant to 47 C.F.R. § 64.2011(b). All reports of noncompliance or PI/CPNI breaches shall be submitted to the Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4-C321, Washington, DC 20554, with a copy submitted electronically to David.Roberts@fcc.gov, Kenneth.Scheibel@fcc.gov, Jennifer.Lewis@fcc.gov, and Dana.Leavitt@fcc.gov.

15 19. **Compliance Reports. Cox shall file compliance reports with the Commission six (6) months after the Effective Date, twelve (12) months after the Effective Date, twenty-four (24) months after the Effective Date, and thirty-six (36) months after the Effective Date.
(a) Each Compliance Report shall include a detailed description of Cox's efforts during the relevant period to comply with the terms and conditions of this Consent Decree and the Privacy Laws. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of Cox, stating that the Compliance Officer has personal knowledge that Cox: (i) has established and implemented the Compliance Plan required by paragraph 17; (ii) has utilized the applicable Operating Procedures since the implementation of the Compliance Plan; and (iii) is not aware of any instances of material noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in paragraph 18 of this Consent Decree.

(b) The Compliance Officer's certification shall be accompanied by a statement explaining the basis for such certification and shall comply with Section 1.16 of the *12317 Rules and be subscribed to as true under penalty of perjury in substantially the form set forth therein.[31]

(c) If the Compliance Officer cannot provide the requisite certification, the Compliance Officer, as an agent of and on behalf of Cox, shall provide the Commission with a detailed explanation of the reason(s) why and describe fully: (i) each instance of such noncompliance; (ii) the steps Cox has taken or will take to remedy such noncompliance, including the schedule on which proposed remedial actions will be taken; and (iii) the steps that Cox has taken or will take to prevent the recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

(d) All Compliance Reports shall be submitted to the Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4-C321, Washington, DC 20554, with copies submitted electronically to Jennifer.Lewis@fcc.gov, Dana.Leavitt@fcc.gov, Kenneth.Scheibel@fcc.gov, and David.Roberts@fcc.gov.

20. **Termination Date**. Unless stated otherwise, the obligations set forth in paragraphs 18 and 19 of this Consent Decree shall expire thirty-six (36) months after the Effective Date. The obligations set forth in paragraphs 16, 17(a) and 17(b) shall expire seven (7) years after the Effective Date. The obligations set forth in paragraphs 17(c)-(j) shall expire six (6) years after the Effective Date.

21. **Section 208 Complaints; Subsequent Investigations**. Nothing in this Consent Decree shall prevent the Commission or its delegated authority from adjudicating complaints filed pursuant to Section 208 of the Act[32] against Cox for alleged violations of the Act, or for any other type of alleged misconduct, regardless of when such misconduct took place. The

Commission's adjudication of any such complaint will be based solely on the record developed in that proceeding. Except as expressly provided in this Consent Decree, this Consent Decree shall not prevent the Commission from investigating new evidence of noncompliance by Cox with the Communications Laws.

16 22. **Civil Penalty Cox shall pay a civil penalty to the United States Treasury in the amount of Five Hundred Ninety-five Thousand dollars ($595,000.00) (Civil Penalty). Cox shall send electronic notification of payment to Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission at Jeffrey.Gee@fcc.gov, David.Roberts@fcc.gov, Kenneth.Scheibel@fcc.gov, Jennifer.Lewis@fcc.gov, and Dana.Leavitt@fcc.gov, on the date said payment is made. The payment must be made by check or similar instrument, wire transfer, or credit card, and must include the Account Number and FRN referenced above. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.[33] When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in block number 24A (payment type code). Below are additional instructions that should be followed based on the form of payment selected:
· Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank — Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

· **12318 . Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.

· Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank —Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

Questions regarding payment procedures should be addressed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES @fcc.gov.

23. **Waivers**. As of the Effective Date, Cox waives any and all rights it may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this Consent Decree and the Adopting Order. Cox shall retain the right to challenge Commission interpretation of the Consent Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the Consent Decree or the Adopting Order, neither Cox nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and Cox shall waive any statutory right to a trial *de novo*. Cox hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act[34] relating to the matters addressed in this Consent Decree.

17 24. **Severability. The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

25. **Invalidity**. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

26. **Subsequent Rule or Order**. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or Order adopted by the Commission (except an Order specifically intended to revise the terms of this Consent Decree to which Cox does not expressly consent) that provision will be superseded by such Rule or Order.

27. **Limitation**. The definitions and terms set out in this Consent Decree are intended solely for this Consent Decree and not as an extension or limitation of the Privacy Laws.

28. **Successors and Assigns**. Cox agrees that the provisions of this Consent Decree shall be binding on its successors,

assigns, and transferees.

29. **Final Settlement**. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigation.

30. **Modifications**. This Consent Decree cannot be modified without the advance written consent of all Parties.

***12319** 31. **Paragraph Headings**. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

32. **Authorized Representative**. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

33. **Counterparts**. This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

_____

Travis LeBlanc, Chief

Enforcement Bureau

_____

Date

_____

Jennifer W. Hightower

Senior Vice President and General Counsel

Cox Communications, Inc.

_____

Date

Footnotes

1 47 U.S.C. § 551(c)(1); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12525 para. 24 n.61 (1996) ("[I]n the Cable Communications Policy Act of 1984, Congress ... sought to restrict unauthorized use of personably identifiable information [PII] by cable operators.").

The Cable Act generally prohibits the disclosure of PII unless such disclosure is necessary to render the services requested or for a legitimate business activity related to such service. *See 47 U.S.C. § 551(c)(2)(A). See also id.* §§ 201, 222(a), (c); 47 C.F.R. § 64.2010.

2 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927,

6959, para. 64 (2007).

3 *See* 47 C.F.R. § 64.2011(b).

4 *See* 47 U.S.C. §§ 201, 222(a), (c); 47 C.F.R. §§ 64.2010, 64.2011.

5 *See* 47 C.F.R. § 1.93(b).

6 47 U.S.C. § 154(i).

7 47 C.F.R §§ 0.111, 0.311.

1 47 U.S.C. §§ 201(b), 222(a) and (c), 551; 47 C.F.R. §§ 64.2010(a) and 64.2011(b).

2 47 U.S.C. § 151 *et seq.*

3 *See, e.g.*, Letter from Jeffrey J. Gee, then-Acting Chief, Investigations and Hearings Division, Enforcement Bureau to Barry J. Ohlson, Esq., Vice President, Regulatory Affairs, Cox Enterprises, Inc., (Feb. 12, 2015) (on file in EB-IHD-14-00017829). Cox responded to that letter and subsequent requests for information, and Cox requested confidential treatment of specified information contained in its responses (including material contained in the accompanying exhibits) pursuant to Sections 0.457 and 0.459 of the Rules. *See* 47 C.F.R. §§ 0.457, 0.459. Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox, to Jennifer A. Lewis, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission (Mar. 16, 2015) (on file in EB-IHD-14-00017829) (LOI Response); Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox Communications, to Marlene H. Dortch, Secretary, Federal Communications Commission (May 4, 2015) (on file in EB-IHD-14-00017829) (Supplemental LOI Response); Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox Communications, to Marlene H. Dortch, Secretary, Federal Communications Commission (May 20, 2015) (on file in EB-IHD-14-00017829). Because we do not disclose material Cox identified as confidential, we defer ruling on the requests unless and until necessary. *See* 47 C.F.R. § 0.459(d)(3) (permitting deferred rulings until a request for inspection has been made pursuant to Sections 0.460 or 0.461 of the Rules; such materials will be accorded confidential treatment until the Commission acts on such requests and all subsequent appeal and stay proceedings have been exhausted).

4 47 U.S.C. § 551(c)(1).

5 *See id.* § 222.

6 *Id.* § 222(a).

7 *See, e.g., Terracom Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13330-13332, paras. 14-19 (2014) (citing *Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed

Rulemaking, 27 FCC Rcd 6656, 6745 para. 207 (2012)) (*Terracom NAL*), *settled by* *TerraCom, Inc. and YourTel America, Inc.*, Order and Consent Decree, 30 FCC Rcd 7075 (Enf. Bur. 2015).

8 *Id.*

9 *Id.* at 13331, para. 17.

10 *See* 47 U.S.C. § 222(c).

11 *See* 47 C.F.R. § 64.2010(a).

12 *Id.* § 64.2011(b).

13 47 U.S.C. § 201(b).

14 *Terracom NAL*, 29 FCC Rcd at 13335-36, paras. 31-32.

15 *Id.*

16 Cox Communications Fact Sheet, http://newsroom.cox.com/company-overview (last visited Nov. 3, 2015).

17 *See* Cox Communications Digital Telephone Fact Sheet, http://newsroom.cox.com/product-fact-sheets (last visited Nov. 3, 2015).

18 *See* LOI Response at 1-2, 8-10.

19 "Pretexting" is a form of misrepresentation whereby the perpetrator adopts the identity of a legitimate person or entity to obtain confidential and personal information belonging to the targeted individual. *See* Federal Bureau of Investigation, "Owner, Employee, and Contractor of Private Investigative Firm Sentenced in Connection with Pretexting" (Dec. 14, 2012), https://www.fbi.gov/sanfrancisco/press-releases/2012/owner-employee-and-contractor-of-private-investigative-firm-sentenced-in-connection-with-pretexting.

20 *See* LOI Response at 1-2, 8-9. "Phishing" is the deceptive use of an identity that appears to come from a legitimate, well-known source in order to trick an individual into divulging sensitive or personal information, such as account numbers or passwords, often through a link to a copycat of the purported source's Web site. *See* Federal Trade Commission, FTC Issues Staff Report on Roundtable Discussion About Phishing Education (Jul. 14, 2008),

https://www.ftc.gov/news-events/press-releases/2008/07/ftc-issues-staff-report-roundtable-discussion-about-phishing.

21 LOI Response at 1-2, 8-9.

22 *See* LOI Response at 1-2, 8-10. The Bureau's review of the record also shows that a single Cox subscriber reported a possible incident by a hacker using the alias "chF," (an apparent member of the Lizard Squad) to Cox on July 22 and 31, 2014. *See, e.g.*, LOI Response at Bates # 00643-48, 01640-41.

23 *See* Supplemental LOI Response at 8-9.

24 *See* LOI Response at 2; Supplemental LOI Response at 10. No credit card information could have been viewed and only the last four digits of the Social Security number and driver's license number, not the entire Social Security or driver's license number, could have been viewed. LOI Response at 11; Supplemental LOI Response at 8-9.

25 *See* Supplemental LOI Response at 2.

26 *Id.*

27 *See* LOI Response at 9-10.

28 *See id.* at 9-10; 17-18.

29 *See id.* at 14.

30 *See* 47 C.F.R. § 1.93(b).

31 *See* 47 C.F.R. § 1.16.

32 47 U.S.C. § 208.

33 An FCC Form 159 and detailed instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

[34] *See* 5 U.S.C. § 504; 47 C.F.R. §§ 1.1501-1.1530.

30 FCC Rcd. 12302 (F.C.C.), 30 F.C.C.R. 12302, 63 Communications Reg. (P&F) 1064, 2015 WL 6779864

No. 23-55375

IN THE UNITED STATES COURT OF APPEAL

FOR THE NINTH CIRCUIT

MICHAEL TERPIN, *Plaintiff-Appellant*,

v.

AT&T MOBILITY LLC, *Defendant-Appellee*.

On Appeal from the United States District Court
for the Central District of California
Case No. 2:18-cv-06975-ODW-KS

APPELLANT'S ADDENDUM OF AUTHORITIES

VOLUME 2

Pierce O'Donnell
Timothy J. Toohey
Emily Avazian
GREENBERG GLUSKER FIELDS
CLAMAN & MACHTINGER LLP
2049 Century Park East,
Suite 2600
Los Angeles, California 90067
Telephone: (310) 553-3610
Email: POdonnell@ggfirm.com
TToohey@ggfirm.com
EAvazian@ggfirm.com

Attorneys for Plaintiff-Appellant
MICHAEL TERPIN

INDEX

ADDENDUM OF STATUTES, REGULATIONS AND UNPUBLISHED OPINIONS ("ADD")

STATUTES

REGULATORY MATERIALS: FEDERAL COMMMUNICATOINS COMMISSION (FCC)

Document	Description	ADD Nos.
	and Other Customer Information (June 27, 2013)	
29 FCC Rcd 13325, 29 F.C.C.R. 13325, 2014 WL 5439575	*In the Matter of Terracom, Inc. and Yourtel America, Inc. Apparent Liability for Forfeiture* (October 24, 2014)	ADD-180 – ADD-211
30 FCC Rcd. 2808, 30 F.C.C.R. 2808, 2015 WL 1577197	*In the Matter of AT&T Services, Inc.* (April 8, 2015)	ADD-212 – ADD-225
30 FCC Rcd. 7075, 30 F.C.C.R. 7075, 2015 WL 4159266	*In the Matter of Terracom, Inc., and Yourtel America, Inc.* (July 9, 2015)	ADD-226 – ADD-244
30 FCC Rcd. 12302, 30 F.C.C.R. 12302, 2015 WL 6779864	*In the Matter of Cox Communications, Inc.* (November 5, 2015)	ADD-245 – ADD-260
31 FCC Rcd. 13911, 31 F.C.C.R. 13911, 2016 WL 6538282	*In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (November 2, 2016), superseded by Rule *In the Matter of Restoring Internet Freedom*, January 4, 2018	ADD-266 – ADD-493
FCC 20-26, File No.: EB-TCD-18-00027704	*In the Matter of AT&T Inc.: Notice of Apparent Liability for Forfeiture and Admonishment* (February 28, 2020)	ADD-494 – ADD-535
36 FCC Rcd 14120, 36 F.C.C.R. 14120, 2021 WL 4735472	*In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud* (September 30, 2021)	ADD-541 – ADD-587

UNPUBLISHED DECISIONS

Document	ADD Nos.
Fraser v. Mint Mobile, LLC, No. C 22-00138 WHA, 2022 WL 1240864 (N.D. Cal. Apr. 27, 2022)	ADD-588 – ADD-595
Gatton v. T-Mobile USA, Inc., No. SACV 03-130 DOC, 2003 WL 21530185 (C.D. Cal. Apr. 18, 2003)	ADD-596 – ADD-606
Warren v. PNC Bank National Association, --- F. Supp. 3d --- (2023), No. 22-cv-07875-WHO, 2023 WL 3182952 (N.D. Cal. Apr. 30, 2023)	ADD-607 – ADD-621

31 FCC Rcd. 13911 (F.C.C.), 31 F.C.C.R. 13911, 65 Communications Reg. (P&F) 1349, 2016 WL 6538282

Federal Communications Commission (F.C.C.)
Report and Order

IN THE MATTER OF PROTECTING THE PRIVACY OF CUSTOMERS OF BROADBAND AND OTHER TELECOMMUNICATIONS SERVICES

WC Docket No. 16-106
FCC 16-148
Released: November 2, 2016
Adopted: October 27, 2016

****1 *13911** By the Commission: Chairman Wheeler and Commissioner Rosenworcel issuing separate statements; Commissioner Clyburn approving in part, concurring in part and issuing a statement; Commissioners Pai and O'Rielly dissenting and issuing separate statements.

TABLE OF CONTENTS

I. INTRODUCTION

1. In this Report and Order (Order), we apply the privacy requirements of the Communications Act of 1934, as amended (the Act) to the most significant communications technology of today—broadband Internet access service (BIAS). Privacy rights are fundamental because they protect important personal interests—freedom from identity theft, financial loss, or other economic harms, as well as concerns that intimate, personal details could become the grist for the mills of public embarrassment or harassment or the basis for opaque, but harmful judgments, including discrimination. In adopting Section 222 of the Communications Act, Congress recognized the importance of protecting the privacy of customers using telecommunications networks. Section 222 requires telecommunications ***13913** carriers to protect the confidentiality of customer proprietary information. By reclassifying BIAS as telecommunications service, we have an obligation to make certain that BIAS providers are protecting their customers' privacy while encouraging the technological and business innovation that help drive the many benefits of our increasingly Internet-based economy.

2. Internet access is a critical tool for consumers—it expands our access to vast amounts of information and countless new services. It allows us to seek jobs and expand our career horizons; find and take advantage of educational opportunities; communicate with our health care providers; engage with our government; create and deepen our ties with family, friends and communities; participate in online commerce; and otherwise receive the benefits of being digital citizens. Broadband providers provide the "on ramp" to the Internet. These providers therefore have access to vast amounts of information about their customers including when we are online, where we are physically located when we are online, how long we stay online, what devices we use to access the Internet, what websites we visit, and what applications we use.

****3** 3. Without appropriate privacy protections, use or disclosure of information that our broadband providers collect about us would be at odds with our privacy interests. Through this Order, we therefore adopt rules that give broadband customers the tools they need to make informed choices about the use and sharing of their confidential information by their broadband providers, and we adopt clear, flexible, and enforceable data security and data breach notification requirements. We also revise our existing rules to provide harmonized privacy protections for voice and broadband customers—bringing privacy protections for voice telephony and other telecommunications services into the modern framework we adopt today.

4. In response to the *NPRM*, we received more than 275,000 submissions in the record of this proceeding, including comments, reply comments, and *ex parte* communications from consumers; broadband and voice providers and their associations; public interest groups; academics; federal, state, and local governmental entities; and others. We have listened and learned from the record. In adopting final rules, we rely on that record and in particular we look to the privacy and data security work done by the Federal Trade Commission (FTC), as well as our own work adopting and revising rules under Section 222. We have also taken into account the concepts that animate the Administration's Consumer Privacy Bill of Rights (CPBR), and existing privacy and data security best practices.

5. The privacy framework we adopt today focuses on transparency, choice, and data security, and provides heightened protection for sensitive customer information, consistent with customer expectations. In adopting these rules we honor customer's privacy rights and implement the statutory requirement that carriers protect the confidentiality of customer proprietary information. These rules do not prohibit broadband providers from using or sharing customer information, but rather are designed to protect consumer choice while giving broadband providers the flexibility they need to continue to innovate. By bolstering customer confidence in broadband providers' treatment of confidential customer information, we also promote the virtuous

cycle of innovation in which new uses of the network lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses, business growth, and innovation.

II. EXECUTIVE SUMMARY

6. Today we adopt rules protecting the privacy of broadband customers. We also revise our current rules to harmonize our rules for all telecommunications carriers. In this Order, we first offer some background, explaining the need for these rules, and then discuss the scope of the rules we adopt. In discussing the scope of the rules, we define "telecommunications carriers" that are subject to our rules and the "customers" those rules are designed to protect. We also define the information protected under Section 222 as customer proprietary information (customer PI).[1] We include within the definition of ***13914** customer PI three types of information collected by telecommunications carriers through their provision of broadband or other telecommunications services that are not mutually exclusive: (i) individually identifiable Customer Proprietary Network Information (CPNI) as defined in Section 222(h);[2] (ii) personally identifiable information (PII); and (iii) content of communications. We also adopt and explain our multi-part approach to determining whether data has been properly de-identified and is therefore not subject to the customer choice regime we adopt for customer PI.

****4** 7. We next adopt rules protecting consumer privacy using the three foundations of privacy—transparency, choice, and security:

8. *Transparency*. Recognizing the fundamental importance of transparency to enable consumers to make informed purchasing decisions, we require carriers to provide privacy notices that clearly and accurately inform customers about what confidential information the carriers collect, how they use it, under what circumstances they share it, and the categories of entities with which they will share it. We also require that carriers inform their customers about customers' rights to opt in to or opt out (as the case may be) of the use or sharing of their confidential information. We require that carriers present their privacy notice to customers at the point of sale, and that they make their privacy policies persistently available and easily accessible on their websites, applications, and the functional equivalents thereof. Finally, consistent with FTC best practices and with the requirements in the CPBR,[3] we require carriers to give their customers advance notice of material changes to their privacy policies.

9. *Choice*. We find that because broadband providers are able to view vast swathes of customer data, customers must be empowered to decide how broadband providers may use and share their data. In this section, we adopt rules that give customers of BIAS and other telecommunications services the tools they need to make choices about the use and sharing[4] of customer PI, and to easily adjust those choices over the course of time. In adopting rules governing customer choice, we look to the best practices framework recommended by the FTC in its 2012 Privacy Report[5] as well as the choice framework in the Administration's CPBR and adopt a framework that provides heightened protections for sensitive customer information. For purposes of the sensitivity-based customer choice framework we adopt today, we find that sensitive customer PI includes financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, application usage history, and the functional equivalents of web browsing history or application usage history. With respect to voice services, we also find that call detail information is sensitive information. We also adopt a tiered approach to choice, by reference to consumer expectations and context that recognizes three categories of approval with respect to use of customer PI obtained by virtue of providing the telecommunications service:

***13915** · *Opt-in Approval.* We adopt rules requiring carriers to obtain customers' opt-in approval for use and sharing of sensitive customer PI (and for material retroactive changes to carriers' privacy policies). A familiar example of opt-in practices appears when a mobile application asks for permission to use geo-location information.

****5** · *Opt-out Approval.* Balancing important governmental interests in protecting consumer privacy and the potential benefits that may result from the use of non-sensitive customer PI, we adopt rules requiring carriers to obtain customers' opt-out approval for the use and sharing of non-sensitive customer PI.

· *Congressionally-Recognized Exceptions to Customer Approval Requirements*. Consistent with the statute, we adopt rules that always allow broadband providers to use and share customer data in order to provide broadband services (for example to ensure that a communication destined for a particular person reaches that destination), and for certain other purposes.

10. *Data Security and Breach Notification*. At its most fundamental, the duty to protect the confidentiality of customer PI requires telecommunications carriers to protect the customer PI they collect and maintain. We encourage all carriers to consider data minimization strategies and to embrace the principle of privacy by design. To the extent carriers collect and maintain customer PI, we require BIAS providers and other telecommunications carriers to take reasonable measures to secure customer PI. To comply with this requirement, a carrier must adopt security practices appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider, and technical feasibility. We decline to mandate specific activities that carriers must undertake in order to meet the reasonable data security requirement. We do, however, offer guidance on the types of data security practices we recommend providers strongly consider as they seek to comply with our data security requirement, while recognizing that what constitutes "reasonable" data security evolves over time.

11. We also adopt data breach notification requirements. In order to ensure that affected customers and the appropriate federal agencies receive notice of data breaches that could result in harm, we adopt rules requiring BIAS providers and other telecommunications carriers to notify affected customers, the Commission, and the FBI and Secret Service unless the carrier is able to reasonably determine that a data breach poses no reasonable risk of harm to the affected customers. In the interest of expedient law enforcement response, such notice must be provided to the Commission, the FBI, and Secret Service within seven business days of when a carrier reasonably determines that a breach has occurred if the breach impacts 5,000 or more customers; and must be provided to the applicable federal agencies at least three days before notice to customers. For breaches affecting fewer than 5,000 customers, carriers must notify the Commission without unreasonable delay and no later than thirty (30) calendar days following the carrier's reasonable determination that a breach has occurred. In order to allow carriers more time to determine the specifics of a data breach, carriers must provide notice to affected customers without unreasonable delay, but within no more than 30 days.

****6** 12. *Particular Practices that Raise Privacy Concerns*. Next, we find that take-it-or-leave-it offerings of broadband service contingent on surrendering privacy rights are contrary to the requirements of Sections 222 and 201 of the Act, and therefore prohibit that practice. We also adopt heightened disclosure and affirmative consent requirements for BIAS providers that offer customers financial incentives, such as lower monthly rates, in exchange for the right to use the customers' confidential information. Because the record contains very little about financial incentive practices of voice providers, this section of the Order is limited to BIAS providers.

13. Next we address several other issues raised in our rulemaking, including dispute resolution; the request for an exemption for enterprise customers of telecommunications services other than BIAS; federal preemption; and the timeline for implementation.

14. *Dispute Resolution*. We reaffirm customers' right to use the Commission's existing dispute resolution procedures and commit to initiating a rulemaking on the use of mandatory arbitration ***13916** requirements in consumer contracts for broadband and other communications services, acting on a notice of proposed rulemaking in February 2017.

15. *Exemption for Enterprise Customers of Telecommunications Services other than BIAS*. Recognizing that enterprise customers of telecommunications services other than BIAS have different privacy concerns and the capacity to protect their own interests, we find that a carrier that contracts with an enterprise customer for telecommunications services other than BIAS need not comply with the privacy and data security rules we adopt today if the carrier's contract with that customer specifically addresses the issues of transparency, choice, data security, and data breach and provides a mechanism for the customer to communicate with the carrier about privacy and data security concerns. As with the existing, more limited business customer exemption from our existing authentication rules, carriers will continue to be subject to the statutory requirements of Section 222 even where this exemption applies.

16. *Preemption*. In this section, we adopt the proposal in the *NPRM* and announce our intent to continue to preempt state privacy laws, including data security and data breach laws, *only* to the extent that they are inconsistent with any rules adopted by the Commission. This limited application of our preemption authority is consistent with our precedent in this area and with our long appreciation for the valuable role the states play in protecting consumer privacy.

17. *Implementation Timeline*. The Order provides a timeline for orderly transition to the new rules with additional time given for small carriers to the extent that they may need to change their practices.

18. *Legal Authority*. Finally, the Order closes by discussing our legal authority to adopt the rules.

III. ESTABLISHING BASELINE PRIVACY PROTECTIONS FOR CUSTOMERS OF TELECOMMUNICATIONS SERVICES

****7** 19. In this section, we adopt a set of rules designed to protect the privacy of customers of BIAS and other telecommunications services. The rules we adopt today find broad support in the record, and are consistent with and build on existing regulatory and stakeholder-driven frameworks, including the Commission's prior decisions and existing Section 222 rules, other federal privacy laws, state privacy laws, and recognized best practices. The framework for our baseline privacy protections focuses on providing transparency of carriers' privacy practices; ensuring customers have meaningful choice about the use and disclosure of their private information; and requiring carriers to adopt robust data security practices for customer information. In this section, we explain the rules we adopt to protect the privacy of customers of BIAS and other telecommunications services.

A. Background and Need for the Rules

20. The Commission has a long history of protecting customer privacy in the telecommunications sector. Section 705 of the Communications Act, for example, is one of the most fundamental and oldest sector-specific privacy requirements, and protects the privacy of information carried by communications service providers.[6] As early as the 1960s the Commission began to wrestle with the privacy implications of the use of communications networks to provide shared access to computers and the sensitive, personal data they often contained.[7] Throughout the 1980s and 1990s, the ***13917** Commission imposed limitations on incumbent telephone companies' use and sharing of customer information.[8]

21. Then, in 1996, Congress enacted Section 222 of the Communications Act providing statutory protections to the privacy of the data that all telecommunications carriers collect from their customers. Congress recognized that telecommunications networks have the ability to collect information from consumers who are merely using networks as conduits to move information from one place to another "without change in the form or content" of the communications.[9] Specifically, Congress sought to ensure "(1) the right of consumers to know the specific information that is being collected about them; (2) the right of consumers to have proper notice that such information is being used for other purposes; and (3) the right of consumers to stop the reuse or sale of that information."[10]

22. Section 222(a) imposes a duty on all telecommunications carriers to protect the confidentiality of their customers' "proprietary information," or PI.[11] Section 222(c) imposes restrictions on telecommunications carriers' use and sharing of customer proprietary network information (CPNI) without customer approval, subject to certain exceptions including as necessary to provide the telecommunications service (or services necessary to or used in providing that telecommunications service), and as otherwise provided for by law.[12] While we recognize, applaud, and encourage existing and continued marketplace self-regulation and privacy innovations, Congress has made clear that telecommunications carriers' privacy

practices must comply with the obligations imposed by Section 222. We therefore reject arguments that we rely entirely on self-regulatory mechanisms.[13]

**8 23. Over the last two decades, the Commission has promulgated, revised, and enforced privacy rules for telecommunications carriers that are focused on implementing the CPNI requirements of Section 222. As practices have changed, the Commission has refined its Section 222 rules. For example, after the emergence and growth of an industry made possible by "pretexting"—the practice of improperly accessing and selling details of residential telephone calls—the Commission strengthened its Section 222 rules to add customer authentication and data breach notification requirements.[14] The current Section 222 rules focus on transparency, choice, data security, and data breach notification.

*13918 24. Meanwhile, as consumer use of the Internet exploded, the FTC, using its authority under Section 5 of the FTC Act to prohibit "unfair or deceptive acts or practices in or affecting commerce,"[15] has entered into a series of precedent-setting consent orders addressing privacy practices on the Internet, held workshops and conferences, and issued influential reports about privacy.[16] Taken together, the FTC's privacy work has focused on the importance of transparency; honoring consumers' expectations about the use of their personal information and the choices they have made about sharing that information; and the obligation of companies that collect personal information to adopt reasonable data security practices. Because common carriers subject to the Communications Act are exempt from the FTC's Section 5 authority, the responsibility falls to this Commission to oversee their privacy practices consistent with the Communications Act.[17]

25. Last year the Administration proposed a Consumer Privacy Bill of Rights. The goal of the CPBR is to "establish baseline protections for individual privacy in the commercial arena and to foster timely, flexible implementations of these protections through enforceable codes of conduct developed by diverse stakeholders."[18] It recognizes that Americans "cherish privacy as an element of their individual freedom," and that "[p]reserving individuals' trust and confidence that personal data will be protected appropriately, while supporting flexibility and the free flow of information, will promote continued innovation and economic growth in the networked economy."[19]

26. Prior to 2015, BIAS was classified as an information service, which excluded such services from the ambit of Title II of the Act, including Section 222, and the Commission's CPNI rules.[20] Instead, broadband providers were subject to the FTC's unfair and deceptive acts and practices authority.[21] In the *2015 Open Internet Order*, we reclassified BIAS as a telecommunications service subject to Title II of the Act, an action upheld by the D.C. Circuit in *United States Telecom Ass'n v. FCC*.[22] While we granted BIAS forbearance from many Title II provisions, we concluded that application and enforcement of the privacy protections in Section 222 to BIAS is in the public interest and necessary for the protection of consumers.[23] However, we questioned whether "the Commission's current rules *13919 implementing section 222 necessarily would be well suited to broadband Internet access service,"" and forbore from the application of these rules to broadband service, "pending the adoption of rules to govern broadband Internet access service in a separate rulemaking proceeding."[24]

**9 27. In March 2016, we adopted the *Broadband Privacy NPRM*, which proposed a framework for applying the longstanding privacy requirements of the Act to BIAS.[25] In the *NPRM*, we proposed rules protecting customer privacy using the three foundations of privacy—transparency, choice, and security—and also sought comment on, among other things, whether we should update rules that govern the application of Section 222 to traditional telephone service and interconnected VoIP service in order to harmonize them with the results of this proceeding.[26]

28. A number of broadband providers, their associations, as well as some other commenters argue that because broadband providers are part of a larger online eco-system that includes edge providers, they should not be subject to a different set of regulations.[27] These arguments ignore the particular role of network providers and the context of the consumer/BIAS provider relationship, and the sector specific privacy statute that governs the use and sharing of information by providers of

telecommunications services. Based on our review of the record, we reaffirm our earlier finding that a broadband provider "sits at a privileged place in the network, the bottleneck between the customer and the rest of the Internet"[28] —a position that we have referred to as a gatekeeper.[29] As such, BIAS providers can collect "an unprecedented breadth" of electronic personal information.[30]

***13920** 29. We disagree with commenters that argue that BIAS providers' insight into customer online activity is no greater than large edge providers because customers' Internet activity is "fractured" between devices, multiple Wi-Fi hotspots, and different providers at home and at work.[31] As commenters have explained, "customers who hop between ISPs on a daily basis often connect to the same networks routinely,"[32] and as such, over time, " each ISP can see a substantial amount of that user's Internet traffic."[33]

30. While we recognize that there are other participants in the Internet ecosystem that can also see and collect consumer data,[34] the record is clear that BIAS providers' gatekeeper position allows them to see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents.[35] By contrast, edge providers only see a slice of any given consumers Internet traffic. As explained in the record, edge providers' visibility into consumers' web browsing activity is necessarily limited. According to the record, only three companies (Google, Facebook, and Twitter) have third party tracking capabilities across more than 10 percent of the top one million websites, and none of those have access to more than approximately 25 percent of web pages.[36] In contrast, a BIAS provider sees 100 percent of a customer's unencrypted Internet traffic.[37]

****10** 31. At the same time, users have much more control over tracking by web third parties than over tracking by BIAS providers. A range of browser extensions are largely effective at blocking ***13921** prominent third parties, "but these tools do nothing to stop data collection on the wire."[38] Further, Professor Nick Feamster explains that unlike other Internet participants that see Domain Name System (DNS) lookups only to their own domains (e.g., google.com, facebook.com, netflix.com), BIAS providers can see DNS lookups every time a customer uses the service to go to a new site.[39]

32. Return Path explains additional unique data to which only BIAS providers have access:

Many BIAS customers are assigned a dynamic ('changing') IP address when they connect to their provider. In these cases, each time a consumer's computer (or router) is rebooted, the ISP dynamically assigns a new IP address to the networking device. While the BIAS provider will have a record of precisely which user was connected to an IP address at a specific point in time, any third party will not, unless they subpoena the BIAS provider for data.[40]

Furthermore, as Mozilla explains, "[b]ecause these are paid services, [the broadband provider has] the subscriber's name, address, phone number and billing history. The combination gives ISPs a very unique, detailed and comprehensive view of their users that can be used to profile them in ways that are commercially lucrative."[41]

33. We agree with commenters that point out that encryption can significantly help protect the privacy of consumer content from BIAS providers.[42] However, even with encryption, by virtue of providing BIAS, BIAS providers maintain access to a significant amount of private information about their customers' online activity, including what websites a customer has visited, how long and during what hours of the day the customer visited various websites, the customer's location, and what mobile device the customer used to access those websites.[43] Moreover, research shows that encrypted web traffic ***13922** can be used to infer the pages within an encrypted site that a customer visits, and that the amount of data transmitted over encrypted connections can also be used to infer the pages a customer visits.[44]

34. The record also indicates that truly pervasive encryption on the Internet is still a long way off, and that many sites still do not encrypt.[45] We observe that several commenters rely on projections that 70 percent of Internet traffic will be encrypted by the end of 2016.[46] However, a significant amount of this encrypted data is video traffic from Netflix, which, according to commenters, accounts for 35 percent of North American Internet traffic.[47] Moreover, "raw packets make for a misleading metric."[48] As further explained by one commenter "watching the full Ultra HD stream of The *Amazing Spider-Man* could generate more than 40GB of traffic, while retrieving the WebMD page for 'pancreatic cancer' generates less than 2MB."[49] What's more, research shows that approximately 84 percent of health websites, 86 percent of shopping websites, and 97 percent of news websites remain unencrypted.[50] These types of websites generate less Internet traffic but contain "much more personalized data."[51] We encourage continued efforts to encrypt personal information both in transit and at rest. At the same time, our policy must account for the fact that encryption is not yet ubiquitous and, in any event, does not preclude BIAS providers from having unique access to customer data.[52]

****11** 35. Thus, the record reflects that BIAS providers are not, in fact, the same as edge providers in all relevant respects. In addition to having access to all unencrypted traffic that passes between the user and edge services while on the network, customers' relationships with their broadband provider is different from those with various edge providers, and their expectations concomitantly differ. For example, customers generally pay a fee for their broadband service, and therefore do not have reason to ***13923** expect that their broadband service is being subsidized by advertising revenues as they do with other Internet ecosystem participants.[53] In addition, consumers have a choice in deciding each time whether to use—and thus reveal information—to an edge provider, such as a social network or a search engine, whereas that is not an option with respect to their BIAS provider when using the service.[54]

36. While some customers can switch BIAS providers, others do not have the benefit of robust competition, particularly in the fixed broadband market. Moreover, we have previously observed that "[b]roadband providers have the ability to act as gatekeepers even in the absence of 'the sort of market concentration that would enable them to impose substantial price increases on end users.'"[55] Their position is strengthened by the high switching costs customers face when seeking a new service, which could deter customers from changing BIAS providers if they are unsatisfied the providers' privacy policies.[56] Moreover, even if a customer was willing to switch to a new broadband provider, the record shows consumers often have limited options.[57] We note, as stated in the 2016 *Broadband Progress Report*, approximately 51 percent of Americans still have only one option for a provider of fixed broadband at speeds of 25 Mbps download/3 Mbps upload.[58] Given all of these factors, we conclude ***13924** that, contrary to assertions in the record,[59] BIAS providers hold a unique position in the Internet ecosystem, and disagree with commenters that assert that rules to protect the privacy of broadband customers are unnecessary.[60]

37. As discussed above and throughout this Order, our sector-specific privacy rules are necessary to address the distinct characteristics of telecommunications services. The record demonstrates that strong customer privacy protections will encourage broadband usage and, in turn investment.[61] We further find that when consumers are confident that their privacy is protected, they will be more likely to adopt and use broadband services.[62] As aptly explained by Mozilla, "[t]he strength of the Web and its economy rests on a number of core building blocks that make up its foundational DNA. When these building blocks are threatened, the overall health and well-being of the Web are put at risk. Privacy is one of these building blocks."[63] The privacy framework we adopt today will bolster consumer trust in the broadband ecosystem, which is essential for business growth and innovation.[64]

B. Scope of Privacy Protections under Section 222

****12** 38. In adopting rules to protect the privacy of customers of BIAS and other telecommunications services, we must begin by specifying the entities and information at issue. We look to the language of the statute to determine the appropriate scope of

our implementing rules. As discussed above, Section 222(a) specifies that telecommunications carriers have a duty to protect the confidentiality of proprietary information of and relating to their customers, while Section 222(c) provides direction about protections to be accorded ""customer proprietary network information." We therefore first adopt rules identifying the set of "telecommunications carriers" that are subject to our rules and define the ***13925** "customers" these rules protect. Next we define "customer proprietary information" and include within that definition " individually identifiable customer proprietary network information," " personally identifiable information," and content of communications.

1. The Rules Apply to Telecommunications Carriers and Interconnected VoIP Providers

39. For purposes of the rules we adopt today to implement Section 222, we adopt a definition of "telecommunications carrier" that includes all telecommunications carriers providing telecommunications services subject to Title II, including broadband Internet access service (BIAS). We also include interconnected VoIP services, which have been covered since 2007.[65] Although not limited to voice services, our existing rules have been focused on voice services.[66] When we reclassified BIAS as a telecommunications service, we recognized that our existing CPNI rules were not necessarily well suited to the broadband context, and we therefore forbore from applying the existing Section 222 rules to BIAS.[67] As part of this rulemaking we have explored what privacy and data security rules we should adopt for BIAS and whether we can harmonize our rules for voice and BIAS. Throughout this Order we find that it is in the interests of consumers and providers to harmonize our voice and broadband privacy rules. We therefore adopt a single definition of telecommunications carrier for purposes of these rules, and except as otherwise provided, adopt harmonized rules governing the privacy and data security practices of all such telecommunications carriers.

40. Because we adopt a single definition of telecommunications carrier we need not change the definitions of "telecommunications carrier or carrier" currently in our rules implementing Section 222.[68] We do amend the definition of telecommunications service to conform to the definition of telecommunications carrier. We also observe that because BIAS is now a telecommunications service, BIAS providers are now telecommunications carriers within the meaning of those rules. To remove any doubt as to the scope of these rules, we define BIAS for purposes of our rules pursuant to Section 222 identically to our definition in the *2015 Open Internet Order*.[69] We define "broadband Internet access service provider" or "BIAS provider" to mean a person engaged in the provision of BIAS.[70] Under the ***13926** *2015 Open Internet Order*'s definition of BIAS, the term BIAS provider does not include "premises operators — such as coffee shops, bookstores, airlines, private end-user networks (e.g., libraries and universities), and other businesses that acquire broadband Internet access service from a broadband provider to enable patrons to access the Internet from their respective establishments.""[71] Moreover, consistent with the *2015 Open Internet Order*,[72] our rules do not govern information that BIAS providers obtain by virtue of providing other non-telecommunications services, such as edge services that the BIAS provider may offer like email, websites, cloud storage services, social media sites, music streaming services, and video streaming services (to name a few).[73]

2. The Rules Protect Customers' Confidential Information

****13** 41. Section 222 governs how telecommunications carriers treat the ""proprietary" and "proprietary network" information of their "customers."[74] For purposes of the rules we adopt today implementing Section 222, we define "customer" as (1) a current or former subscriber to a telecommunications service; or (2) an applicant for a telecommunications service. We adopt a single definition of customer, because we agree with those commenters that argue that harmonizing the definition of "customer" for both BIAS and other telecommunications services will ease consumer expectations, reduce confusion, and streamline compliance costs for BIAS providers, especially small providers.[75] We also find that voice and BIAS customers face similar issues related to the protection of their private information when they apply for, subscribe to, and terminate their telecommunications services.[76]

42. In adopting this definition of customer, we find that BIAS providers' and other telecommunications carriers' duty to protect customer proprietary information under Section 222 begins when a person applies for service and continues after a subscriber terminates his or her service. Our existing rules for voice services apply only to current customers.[77] We are, however, persuaded by commenters that argue that the existing rule's limitation to current subscribers is too narrow.[78] As data ***13927** storage costs decrease and computing power increases, previous barriers to data analysis based on cost, time, or feasibility are receding.[79] BIAS providers and other telecommunications carriers have the technical ability to retain and use applicant and customer information long after the application process or termination of service.[80] If our rules do not protect applicants, consumers would lack basic privacy protections when they share any confidential information in order to apply for a telecommunications service. Similarly, current customers would be penalized for switching providers given that the ""losing" carrier would be free to stop protecting the confidentiality of any private information it retains.[81] These outcomes would run counter to our firm commitment to promote broadband adoption, competition, and innovation.[82] Making this change is consistent with the 2014 Notice of Apparent Liability issued in *TerraCom*, in which we explained that that "the carrier/customer relationship commences when a consumer applies for service."[83]

43. We disagree with commenters that assert that including prospective and former customers within the definition of customer could unduly burden providers.[84] If carriers want to limit their obligations with respect to applicants and former customers, they can and should adopt data minimization practices and destroy applicants' and former customers' confidential information as soon as practicable, in a manner consistent with any other applicable legal obligations.

****14** 44. In addition, for purposes of these rules, we find it appropriate to attribute all activity on a subscription to the subscriber. We recognize that multiple people often use the BIAS or voice services purchased by a single subscriber. For example, residential fixed broadband and voice services often have a single named account holder, but all household members and their guests may use the Internet connection and voice service purchased by that subscriber. Likewise, enterprise customers may have many users on the same account. And, for mobile services, multiple users using separate devices may ***13928** share one account.[85] However, treating each individual user as a separate customer would be burdensome because the provider does not have a separate relationship with each of those users, outside of the relationship with the subscriber. To minimize burdens on both providers and customers, we find it is reasonable to define "customer" to include users of the subscription (such as household members and their guests), but treat the subscriber as the person with authority to make privacy choices for all of the users of the service.[86] As such, we disagree with commenters who argue that every individual using a BIAS subscription should qualify as a distinct customer with separate privacy controls.[87]

45. We recognize that some BIAS or voice subscriptions identify multiple users. For example, some mobile BIAS providers offer group plans in which each person has their own identified device, user ID, and/or telephone number. If a BIAS or other telecommunications provider is already treating each user as distinct and the subscriber authorizes the other users to control their account settings, we encourage carriers to give these users individualized privacy controls.[88]

3. Scope of Customer Information Covered by These Rules

46. In this section, we define the scope of information covered by the rules implementing Section 222. Specifically, we import the statutory definition of customer proprietary network information (CPNI) into our implementing rules, and define customer proprietary information (customer PI) as including individually identifiable CPNI, personally identifiable information (PII), and content of communications. We recognize that these categories are not mutually exclusive, but taken together they identify the types of confidential customer information BIAS providers and other telecommunications carriers may collect or access in connection with their provision of service. Below, we provide additional guidance on the scope of these categories of customer information in the telecommunications context.

a. Customer Proprietary Network Information

47. Consistent with the preexisting voice rules, we adopt the statutory definition of customer proprietary network information (CPNI) for all telecommunications services, including BIAS. Since this is our first opportunity to address this definition's application to BIAS, to offer clarity we provide guidance on the meaning of CPNI as it applies to BIAS. We focus on Section 222(h)(1), which defines CPNI to mean:

****15** (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service ***13929** received by a customer of a carrier; except that [CPNI] does not include subscriber list information.[89]

We agree with commenters that, due to its explicit focus on telephone exchange and telephone toll service, Section 222(h)(1)(B) is not relevant to BIAS.[90]

48. We interpret the phrase "made available to the carrier by the customer solely by virtue of the carrier-customer relationship" in Section 222(h)(1)(A) to include any information falling within a CPNI category that the BIAS provider collects or accesses in connection with the provision of BIAS.[91] This includes information that may also be available to other entities. We disagree with commenters who propose that the phrase "made available to the carrier by the customer solely by virtue of the carrier-customer relationship" means that *only* information that is *uniquely* available to the BIAS provider may satisfy the definition of CPNI.[92] These commenters contend that if a customer's information is available to a third party, it cannot qualify as CPNI, focusing on the term "solely" in the clause. However, the term "solely" modifies the phrase "by virtue of," *not* the phrase "made available to the carrier." We therefore conclude that "solely by virtue of the carrier-customer relationship" means that information constitutes CPNI under Section 222(h)(1)(A) if the provider acquires the information as a product of the relationship and not through an independent means.[93]

49. We also agree with the Center for Democracy and Technology that the fact that third-parties might gain access to the same data when a consumer uses their services "does not negate the fact that the BIAS provider has gained access to the data only because the customer elected to use the BIAS provider's telecommunications service."[94] The statute is silent as to whether such information might be available to other parties, which indicates that Congress did not intend for the definition of CPNI to hinge on such information being solely available to the customers' carrier.[95] Indeed, in the voice context, CPNI certainly is available to other parties besides the customer's carrier and Section 222 protects that data. For example, when a customer calls someone else, CPNI is also made available to the recipient's carrier and intermediaries facilitating the completion of the call. Furthermore, we find that commenters' narrow definition of CPNI is inconsistent with the privacy-protective purpose of the statute.[96] We agree with ***13930** some commenters' assertions that when a BIAS provider acquires information wholly apart from the carrier-customer relationship, such as purchasing public records from a third party, that information is not CPNI.[97]

****16** 50. However, consistent with the Commission's *2013 CPNI Declaratory Ruling*, we find that information that a BIAS provider causes to be collected or stored on a customer's device, including customer premises equipment (CPE) and mobile stations, also meets the statutory definition of CPNI.[98] The "fact that CPNI is on a device and has not yet been transmitted to the carrier's own servers also does not remove the data from the definition of CPNI, if the collection has been done at the carrier's direction."[99]

51. BIAS providers also have the ability, by virtue of the customer-carrier relationship, to create and append CPNI to a customer's Internet traffic. For example, if a carrier inserts a unique identifier header (UIDH), that UIDH is CPNI because, as we will

discuss in greater detail below, it is information in the application layer header that relates to the technical configuration, type, destination, and amount of use of a telecommunications service.[100]

52. We do not believe it is necessary to categorize all personally identifiable information (PII) as CPNI, as suggested by Public Knowledge.[101] While we agree with Public Knowledge's sentiment that PII is confidential information that deserves protection under the Act, and we agree that some information is both PII and CPNI, we find that the Act categorizes and protects all PII as proprietary information, under Section 222(a), as discussed below.[102]

(i) Guidance Regarding Information that Meets the Statutory Definition of CPNI in the Broadband Context

53. In keeping with the Commission's past practice,[103] we decline to set out a comprehensive list of data elements that do or do not satisfy the statutory definition of CPNI in the broadband context.[104] We agree with commenters that "no definition of CPNI should purport or aim to be comprehensive and exhaustive, as technology changes quickly and business models continually seek new ways to monetize ***13931** and market user data."[105] In the past, the Commission has enumerated certain data elements that it considers to be voice CPNI—including call detail records (including caller and recipient phone numbers, and the frequency, duration, and timing of calls) and any services purchased by the customer, such as call waiting; these data continue to be voice CPNI going forward.[106] Similarly, we follow past practice and identify a non-exhaustive list of the types of information that we consider to constitute CPNI in the BIAS context. We find that such guidance will help provide direction regarding the scope of providers' obligations and help to increase customers' confidence in the security of their confidential information as technology continues to advance.[107] We find that the following types of information relate to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and as such constitute CPNI when a BIAS provider acquires or accesses them in connection with its provision of service:
****17** · Broadband Service Plans

· Geo-location

· MAC Addresses and Other Device Identifiers

· IP Addresses and Domain Name Information

· Traffic Statistics

· Port Information

· Application Header

· Application Usage

· Application Payload

· Customer Premises Equipment and Device Information

54. We will first give a brief overview of the structure of Internet communications, to help put these terms in context, and then discuss why each of these types of information, and other related components of Internet Protocol packets, qualify as CPNI.

(a) Background — Components of an Internet Protocol Packet

55. The layered architecture of Internet communications informs our analysis of CPNI in the broadband context. While the concept of layering is not unique to the Internet, layering plays a uniquely prominent role for Internet-based communications and devices. For that reason, we begin with a brief technical overview of the layered structure of Internet communications.

56. Multiple layers—often represented as a vertical stack—comprise every Internet communication. Each layer in the stack serves a particular logical function and uses a network protocol that standardizes communication between systems,[108] enabling rapid innovation in Internet-based ***13932** protocols and applications.[109] Within one device, information is typically transmitted vertically through the various layers.[110] When an application sends data over the Internet, the process begins with application data moving downwards through the layers. Each layer adds additional networking information and functionality, wrapping the output of the layers above it with a "header." The communication sent out over the Internet—consisting of the application data wrapped in headers from each layer—is called a "packet."[111] When a device receives data over the Internet, the reverse process occurs. Data moves upwards through the layers; each layer unwraps its associated information and passes the output upward, until the application on the recipient's device recovers the original application data.[112] As a component of their provision of service, BIAS providers may analyze each of these layers for reasonable network management.[113]

57. Common representations of the Internet's architecture range from four to seven layers.[114] To highlight design properties relevant to the broadband CPNI analysis, we describe a five-layer model in this explanation. From top to bottom, the layers are: application payload, application header, transport, network, and link. We will briefly describe each of the five layers, from top to bottom:

58. *Application Payload*. The information transmitted to and from each application a customer runs is commonly referred to as the application layer payload.[115] The application payload is the substance of the communication between the customer and the entity with which she is communicating. Examples of application payloads include the body of a webpage, the text of an email or instant message, the video served by a streaming service, the audiovisual stream in a video chat, or the maps served by a turn-by-turn navigation app.

****18** 59. *Application Header*. The application will usually append one or more headers to the payload; these headers contain information *about* the application payload that the application is sending or requesting. For example, in web browsing, the Uniform Resource Locator (URL) of a webpage constitutes application header information. In a conversation via email, instant message, or video chat, an application header may disclose the parties to the conversation.[116]

60. *Transport Layer*. Below the application header layer is the transport layer, which forwards data to the intended application on each device and can manage the flow of communications from one device to another device.[117] Port numbers are an example of data within the transport layer header; a port number specifies which application on a device should handle a network communication.

***13933** 61. *Network Layer*. The network layer is below the transport layer, and contains information used to route packets across the Internet from one device to another device. Almost all Internet traffic uses the Internet Protocol (IP) at the network layer.[118] IP addresses are the most common example of data at the network layer; an IP address in a network header indicates the sender or recipient of an Internet packet.[119]

62. *Link Layer*. The final layer is the link layer, which is below the network layer. Link layer protocols route data between devices on the same local network. For example, devices on the same wired or wireless network can usually communicate directly with each other at the link layer.[120] MAC addresses are an example of data at the link layer, and a wide range of link

technologies (Ethernet, DOCSIS, Wi-Fi, and Bluetooth, among others) use them. A MAC address functions as a globally unique device identifier, ensuring that every device on a local network has a distinct address for sending and receiving data.[121]

(b) Specific Examples of CPNI in the BIAS Context

63. With this understanding of the architecture of Internet communications, we can now examine how the components of an IP data packet map to the statutory definition of CPNI.[122] Below, we provide guidance addressing how various data elements constitute CPNI under Section 222.

64. *Broadband Service Plans*. We find that broadband service plans meet the statutory definition of CPNI in the broadband context because they relate to the quantity, type, amount of use, location, and technical configuration of a telecommunications service.[123] We agree with NTCA that "information related to a customer's broadband service plan can be viewed as analogous to voice telephony service plans,"[124] which the Commission has long considered to be CPNI in the voice context.[125] These plans detail subscription information, including the type of service (e.g., fixed or mobile; cable or fiber; prepaid or term contract), speed, pricing, and capacity (e.g., data caps). These data relate to the "type" of telecommunications service to which the customer subscribes, as well as how the BIAS provider will adjust the "technical configuration" of their network to serve that customer. Information pertaining to subscribed capacity and speed relate to the ""quantity" of services the customer purchases, as well as the "amount" of services the customer consumes. Service plans often include the ***13934** customer's address (for billing purposes or to identify the address of service), which relates to the location of use of the service.

****19** 65. *Geo-location*. Geo-location is information related to the physical or geographical location of a customer or the customer's device(s), regardless of the particular technological method used to obtain this information. Providers often need to know where their customers are so that they can route communications to the proper network endpoints. The Commission has already held that geo-location is CPNI,[126] and Congress emphasized the importance of geo-location data by adding Section 222(f).[127]

66. We disagree with commenters who ask us to draw technology-based distinctions for what types of location information are sufficiently precise to qualify as geo-location CPNI.[128] BIAS providers can use many types of data—either individually or in combination—to locate a customer, including but not limited to GPS, address of service, nearby Wi-Fi networks, nearby cell towers, and radio-frequency beacons.[129] We caution that these and other forms of location information in place now or developed in the future constitute geo-location CPNI when made available to the BIAS provider solely by virtue of the carrier-customer relationship.

67. *Media Access Control (MAC) Addresses and Other Device Identifiers*. We conclude that device identifiers, such as MAC addresses, are CPNI in the broadband context because they relate to the technical configuration and destination of use of a telecommunications service.[130] Link layer protocol headers convey MAC addresses, along with other link layer protocol information.[131] A MAC address uniquely identifies the network interface on a device, and thus uniquely identifies the device itself (including the device manufacturer and often the model).[132] MAC addresses relate to the technical configuration and destination of communications because BIAS providers use them to manage their networks and route data packets to the appropriate network device.[133] For the same reasons, we conclude that other device identifiers and other information in link layer protocol headers are CPNI in the ***13935** broadband context because they relate to the technical configuration and destination of use of a telecommunications service.[134]

68. *Internet Protocol (IP) Addresses and Domain Name Information*. We conclude that source and destination IP addresses constitute CPNI in the broadband context because they relate to the destination, technical configuration, and/or location of a telecommunications service.[135] An IP address is a routable address for each device on an IP network,[136] and BIAS providers

use the end user's and edge provider's IP addresses to route data traffic between them.[137] As such, source and destination IP addresses are roughly analogous to telephone numbers in the voice telephony context.[138]

69. We agree with those commenters that argue that the IP addresses a customer uses and those with which she exchanges packets constitute CPNI because both source and destination IP addresses relate to the destination of use of a telecommunications service; one links to the destination for inbound traffic while the other links to the destination for outbound traffic.[139] IP addresses are also frequently used in geo-location.[140] As Public Knowledge explains, "IP addresses can easily be mapped to geographic locations, meaning that both the subscriber and the service can be located."[141] IP addresses relate to technical configuration because BIAS providers configure their systems to use IP addresses in the network layer to communicate data packets between senders and receivers.[142]

**20 70. We disagree with commenters who argue that a customer's IP address is not CPNI. Some commenters argue that a customer's IP address is not CPNI because the BIAS provider assigns the *13936 IP address to the customer,[143] and thus it is not "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[144] This reading of the text undermines the privacy-protective purpose of the statute. First, as the Commission has previously held, information that the provider causes to be generated by a customer's device or appended to a customer's traffic, in order to allow the provider to collect, access, or use that information, can qualify as CPNI if it falls within one of the statutory categories.[145] Second, while the provider generates and assigns the number that will become the customer's IP address, that number is ultimately just a proxy for the customer, translated into a language that Internet Protocol understands. But for the carrier-customer relationship, the customer would not have an IP address. Other commenters argue that IP addresses should not qualify as CPNI because "this information is necessarily sent onto the open Internet in order to make the service work."[146] However, as discussed above, whether information is available to third parties does not affect whether it meets the statutory definition of CPNI.[147]

71. We also disagree with commenters who assert that dynamic IP addresses[148] do not meet the statutory definition of CPNI. As Return Path explains, "[w]hile the BIAS provider will have a record of precisely which user was connected to [a dynamic] IP address at a specific point in time, any third party will not."[149] A dynamic IP address may be used for a shorter period of time than a static IP address.[150] But a dynamic IP address still meets the statutory definition of CPNI because it relates to the technical configuration, type, destination, and/or location of use of a telecommunications service, for the reasons discussed above.

72. We also conclude that information about the domain names visited by a customer constitute CPNI in the broadband context. Domain names (e.g., ""fcc.gov") are common monikers that the *13937 customer uses to identify the end point to which they seek to connect.[151] Domain names also translate directly into IP addresses. Because of this easy translation, domain names relate to the destination and technical configuration of a telecommunications service.

73. As discussed above, Internet traffic is communicated through a layered architecture, including a network layer that uses protocol headers containing IP addresses to route communications to the intended devices.[152] Similar to IP addresses, other information in the network layer protocol headers is CPNI in the broadband context. BIAS providers configure their networks to use this information for routing, network management, and security purposes. These headers will also indicate the total size of the packet.[153] As such, other information in the network layer protocol headers relates to the technical configuration and amount of use of a telecommunications service.[154]

**21 74. *Traffic Statistics*. We conclude that traffic statistics meet the statutory definition of CPNI in the broadband context because they relate to the amount of use, destination, and type of a telecommunications service.[155] We use the technology-neutral term "traffic statistics" to encompass any quantification of the communications traffic, including short-term measurements (e.g., packet sizes and spacing) and long-term measurements (e.g., monthly data consumption, average speed, or frequency of contact

with particular domains and IP addresses).[156] We believe that traffic statistics are analogous to call detail information regarding the "duration[[] and timing of [phone] calls" and aggregate minutes used in the voice telephony context, both of which are CPNI.[157] BIAS providers use traffic statistics to optimize the efficiency of their networks and protect against cyber threats, but can also use this data to draw inferences that implicate the amount of use, destination, and type of a telecommunications service. For example, BIAS providers can use traffic statistics to determine the amount of use (e.g., date, time, and duration), and to identify patterns such as when the customer is at home, at work, or elsewhere, or reveal other highly personal information. Traffic statistics related to browsing history and other usage can reveal the "destination" of customer communications. Further, a BIAS provider could deduce the "type" of application (e.g., VoIP or web browsing) that a customer is using based on traffic patterns, and thus the purpose of the communication.

75. *Port Information*. We conclude that port information is CPNI in the broadband context because it relates to the destination, type, and technical configuration, of a telecommunications service.[158] A port is a logical endpoint of communication with the sender or receiver's application, and consequently ***13938** relates to the "destination" of a communication.[159] The transport layer protocol header of a data packet contains the destination port number, which determines which application receives the communication.[160] Port numbers identify or at least provide a strong indication of the type of application used, and thus the purpose of the communication, such as email, web browsing, or other activities.[161] BIAS providers configure their networks using port information for network management purposes, such as to block certain ports to ensure network security. As such, these practices relate to the "technical configuration" of the telecommunications service. We agree with commenters that other transport layer protocol header information is CPNI in the broadband context because it relates to the technical configuration and amount of use of a telecommunications service.[162] BIAS providers use other header information in this layer to configure their networks and monitor for security threats. For example, because UDP headers indicate packet size, they can reveal the amount of data the customer is consuming, and because TCP headers include sequence numbers, they can reveal information about a customer's device configuration.[163]

****22** 76. *Application Header*. We conclude that application header information is CPNI in the broadband context because it relates to the destination, type, technical configuration, and amount of use of a telecommunications service.[164] As discussed above, the top-most layer of network architecture is the application layer; IP data packets contain application headers to instruct the recipient application on how to process the communication.[165] Application headers contain data for application-specific protocols to help request and convey application-specific content.[166] The application header communicates ***13939** information between the application on the end user's device and the corresponding application at the other endpoint of the communication.[167] For example, application headers for web browsing typically use the Hypertext Transfer Protocol (HTTP) and contain the Uniform Record Locator (URL), operating system, and web browser; application headers for email typically contain the source and destination email addresses.[168] The type of applications used, the URLs requested, and the email destination all convey information intended for use by the edge provider to render its service. Application headers can also reveal information about the amount of data being conveyed in the packet.[169] BIAS providers may configure their networks using application headers for network management or security purposes.

77. Consistent with our decision in the *2013 CPNI Declaratory Ruling*, we agree with commenters[170] that any information that the BIAS provider injects into the application header, such as a unique identifier header (UIDH), is also CPNI in the broadband context.[171] BIAS providers sometimes append information to application headers, in particular HTTP headers, in order to uniquely tag communications with a specific subscriber account.[172] Like other application header information, these data relate to the technical configuration, type, destination, and amount of use of a telecommunications service.

78. *Application Usage*. We conclude that information detailing the customer's use of applications is CPNI in the broadband context because it relates to the type and destination of a telecommunications service.[173] Unlike an application payload, which

contains the substance of a communication in an IP packet, application usage information is data that reveals the customer's use of an application more generally. A BIAS provider often collects application usage information through its provision of service.[174] Sometimes application usage information is quantified—similar to traffic statistics— into short-term or long-term measurements. Such information can reveal the type of applications the customer uses and with whom she communicates. As such, to the extent that the BIAS ***13940** provider directs the collection or storage of such information, we conclude that it is CPNI.[175] For the reasons discussed above, we disagree with commenters who contend that we should not consider such information to be CPNI because it is also available to other parties.[176]

****23** 79. *Application Payload*. We conclude that the application payload, which is the part of the IP packet containing the substance of the communication between the customer and entity with which the customer is communicating, can be considered CPNI.[177] Examples of application payloads include the body of a webpage, the text of an email or instant message, the video shared by a streaming service, the audiovisual stream in a video chat, or the maps served by a ride-sharing app. It is available to the carrier only because of the customer-carrier relationship and can relate to technical configuration, type, destination and amount of the use of the telecommunications service. BIAS providers are technically capable of configuring their networks to scan all parts of the data packet, including the payload, to detect security threats and block malicious packets.[178] The application payload can help identify the parties to the communication (e.g., the online streaming video distributor of a streaming video, or the homepage of a news website), and thus the communication's destination. The payload's size and substance can also indicate the amount of data the customer is using, the type of communication, and the duration of the use of the service. Another way to think of the application payload is as the "content of the communication." Because of the importance given to protecting content of communications in our legal system, we also discuss content separately as its own element of customer proprietary information.[179]

80. *Customer Premises Equipment (CPE) and other Customer Device Information*. Information pertaining to customer premises equipment (CPE) and other customer device information, such as that relating to mobile stations, is CPNI in the broadband context because it relates to the technical configuration, type, and destination of a telecommunications service.[180] The Act defines CPE as "equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications."[181] The Commission has long-understood CPE to include customers' mobile devices, such as cell phones.[182] Given this precedent, we believe that other consumer devices capable of being connected to broadband services, such as smartphones and tablets, also fall under the rubric of CPE, along with more traditional CPE such as a customer's computer, modem, router, videophone, or IP caption phone. However, we also observe that such devices would be considered "mobile stations," which the Act defines as "a radio-communication station capable of being moved and which ordinarily does move."[183] We disagree with commenters that argue that only devices furnished by the BIAS provider can qualify as CPE;[184] there is no such limitation in the statutory language.

81. We find that the traits of CPE and other customer devices (e.g., model, operating system, software, and/or settings) a customer uses relates to the technical configuration and communications ***13941** protocols the BIAS provider uses to interface that device with its network, as well as the type of service to which the customer subscribes (e.g., fixed or mobile, cable or fiber). CPE and mobile station information relates to the destination of the use of BIAS because it can identify the endpoint for inbound communications.

****24** 82. We disagree with commenters who argue that we should not consider CPE and by extension other customer device information to be CPNI because CPE and other customer devices are also used for purposes other than BIAS, or because such information may be available to other parties.[185] As discussed above,[186] what matters is the nature of the information made available to the BIAS provider through its provision of service.

83. We disagree with NTCA, which misinterprets the Bureau-level *1998 CPNI Clarification Order* to argue that the Commission has previously found that CPE is not covered by Section 222.[187] In the *1998 CPNI Clarification Order*, the Bureau addressed the issue of "customer information independently derived from the carrier's prior sale of CPE to the customer or the customer's subscription to a particular information service offered by the carrier in its marketing of new CPE[.]"[188] By contrast, here we are addressing information about the CPE itself that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, i.e., information derived in the course of providing BIAS or another telecommunications service.

84. *Other Types of CPNI*. We reiterate that the examples of CPNI discussed above are illustrative, not exhaustive. To the extent that other types of information satisfy the statutory definition of CPNI, those data may also be CPNI, either in the BIAS context or in the context of other telecommunications services.

b. Customer Proprietary Information (Customer PI)

85. Section 222(a) imposes a general duty on all telecommunications carriers "to protect the confidentiality of proprietary information of, and relating to, ... customers."[189] "[P]roprietary information of, and relating to, ... customers" is information that BIAS providers and other telecommunications carriers acquire in connection with their provision of service, which customers have an interest in protecting from disclosure.[190] We call this information "customer proprietary information" or "customer PI." Customer PI consists of three non-mutually-exclusive categories: (1) individually identifiable customer proprietary network information (CPNI), (2) personally identifiable information (PII), and (3) content of communications.[191] This interpretation of Section 222(a) is consistent with other provisions of the Communications Act that use the term "proprietary information,"[192] and with the ***13942** Commission's use of that term before enactment of Section 222.[193] As we discuss in more detail below, protecting PII and content is at the heart of most privacy regimes[194] and we recognized in *TerraCom* that the Communications Act protects them as customer PI because it "clearly encompasses private information that customers have an interest in protecting from public exposure."[195]

****25** 86. As we previously explained, "[i]n the context of Section 222, it is clear that Congress used the term 'proprietary information' broadly to encompass all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy.[196] We reaffirm our conclusion that "proprietary information' in Section 222(a), as applied to customers ... clearly encompass[es] private information that customers have an interest in protecting from public exposure."[197] As such, we disagree with commenters that argue that the word "proprietary" in Section 222(a) means the statute only protects information the customer keeps secret from any other party.[198] If only secret information qualified as private information, then not even Social Security numbers would be "proprietary" and subject to the protections of Section 222 and our implementing rules.[199] People regularly give their Social Security numbers to banks, doctors, utility companies, telecommunications carriers, employers, schools, and other parties in order to obtain various services — but this does not mean the information is not ""proprietary" to them. To define "proprietary" as these commenters propose would render Section 222(a) at worst meaningless and at best leaving a gap whereby sensitive proprietary information like a Social Security number would be unprotected.[200]

87. We disagree with commenters that assert that defining the category of customer PI in this way would dramatically expand the scope of providers' duties to protect private customer ***13943** information.[201] Based on the record before us, we find that BIAS providers—like other telecommunications carriers—are already on notice that they have a duty to keep such information secure and confidential based on, among other things, FTC guidance that applied to them prior to the reclassification of broadband in the *2015 Open Internet Order*.[202] According to FTC staff, "[t]o date, the FTC has brought over 500 cases protecting the privacy and security of consumer information."[203] We have held providers responsible for protecting these private data under Section 222(a).[204] In *TerraCom*, we also found that the failure to protect customer's private information was an unjust and

unreasonable practice under Section 201(b).[205] Likewise, providers have been required to protect the content of communications for decades.[206] Moreover, customers reasonably expect and want their providers to keep these data secure and confidential.[207] Surveys reflect that 74 percent of Americans believe it is "very important" to be in control over their own information; as a Pew study found, "[i]f the traditional American view of privacy is the 'right to be left alone,' the 21st-century refinement of that idea is the right to control their identity and information."[208] We agree with the Center for Democracy & Technology that "[e]xcluding PII from the proposed rules would be contrary to decades of U.S. privacy regulation and public policy."[209] We also observe that omitting PII from the scope of these rules would ***13944** result in a gap in protection for PII under the Act's primary privacy regime for telecommunications services.[210] Thus, were PII not included within the scope of customer PI, sensitive PII like Social Security numbers or private medical records would receive fewer protections than a broadband plan's monthly data allowance, a result we do not think intended by Congress. We discuss and define PII below.

c. Personally Identifiable Information (PII)

****26** 88. Protecting personally identifiable information is at the heart of most privacy regimes.[211] Historically, legal definitions of PII have varied. Some incorporated checklists of specific types of information; others deferred to auditing controls. Privacy protections must evolve and improve as technology—and our understanding of its potential—evolves and improves.[212] Our definition incorporates this modern understanding of data privacy and tracks the FTC, the Administration's proposed CPBR, and National Institute of Standards and Technology (NIST) guidelines on PII.[213]

89. We define personally identifiable information, or PII, as any information that is linked or reasonably linkable to an individual or device.[214] Information is linked or reasonably linkable to an individual or device if it can reasonably be used on its own, in context, or in combination to identify an individual or device, or to logically associate with other information about a specific individual or device.[215] The "linked or reasonably linkable" standard for determining the metes and bounds of personally identifiable information is well established and finds strong support in the record.[216] In addition to NIST, CPBR, and the FTC, the Department of Education, the Securities and Exchange ***13945** Commission, the Department of Defense, the Department of Homeland Security, the Department of Health and Human Services, and the Office of Management and Budget all use a version of this standard in their regulations and policies.[217]

90. We agree with the FTC staff that "[w]hile almost any piece of data *could* be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology."[218] While we recognize that "'[i]dentifiable' information is increasingly contextual"[219] — especially when a provider can cross-reference multiple types and sources of information—anchoring the standard to a mere "possibility of logical association"[220] could result in "an overly-expansive definition."[221] Thus, we adopt the recommendation of the FTC staff and others to add the term ""reasonably" to our proposed "linked or linkable" definition of PII.[222] This conclusion has broad support in the record.[223]

91. We also adopt the FTC staff recommendation that PII should include information that is linked or reasonably linkable to a customer device.[224] We agree with the FTC staff that "[a]s consumer devices become more personal and associated with individual users, the distinction between a device and its user continues to blur."[225] The Digital Advertising Alliance likewise recognizes the connection between individuals and devices, stating in its guidance that information "connected to or associated with a particular computer or device" is identifiable.[226] While some commenters argue that we should not include information linkable to a device in the definition of PII,[227] we find that such identifiers are often and easily linkable to an individual, as we discussed above.[228]

**27 *13946 92. We disagree with commenters that argue that PII should only include information that is sensitive or capable of causing harm if disclosed.[229] The ability of information to identify an individual defines the scope of PII. Whether or not any particular PII is sensitive or capable of causing harm if disclosed is a separate question from the definitional question of identifiability.[230] We address the treatment of sensitive versus non-sensitive information below.[231]

93. We agree with commenters that we should offer illustrative, non-exhaustive examples of PII.[232] We have analyzed descriptions of PII in the record, our prior orders,[233] NIST,[234] the FTC,[235] the Administration's proposed CPBR,[236] and other federal and state statutes and regulations.[237] We find that examples of PII include, but are not limited to: name; Social Security number; date of birth; mother's maiden name; government-issued identifiers (e.g., driver's license number); physical address; email address or other online contact information;[238] phone numbers; MAC addresses or other unique device identifiers; IP addresses; and persistent online or unique advertising identifiers. Several of these data elements may also be CPNI.

94. We disagree with commenters that argue that we should not consider MAC addresses, IP addresses, or device identifiers to be PII.[239] First, as discussed above,[240] a customer's IP address and *13947 MAC address each identify a discrete customer and/or customer device by routing communications to a specific endpoint linked to the customer. Information does not need to reveal an individual's name to be linked or reasonably linkable to that person. A unique number designating a discrete individual —such as a Social Security number or persistent identifier—is at least as specific as a name.[241] Second, MAC addresses, IP addresses, and other examples of PII do not need to be able to identify an individual in a vacuum to be linked or reasonably linkable. BIAS providers can combine this information with other information to identify an individual (e.g., the BIAS provider's records of which IP addresses were assigned to which customers, or traffic statistics linking MAC addresses with other data).[242] As the Supreme Court has observed, "[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context."[243]

95. *Customer Contact Information — Names, Addresses, and Phone Numbers of Individuals*. Names, addresses, telephone numbers, and other information that is used to contact an individual are classic PII because they are linked or reasonably linkable to an individual or device.[244] Some commenters argue that contact information is not protected under Section 222 because "Subscriber list information" is exempt from the choice requirements for CPNI under Section 222(e). However, subscriber list information, a relatively small subset of customer contact information, was subject to other considerations at the time of enactment.

**28 96. Subscriber list information is defined in the statute as "any information (A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format."[245] Through this definition, Congress recognized that a dispositive factor is whether the information has been published or accepted for publication in a directory format.

*13948 97. The legislative history shows that Congress created a narrow carve out from the definition of CPNI for subscriber list information in order to protect the longstanding practice of publishing telephone books and to promote competition in telephone book publishing.[246] The legislative history is clear that Congress did not intend for subscriber list information " to include any information identifying subscribers that is prepared or distributed within a company or between affiliates or that is provided to any person in a non-public manner."[247] Instead, Congress intended subscriber list information to be "data that local exchange carriers traditionally and routinely make public. Subscribers have little expectation of privacy in this information because, by agreeing to be listed, they have declined the opportunity to limit its disclosure."[248] Based on this legislative history, we find that the phrase "published, caused to be published, or accepted for publication in any directory format" is best read as

limited to publicly available telephone books of the type that were published when Congress enacted the statute, or their direct equivalent in another medium, such as a website republishing the contents of a publicly available telephone book.

98. Unlike landline voice carriers, neither mobile voice carriers nor broadband providers publish publicly-available directories of customer information.[249] Nor does the record reflect more than speculation about any future interest in publishing directories.[250] Because publishing of broadband customer directories is neither a common nor a long-standing practice, we find that broadband customers have no expectation that that they are consenting to the public release of their name, postal address, or telephone number when they subscribe to BIAS.[251] We therefore conclude that a directory of BIAS customers' names, addresses, and phone numbers would not constitute information published in a "directory format" within the meaning of the statute, and therefore there is no "subscriber list information" in the broadband context.[252] As such, we disagree with commenters who ask us to ignore ***13949** the publication requirement in order to exempt names, addresses, telephone numbers, and IP addresses from these rules.[253]

****29** 99. We recognize that the Commission has previously found that names, addresses, and telephone numbers are not CPNI, even when not published as subscriber list information.[254] However, the Commission has not analyzed whether such customer contact information is PII, and therefore subject to protections under Section 222(a). As discussed above, we make clear today that it is PII.[255]

100. *Harmonization*. We agree with the American Cable Association and various small providers who urge us to harmonize our BIAS and voice definitions under Section 222.[256] Having one uniform set of definitions will simplify compliance and reduce consumer confusion. This is especially true for small providers who collect less customer information, use it for narrower purposes, and do not have the resources to maintain a bifurcated system. Consequently, we extend this definition of PII to all Section 222 contexts.

d. Content of Communications

101. We find that the Act protects the content of communications as customer PI. Content is a quintessential example of a type of "information that should not be exposed widely to the public ... [and] that customers expect their carriers to keep private."[257] Content is highly individualistic, private, and sensitive.[258] Except in limited circumstances where savvy customers deploy protective tools, BIAS providers often have access to at least some, if not most, content through their provision of service.[259] We agree with FTC staff that "[c]ontent data can be highly personalized and granular, allowing analyses that ***13950** would not be possible with less rich data sets."[260] In recognition of its importance, Congress has repeatedly and emphatically protected the privacy of communications content in various legal contexts, expressly prohibiting service providers from disclosing the contents of communications they carry, subject to statutorily enumerated exceptions, since at least 1912.[261] We agree with commenters that "Americans do not expect their broadband providers to be reading their electronic communications any more than they expect them to be keeping a list of their correspondents."[262] The same rationale that supports the treatment of the content of BIAS communications as customer PI supports the treatment of the content carried through other telecommunications services as customer PI.

102. *Definition of Content*. At the outset, we define content as any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication. We sought comment on how to define content in the *NPRM*, but received no substantive recommendations; consequently we base our definition on the long-established terminology of ECPA and Section 705.[263] We recognize that sophisticated monitoring techniques have blurred the line between content and metadata, with metadata increasingly being used to make valuable determinations about users previously only possible with content.[264] This has complicated traditional notions of how to define and treat content. We intend our definition to be flexible enough to encompass any element of the BIAS communication that

conveys or implies any part of its substance, purport, or meaning. As a definitional matter, content in an inbound communication is no different from content in an outbound communication. As discussed above, because the categories of customer PI are not mutually exclusive, some content may also satisfy the definitions of CPNI and/or PII.[265]

****30** 103. Multiple components of an IP data packet may constitute or contain BIAS content.[266] First and foremost, we agree with commenters that the application payload is always content.[267] As ***13951** discussed above,[268] the application payload is the part of the IP packet containing the substance of the communication between the customer and the entity with which she is communicating.[269] Examples of application payloads include the body of a webpage, the text of an email or instant message, the video served by a streaming service, the audiovisual stream in a video chat, or the maps served by a ride-sharing app.[270] However, other portions of the packet also may contain content.[271] For example, as discussed above, the application header may reveal aspects of the application payload from which the content may be easily inferred—such as source and destination email addresses or website URLs.[272] Application usage information may also reveal content by disclosing the applications customers use or the substance of how they use them.[273] We agree with FTC Staff that BIAS content includes, but is not limited to, the "contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read, [and] movies watched[[.]"[274] We emphasize that our examples of BIAS content are not exhaustive and others may manifest over time as analytical techniques improve.

104. We reject arguments that protecting BIAS content under Section 222 is unnecessary or unlawful because Section 705 of the Act,[275] and the Electronic Communications Privacy Act (ECPA)[276] or the Communications Assistance for Law Enforcement Act (CALEA),[277] already protect content.[278] Commenters do not claim that these various other laws are mutually exclusive with each other, belying the notion that the existence of multiple sources of authority in this area is inherently a problem. Instead, we find that Section 222 complements these other laws in establishing a framework for protecting the ***13952** content carried by telecommunications carriers.[279] Given the importance of protecting content, it is reasonable to interpret Section 222 as creating additional, complementary protection.[280]

105. We also disagree with the argument that because the data protected by Section 705 "bear scant resemblance" to content or other forms of customer PI, our interpretation of Section 222 is erroneous.[281] Congress can enact two statutory provisions that contain different scopes, and it is a cardinal principle of statutory construction that we should attempt to give meaning to both. Any incongruity between the scope of Sections 222 and 705 only demonstrates that the statutes are complementary and part of Congress's broad scheme to protect customer privacy. Sections 222 and 705 independently require telecommunications carriers to protect communications content.

4. De-identified Data

****31** 106. In this section we describe a corollary regarding the circumstances in which information that constituted customer PI (*i.e.*, PII, content, or individually identifiable CPNI) can comfortably be said to have been de-identified. As discussed below, based on the record we are concerned that carriers not be allowed to skirt the protections of our rules by making unsupported assertions that customer PI has been "de-identified" and thus is not subject to our consent regime, when in fact the information remains reasonably linkable to an individual or device. As 38 public interest organizations pointed out in a joint letter, "[i]t is often trivial to re-identify data that has supposedly been de-identified."[282] We accordingly adopt a strong, multi-part approach regarding the circumstances under which carriers can properly consider data to be de-identified, using the three part test for de-identification articulated by the FTC in 2012.[283] The Administration's CPBR also uses this standard.[284] Specifically, we find that customer proprietary information is de-identified if the carrier (1) determines that the information is not reasonably linkable to an individual or device; (2) publicly commits to maintain and use the data in a non-individually identifiable fashion and to not attempt to re-identify the data; and (3) contractually prohibits any entity to which it discloses or permits access

to the de-identified data from attempting to re-identify the data.[285] We apply these requirements to both BIAS and other telecommunications services.[286]

***13953 a. Adoption of the FTC's Multi-Part Test**

107. The record reflects that advances in technology and data analytics make it increasingly difficult to de-identify information such that it is not re-identifiable.[287] The Administration's 2014 Big Data Report observed that "[m]any technologists are of the view that de-identification of data as a means of protecting individual privacy is, at best, a limited proposition."[288] As the Electronic Privacy Information Center notes, "[w]idely-publicized anonymization failures have shown that even relatively sophisticated techniques have still permitted researchers to identify particular individuals in large data sets."[289] We also agree with the FTC's conclusion in its 2012 Privacy Report that "not only is it possible to re-identify non-PII data through various means, businesses have strong incentives to actually do so."[290]

108. For these reasons, our approach to de-identification establishes a strong, technology-neutral standard as well as safeguards to mitigate the incentives to re-identify customers' proprietary information. Furthermore, because companies, including BIAS providers, have incentives to re-identify customer information so that it can be further monetized,[291] we agree with Privacy Rights Clearinghouse that the burden of proving that individual customer identities and characteristics have been removed from the data must rest with the provider.[292] Taking this burden assignment into account, we find that our multi-part approach, grounded in FTC guidance, will ensure that as technology changes, customer information is protected, while at the same time minimizing burdens and maintaining the utility of de-identified customer information.

****32 *13954** 109. As such, we disagree with those commenters who urge us to use a different de-identification framework, such as that used in the HIPAA safe harbor context.[293] We find that the framework we adopt enables flexibility to accommodate evolving technology and statistical methods. In contrast, we find that developing a list of identifiers that must be removed from data to render such data de-identified is not feasible given the breadth of data to which BIAS providers have access, and would also rapidly become obsolete in the evolving broadband context.

110. The three-part test we adopt today for de-identification also contemplates the statutory exception for "aggregate customer information," as it defines the circumstances in which the Commission will find that "individual customer identities and characteristics have been removed" from collective data.[294] Likewise, our approach addresses arguments in the record that the Commission must give meaning to the fact that the customer approval requirement of Section 222(c)(1) applies to "individually identifiable" CPNI,[295] as our test for de-identification addresses whether an individual's CPNI or PII will not be deemed to be individually identifiable in practice due to steps taken by the carrier prior to using or sharing the data.

(i) Part One — Not Reasonably Linkable

111. First, for information to be de-identified under our rules, we require providers to determine that the information is not linked or reasonably linkable to an individual or device.[296] Because we are describing the scope of what is identifiable, we think it is appropriate to use the same standard that we use to define personally identifiable information (PII).[297] Above we define PII as information that is linked or reasonably linkable to an individual or device, and conversely we find it appropriate to limit de-identified information to information that is *not* linked or reasonably linkable to an individual or device. As we discussed above in our definition of PII, we agree with commenters that the "linked or reasonably linkable" standard—used by the FTC in its Privacy Report—provides useful guidance on what it means for information to be individually identifiable without being either overly rigid or vague.[298] As we discussed above, information is linked or reasonably linkable to an individual or device if it can reasonably be used on its own, in context, or in combination (1) to identify an individual or device, or (2) to logically associate with other information about a specific individual or device.[299] New methods are increasingly capable

of re-identifying information previously thought to be sufficiently anonymized.[300] For these reasons, we will not specify an exhaustive list of identifiers, nor will we declare certain ***13955** techniques to be *per se* sufficient or insufficient to achieve de-identification.[301] The test instead focuses on the outcome required, that is, that to be de-identified, the data must no longer be linked or reasonably linkable to an individual or device. We also agree with AT&T that we should not "dictate specific approaches to de-identifying data" because "[a]ny Commission-mandated approach would quickly become obsolete as new de-identification techniques are developed."[302]

****33** 112. We make clear that reasonableness depends on ease of *re*-identification, not the cost of *de*-identification.[303] As discussed above, customers' privacy interests include many noncommercial values, such as avoidance of embarrassment, concern for one's reputation, and control over the context of disclosure of one's information.[304] The decisive question here is not how difficult it is to de-identify the information, but rather the ease with which the information could be re-identified.[305] The FTC's linkability standard aligns with our approach: "[W]hat qualifies as a reasonable level of [de-identification] depends upon the particular circumstances, including the available methods and technologies. In addition, the nature of the data at issue and the purposes for which it will be used are also relevant."[306]

113. Consistent with the FTC's guidance and the carrier's burden to prove that information is in fact de-identified, if carriers choose to maintain customer PI in both identifiable and de-identified formats, they must silo the data so that one dataset is not reasonably linkable to the other.[307] Cross-referencing the datasets links the de-identified information with an identified customer, thus rendering the de-identified information linked or reasonably linkable.[308] We agree with Verizon that "providers should not be allowed to use de-identification and re-identification to circumvent consumers' privacy choices."[309]

114. We disagree with commenters who argue that the linkability standard should apply only to individuals and should not extend to devices.[310] As explained above, we agree with the FTC staff that "[a]s consumer devices become more personal and associated with individual users, the distinction between a device and its user continues to blur."[311] This is not an uncommon conclusion in the Internet ***13956** ecosystem; the Digital Advertising Alliance also recognizes the connection between individuals and devices in its definition of de-identification, stating that "[d]ata has been De-Identified when ... the data cannot reasonably ... be connected to or associated with a particular computer or device."[312]

115. Similarly, for the reasons discussed above,[313] we disagree with commenters who argue that IP addresses and MAC addresses should not be considered reasonably linkable to an individual or device on the theory that "[t]hey only identify Internet endpoints, each of which, in turn, may reach multiple people or devices."[314] The question in this test is whether the information in question is reasonably linkable to an individual or device. Consider, for example, a typical fixed residential customer. The BIAS provider assigns that customer an IP address, and associates that customer with that IP address in its records. It is difficult to portray that scenario as not involving PII. On the other hand, if the BIAS provider shares the IP address with a third party without other identifying information, it may well be the case that the provider has not shared information that is "reasonably linkable" to an individual or device. Again, when confronted with the question, the Commission will look at all facts available and make a pragmatic determination of whether the information in question is "reasonably linkable" to an individual or device.[315]

(ii) Part Two — Public Commitments

****34** 116. Second, for information to meet our definition of de-identified, carriers must publicly commit to maintain and use de-identified information in a de-identified fashion and to not attempt to re-identify the data. Such public commitments inform customers of their legal rights and the provider's practices, and "promot[e] accountability."[316] As we discussed above, this level of transparency is a cornerstone of privacy best practices generally and these rules specifically.[317] As such, we disagree with commenters who argue that such public commitments are unnecessary.[318] This part of the test is consistent

with FTC guidance[319] —which has broad support in the record[320] —and the CPBR.[321] We agree ***13957** that "[c]ompanies that can demonstrate that they live up to their privacy commitments have powerful means of maintaining and strengthening consumer trust."[322] Further, we find that this requirement will impose a minimal burden on providers, as a carrier can satisfy this requirement with a statement in its privacy policy.[323]

(iii) Part Three — Contractual Limits on Other Entities

117. Third, for information to meet our definition of de-identified, we require telecommunications carriers to contractually prohibit recipients of de-identified information from attempting to re-identify it. This requirement is consistent with the FTC's de-identification guidelines and the Administration's CPBR, as well as industry best practices.[324]

118. Businesses are often in the best position to control each other's practices. For example, AT&T's Privacy FAQ explains, "When we provide individual anonymous information to businesses, we require that they only use it to compile aggregate reports, and for no other purpose. We also require businesses to agree they will not attempt to identify any person using this information ...."[325] The record demonstrates that such contractual prohibitions are an important part of protecting consumer privacy because re-identification science is rapidly evolving.[326] We agree with Verizon and other commenters that "anyone with whom the provider shares such de-identified data should be prohibited from trying to re-identify it."[327] It is our expectation that carriers will need to monitor their contracts to maintain the carriers' continued adherence to these requirements.[328] Consequently, we need not adopt a separate part of the test to delineate monitoring requirements.[329] Further, we observe that third parties will have every incentive to comply with their contractual obligations to avoid both civil liability and enforcement actions by the FTC or the Commission (depending on the agency with authority over the third party). If ***13958** violations occur, we expect carriers to take steps to protect the confidentiality of customer's proprietary information.[330]

****35** 119. We agree with commenters who recommend a narrow clarification to the third part of the de-identification framework in situations involving disclosure of highly abstract statistical information. These situations include, for example, mass market advertisements or annual reports that reference the total number of subscribers or the percentage of customers at certain speed thresholds.[331] AT&T explains that these scenarios can involve customer information that is so "highly abstract[ed]" that it is, "in many circumstances, simply impossible" to re-identify the data.[332] Professor Narayanan concurs, noting that when statistical data is highly abstract, there is minimal risk of re-identification.[333] We agree. Consequently, we will not require contractual commitments when the de-identified customer information is so highly abstracted that a reasonable data science expert would not consider it possible to re-identify it.

120. A number of commenters also ask for a narrow exception to this part of the de-identification test for the purposes of various types of cybersecurity or de-identification research.[334] As explained below, we find that certain uses and disclosures of customer PI for the purpose of conducting research to improve and protect[335] networks and/or services are part of the telecommunications service or "necessary to, or used in" the provision of the telecommunications service for the purposes of these rules.[336]

(iv) Case-by-case application

121. In adopting a technology-neutral standard to determine whether otherwise personally identifiable customer PI has been de-identified, we have eschewed an approach that finds particular techniques to be *per se* acceptable or unacceptable.[337] That said, by adopting the three-part test, we have made clear that a carrier cannot "make an end-run around privacy rules simply by removing certain identifiers from data, while leaving vast swaths of customer details largely intact."[338] As Professor Ohm ***13959** has stated, the FTC guidance on which we pattern our standard is "a very aggressive and appropriately strong form of de-identification"[339] and it is one that requires strong technological protections as well as business processes in its

implementation. The Commission will carefully monitor carriers' practices in this area. We emphasize that carriers relying on de-identification for use and sharing of customer proprietary information should employ well-accepted, technological best practices in order to meet the three-part test described above — and employ practices that keep pace with evolving technology and privacy science.[340]

C. Providing Meaningful Notice of Privacy Policies

122. In this section, we adopt privacy policy notice requirements for providers of broadband Internet access services and other telecommunications services. There is broad recognition of the importance of transparency as one of the core fair information practice principles (FIPPs),[341] and it is an essential component of many privacy laws and regulations, including the Satellite and Cable Privacy Acts.[342] Customer notification is also among the least intrusive and most effective measures at our disposal for giving consumers tools to make informed privacy decisions.[343] In fact, it is only possible for customers to give informed consent to the use of their confidential information if telecommunications carriers give their customers easy access to clear and conspicuous, comprehensible, and not misleading information about what customer data the carriers collect; how they use it; who it is shared with and for what purposes; and how customers can exercise their privacy choices.[344] Therefore, we adopt rules to ensure that BIAS providers' and other telecommunications carriers' privacy notices meet these essential criteria, which provide transparency and enable the exercise of choice.

****36** 123. In adopting these transparency requirements, we build on and harmonize our existing Section 222 rules for voice providers[345] with BIAS providers' existing requirement to disclose their ***13960** privacy policy under the 2010 and 2015 *Open Internet Orders*.[346] For today's rules, we look to the record in this proceeding, which includes submissions from providers, consumer advocates, other government agencies,[347] and others about what does and does not work with respect to privacy policies.[348] Based on that record, we adopt rules that require providers to disclose their privacy practices, but decline to be prescriptive about either the format or specific content of privacy policy notices in order to provide flexibility to providers and to minimize the burden of compliance levied by this requirement.[349] In the interest of further minimizing the burden of transparency, particularly for small providers, we also direct the Consumer Advisory Committee to convene a multi-stakeholder process to develop a model privacy policy notice that will serve as a safe harbor for our notice requirements.

124. We recognize that some commenters have criticized privacy notice requirements as providing incomplete protections for consumers. Notices by themselves do not give consumers the power to control their information; notices are not always read or understood, and newer developments in tracking and analytics can reveal more about consumers than most people realize.[350] However, none of these criticisms eliminates the fundamental need for and benefit of privacy notices.[351] If consumers do not have access to the information they need to understand what personal data is being collected and how their data is being used and shared, they cannot make choices about those practices. The fact that poorly written or poorly distributed notices can confound consumer understanding does not make well-formed notices useless, and while one consumer may ignore a notice, another who has a compelling desire to protect her privacy will benefit substantially from it. Notice also remains an essential part of today's privacy frameworks, even as big data analysis creates new privacy challenges. As the recent ***13961** Administration Big Data Report explains, notice and choice structures may not be sufficient to account for all privacy effects of "big data,"[352] but such frameworks are necessary to protect consumers from a range of active privacy threats.

125. Below we lay out the specific transparency requirements we adopt today. First, we require that those privacy notices inform customers about what confidential information the providers collect, how they use it, and under what circumstances they share it. We also require that providers inform their customers about customers' rights to opt in to or out of (as the case may be) the use or sharing of their confidential information. This information must be presented in a way that is clear and conspicuous, in language that is comprehensible and not misleading.[353] Second, we require that providers present their privacy notice to customers at the point of sale prior to the purchase of service, and that they make their privacy policies persistently available and easily

accessible on their websites, apps, and the functional equivalents thereof. Finally, we require providers to give their customers advance notice of material changes to their privacy policies. In adopting these transparency rules, we are implementing, in part, Sections 222(a) and 222(c)(1), under which we find that supplying customers with the information they need to make informed decisions about the use and sharing of their personal information is an element of "informed" approval within the meaning of Section 222, as well as necessary to protecting the confidentiality of customer proprietary information.[354]

1. Required Privacy Disclosures

****37** 126. Customers must have access to information about the personal data that a BIAS provider or other telecommunications carrier collects, uses, and shares, in order to make decisions about whether to do business with that provider, and in order to exercise their own privacy decisions. Absent such notice, the broad range of data that a provider is capable of gathering by virtue of providing service could leave customers with only a vague concept of how their privacy is affected by their service provider.[355] We also agree with the FTC that disclosing this information "provides an important accountability function,"[356] as disclosure of this information "constitute[[s] public commitments regarding companies' data practices."[357] ***13962** To enable customers to exercise informed choice, and to reduce the potential for confusion, misunderstanding, and carrier abuse,[358] we find that a carrier's privacy notices must accurately describe the carrier's privacy policies with regard to its collection, use, and sharing of its customers' data. Therefore, we adopt rules that require each telecommunications carrier's notice of privacy policies to accurately specify and describe:

· The types of customer PI that the carrier collects by virtue of its provision of service, and how the carrier uses that information;

· Under what circumstances a carrier discloses or permits access to each type of customer PI that it collects, including the categories of entities to which the carrier discloses or permits access to customer PI and the purposes for which the customer PI will be used by each category of entities; and

· How customers can exercise their privacy choices.

We address each of these requirements in turn.

127. *Types of Customer PI Collected, and How It Is Used*. In order to make informed decisions about their privacy, customers must first know *what types* of their information their provider collects through the customers' use of the service. Therefore, we require BIAS providers and other telecommunications carriers to specify the types of customer PI that they collect by virtue of provision of the telecommunications service, and how they use that information.[359] Pursuant to the voice rules and the *2010 Open Internet Order*, all BIAS providers already provide customers with information about their privacy policies.[360] As such, we find that this requirement will not impose a significant burden on providers, and in some cases will decrease existing burdens.[361]

128. Likewise, customers have a right to know *how* their information is being used and under what circumstances it is being disclosed in order to make informed privacy choices.[362] Notices that omit these explanations fail to provide the context that customers need to exercise their choices. We emphasize that the notice must be sufficiently detailed to enable a reasonable consumer to make an informed choice

****38** 129. We do not require providers to divulge the inner workings of their data use programs. Instead, we find that to the extent that the notice requires providers to divulge the existence of such programs, the benefits to the market of more complete information, as well as the benefits to customers in knowing how their information is used, outweighs any individual advantage gained by any one competitor in keeping the existence of the programs secret. We therefore disagree with commenters that ***13963** argue that these descriptions of how consumers' information will be used unduly jeopardize their competitive efforts.[363]

130. *Sharing of Customer PI with Affiliates and Third Parties*. We also require that providers' privacy policies notify customers about the types of affiliates and third parties with which they share customer information, and the purposes for which the affiliates and third parties will use that information. A critical part of deciding whether to approve of the sharing of information is knowing *who* is receiving that information and for what purposes.[364] This information will allow customers to gauge their comfort with the privacy practices and incentives of those other entities, whether they are affiliates or third parties. It will also promote customer confidence in their telecommunications service by providing concrete information and reducing uncertainty as to how their information is being used by the various parties in the data-sharing and marketing ecosystems. While our existing CPNI rules are more specific in requiring that individual entities be disclosed,[365] we seek to minimize customer confusion and provider burden by adopting an approach used by the FTC by allowing disclosure of categories of entities. We also encourage carriers to make these categories of entities as useful and understandable to customers as possible. By way of example, the FTC's regulations implementing the GLBA privacy rules will find a covered institution in compliance with its rules if it lists particular categories of third party entities that it shares information with, distinguishing, for instance, between financial services providers, other companies, and other entities.[366] The FTC's rules further specify that institutions should provide examples of businesses in those categories.[367] In the context of communications customers' information, relevant categories might include providers of communications and communications-related services, customer-facing sellers of other goods and services, marketing and advertising companies, research and development, and nonprofit organizations.

131. We find that requiring providers to disclose categories of entities with which they share customer information and the purposes for which the customer PI will be used by each category of entities balances customers' rights to meaningful transparency with the reality of changing circumstances and the need to avoid overlong or over-frequent notifications.[368] We therefore reject calls to mandate disclosure of a list of the specific entities that receive customer PI.[369] While some customers may benefit from receiving such detailed information, we are persuaded by commenters who assert that requiring such granularity would be unduly burdensome on carriers and induce notice fatigue in many customers. For instance, carriers would be faced with the near-continuous need to provide new notices every time contracts with particular vendors change or if third parties alter their corporate structure—and customers, ***13964** in turn, would be inconvenienced with an overabundance of notices.[370] Furthermore, a list of specific entities may not in itself aid the average consumer in making a privacy decision more than the requirement that we adopt, which ensures that consumers understand what third parties that receive their information do as a general matter. We therefore adopt the requirement that carriers need only provide categories of entities with whom customer PI is shared, minimizing the burden on telecommunications carriers. If a provider finds that providing notice of the specific entities with which it shares customer PI would increase customer confidence, nothing prevents a provider from doing so, and we would encourage notices to include as much useful information to customers as possible, while maintaining their clarity, concision, and comprehensibility, as discussed in Part III.C.3, below.[371] Doing so does not require bombarding customers with pages of dense legal language; providers may make use of layered privacy notices or other techniques to ease comprehension and readability as necessary.[372]

****39** 132. *Customers' Rights with Respect to Their PI*. We also adopt our *NPRM* proposal to require BIAS provider and other telecommunications carrier privacy notices to provide certain minimum information. Carriers need not, however, repeat any of these "rights" statements verbatim, and we encourage carriers to adapt these statements in manners that will be most effective based on their extensive experience with their customer base. Specifically, carriers' privacy notices must:

· Specify and describe customers' opt-in and opt-out rights with respect to their own PI. This includes explaining that:

· a denial of approval to use, disclose, or permit access to customer PI for purposes other than providing telecommunications service will not affect the provision of the telecommunications services of which they are a customer.

· any approval, denial, or withdrawal of approval for use of the customer PI for any purposes other than providing telecommunications service is valid until the customer affirmatively revokes such approval or denial, and that the customer has

the right to deny or withdraw access to such PI at any time. However, the notice should also explain that the carrier may be compelled, or permitted, to disclose a customer's PI when such disclosure is provided for by other laws.

· Provide access to a simple, easy-to-use mechanism for customers to provide or withdraw their consent to use, disclose, or permit access to customer PI as required by these rules.[373]

133. These notice requirements are intended to ensure that providers inform their customers that they have the right to opt into or out of the use and sharing of their information, as well as how to make those choices known to the provider. We discuss the choice mechanism itself in Part III.D.4, *infra*. Requiring providers to describe in a single place how information is collected, used, and shared, as well as what the consumers' rights are to control that collection, use, and sharing, enhances the opportunity for ***13965** customers to make informed decisions.[374] Likewise, requiring the notice to provide access to the choice mechanism ensures that the mechanism is easily available and accessible as soon as the customer receives the necessary privacy information. This is important, since studies have shown that "adding just a 15-second delay between the notice and the loading of [a] webpage where subjects choose whether to reveal their information eliminates the privacy-protective effect of the notice."[375] As discussed further below,[376] we decline to specify particular formats for carriers to provide access to their choice mechanisms, recognizing that different forms of access to the choice mechanism (e.g., a link to a website, a mobile dashboard, or a toll-free number) may be more appropriate depending on the context in which the notice may be given (e.g., on a provider's website, in a provider's app, or in a paper disclosure presented in a provider's store).[377]

****40** 134. Studies have shown that customers are often resigned to an inability to control their information, and may be under a mistaken impression that exercising their rights may result in degraded service.[378] Thus, we require providers' notice of privacy policies to also inform customers that denying a provider the ability to use or share customer PI will not affect their ability to receive service.[379] This parallels the existing Section 222 rules, which require carriers to "clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes."[380] Since providers drafting their notices have clear incentives to encourage customers to permit the use and sharing of customer PI, it can be easy for customers to misconstrue exactly what is conditioned upon their permission.[381] These provisions are intended to make customers aware that the offer of choice is not merely *pro forma*.

135. We permit providers to make clear and neutral statements about potential consequences when customers decline to allow the use or sharing of their personal information. We require that any such statements be clear and neutral in order to prevent them from obscuring the basic fact of the customer's right to prevent the use of her information without loss of service. Allowing difficult-to-read or biased statements would run counter to our goal of ensuring that notices overall are clear and conspicuous, comprehensible, and not misleading.[382] NTCA recommends that we remove or modify from the *NPRM*' s proposal the requirement that the explanation be brief.[383] In the interest of allowing more ***13966** flexibility, we remove this requirement, with the understanding that brevity is often, but not always, a component of clarity.

136. We require providers to inform customers that their privacy choices will remain in effect until the customers change them, and that customers have the right to change them at any time. We acknowledge that "[c]ustomers may make hasty decisions in the moment simply to obtain Internet access ... [and] therefore appreciate the reminder that they have the opportunity to change their mind."[384] We expect carriers' privacy promises to customers and the privacy choices customers make to be honored, including, for example, in connection with a carrier's bankruptcy.[385]

2. Timing and Placement of Notices

137. There is broad agreement that, in order to be useful, privacy policy notices must be clearly, conspicuously, and persistently available, and not overly burdensome to the carrier or fatiguing to the customer.[386] We therefore require telecommunications carriers to provide notices of privacy policies at the point of sale prior to the purchase of service, and also to make them clearly, conspicuously, and persistently available on carriers' websites and via carriers' apps that are used to manage service, if any. We also eliminate periodic notice requirements from the voice CPNI rules.

****41** 138. *Point of Sale*. We agree with commenters that requiring notices at the point of sale ensures that notices are relevant in the context in which they are given,[387] since this is a time when a customer can still decide whether or not to acquire or commit to paying for service, and it also allows customers to exercise their privacy choices when the carrier begins to collect information from them. In this, we agree with the FTC, which finds that the most relevant time is when consumers sign up for service.[388] The proximity in time between sale and use of information means that a point-of-sale notice, in many if not most instances, serves the same function as a just-in-time notice—that of providing information at the most relevant point in time. Consumer groups such as the Center for Digital Democracy and providers such as Sprint also appear to agree on this point.[389] The point-of-sale requirement is also consistent with the transparency requirements of the *2010 Open Internet Order*, which ***13967** requires disclosure of privacy policies at the point of sale.[390] As such, we find that this requirement will impose a minimal incremental burden on BIAS providers. The record further indicates that providing notice at the point of sale can be less burdensome for a carrier, in part because it allows the provider to walk a customer through the terms of the agreement.[391] Providing notice at the point of sale, and not after a customer has committed to a subscription, can also allow carriers to compete on privacy.[392]

139. We clarify that a "point of sale" need not be a physical location. Where the point of sale is over voice communications, we require providers to give customers a means to access the notice, either by directing them to an easily-findable website, or, if the customer lacks Internet access, providing the text of the notice of privacy policies in print or some other way agreed upon by the customer. We find that this requirement adequately addresses record concerns about the burdens associated with communicating polices orally to customers.[393]

140. *Clear, Conspicuous, and Persistent Notice*. We also require telecommunications carriers to make their notices persistently available through a clear and conspicuous link on the carrier's homepage, through the provider's application (if it provides one for account management purposes), and any functional equivalents of the homepage or application.[394] This requirement also reflects the transparency requirements in the *2010 Open Internet Order*, which mandate "at a minimum, the prominent display of disclosures on a publicly available ... website,"[395] and as such, should add a minimal burden for BIAS providers. Persistent and visible availability is critical; customers must be able to review the notice and understand the carrier's privacy practices at any time since they may wish to reevaluate their privacy choices as their use of services change, as their personal circumstances change, or as they evaluate and learn about the programs offered by the provider.[396] Persistent access to the notice of privacy policies also ensures that customers need not rely upon their memory of the notice that they viewed at the point of sale; so long as they have access to the provider's website, app, or equivalent, they can review the notice. As such, we require providers to at least provide a link to the web-hosted notice in ***13968** a clear and conspicuous location on its homepage, to ensure that customers who visit the homepage may easily find it.[397]

****42** 141. We require the notice of privacy policies to be clearly and conspicuously present not only on the provider's website, but to be accessible via any application ("app") supplied to customers by the provider that serves as a means of managing their subscription to the telecommunications service. As more consumers rely upon mobile devices to access online information, a provider's website may become less of a central resource for information about the provider's policies and practices. Certain mobile apps serve much the same function as a mobile website interface, giving customers tools to manage their accounts with their providers.[398] As a significant point of contact with the customer, such apps are an ideal place for customers to be able to find the notice of privacy policies.[399] We do not, however, expect that every app supplied by a provider must carry the notice of privacy policies for the entire service—for instance, a mobile broadband provider that bundles a sports news app or a mobile

game with its phones and services would not need to provide the privacy notice we require here with those apps.[400] Nor do we require providers who lack an app to develop one.[401] However, we require carriers that provide apps that manage a customer's billing or data usage, or otherwise serve as a functional equivalent to a provider's website, to ensure that those apps provide at least a link to a viewable notice of privacy policies.[402]

142. Providing the notice both via the app and on the provider's website increases customers' ability to access and find the policy regardless of their primary point of contact with the provider. We do, however, wish to ensure that customers can still reach notices even as providers may develop other channels of contact with their customers, and thus require that the notice be made available on any functional equivalents of the website or app that may be developed. While we anticipate that all BIAS providers and most other telecommunications providers have a website, those that do not may provide their notices to customers in paper form or some other format agreed upon by the customer.

143. *No Periodic Notice Requirement*. We decline to require periodic notice on an annual or bi-annual basis. While periodic notices might serve to remind customers of their ability to exercise privacy choices,[403] we remain mindful of the potential for notice fatigue and find that notices at the point of sale, supplemented by persistently available notices on providers' websites, and notices of material change to privacy policies,[404] is sufficient to keep customers informed.[405] Additionally, we believe that periodic notices might distract from notices of material changes, reducing the amount of customer ***13969** attention to such changes.[406] We find that annual or periodic notices are unnecessary or even counterproductive in this context, and we reduce burdens on all telecommunications carriers—including smaller carriers—by eliminating the pre-existing every-two-year notice requirement from our Section 222 rules.[407]

3. Form and Format of Privacy Notices

****43** 144. Recognizing the importance of flexibility in finding successful ways to communicate privacy policies to consumers, we decline to adopt any specific form or format for privacy notices. We agree with commenters that, in addition to running the risk of providing insufficient flexibility, mandated standardized requirements may unnecessarily increase burdens on providers, and prevent consumers from benefitting from notices tailored to a specific provider's practices. For example, the record reflects concerns that mandated standardized requirements can increase burdens on providers, and can also create a number of problems, including a lack of flexibility to account for the fact that different carriers may have different needs, such as creating comprehensive policies across different services.[408] This concern is especially prevalent for smaller carriers.[409] At the same time, we agree with commenters that whatever form of privacy notices a provider adopts, in order to adequately inform customers of their privacy rights, such privacy notices must clearly and conspicuously provide information in language that is comprehensible and not misleading, and be provided in the language used by the carrier to transact business with its customer.[410] We therefore require providers to implement these general principles in formatting their privacy policy notices.

145. These basic requirements for the form and format of privacy policies build on existing Commission precedent regarding notice requirements for voice providers and open Internet transparency requirements for BIAS providers, and incorporate FTC guidance on customer notice standards.[411] These basic principles are well suited to accommodating providers' and customers' changing needs as new business models develop or as providers develop and refine new ways to convey complex information to customers.[412] Within these basic guidelines, providers may use any format that conveys the required information, including layering and adopting alternative methods of structuring the notice or highlighting its provisions.[413] We encourage innovative approaches to educating customers about privacy practices and choices.

146. While we decline to mandate a standardized notice at this time, the record demonstrates that voluntary standardization can benefit both customers and providers.[414] As such, as described below, ***13970** we adopt a voluntary safe harbor for a

disclosure format that carriers may use in meeting the rules' standards for being clear and conspicuous, comprehensible, and not misleading.

147. *Clear, Conspicuous, Comprehensible and Not Misleading*. Consistent with existing best practices, we require providers' privacy notices to be readily available and written and formatted in ways that ensure the material information in them is comprehensible and easily understood. The record reflects broad agreement that providers' privacy practices "should be easily available [and] written in a clear way."[415] A number of commenters noted that certain practices frustrate the ability of customers to find and identify the important parts of privacy notices, observing, for example, that notices could be presented among or alongside distracting material, use unclear or obscure language, presented with significant delays in ability for consumers to act, or be placed only at the bottom of "endless scrolling" pages.[416] By mandating that notices be clear, conspicuous, comprehensible, and not misleading, we prohibit such practices and others that render notices unclear, illegible, inaccessible, or needlessly obtuse.[417]

****44** 148. The *NPRM* framed these requirements in several ways, including that notices be "clear and conspicuous," as well as "clearly legible, use sufficiently large type, and be displayed in an area so as to be readily apparent to the consumer."[418] In adopting these rules, we streamline these requirements by interpreting "conspicuous" to include requirements for prominent display, and eliminate the requirement for "sufficiently large type," based upon the understanding that insufficiently large type would not be ""comprehensible" or "clear and conspicuous." Removing this specific requirement also preserves the ability for providers who may be able to convey the necessary information through images or other non-textual means.[419]

149. We agree with the FTC's observation that existing notices of privacy policies are frequently too long and unclear;[420] overlong notices are often inherently less comprehensible.[421] As T-Mobile states, "today's busy consumers often have limited ability to fully review the hundreds of privacy ***13971** policies that apply to the apps, websites, and services they use, and prefer simpler notices that provide meaningful information."[422] We recognize that providers must balance conveying the required information in a comprehensive and comprehensible manner,[423] and therefore encourage, but do not require, providers to make their notices as concise as possible while conveying the necessary information. Layered notices, lauded by a few commenters, may be one of several ways to achieve these parallel objectives.[424]

150. The record also reflects that transparency is only effective in preventing deception when the information shared is meaningful to the recipient.[425] We agree with the California Attorney General that companies should "alert consumers to potentially unexpected data practices," and as such require that providers' notices not be misleading in addition to being comprehensible.[426] This requirement is also consistent with FTC precedent.[427]

151. *Other Languages*. We agree with the FTC that providers should convey notices to their customers in a language that the customers can understand.[428] We therefore require providers to convey their entire notices of privacy policies to customers in another language, if the telecommunications carrier transacts business with the customer in that other language.[429] This requirement ensures that customers who are advertised to in a particular language may also understand their privacy rights in that same language.[430] We conclude that this obligation appropriately balances accommodating customers who primarily use languages other than English and reducing the burden on providers, especially small providers, to translate notices into languages that are unused by their particular customers.[431]

****45** 152. *Mobile-Specific Considerations*. We decline to mandate any additional requirements for notices displayed on mobile devices. The record indicates that providers desire flexibility to adapt notices to be usable in the mobile environment for their customers, while consumer advocates stress that the requirements for usability must be met in some way, regardless of the specific formatting.[432] So long as ***13972** notices on mobile devices meet the above guidelines and convey the necessary

information, they will comply with the rules. Providers are free to experiment within those broad guidelines and the capabilities of mobile display technology to find the best solution for their customers.

153. *Safe Harbor for Standardized Privacy Notices*. To encourage adoption of standardized privacy notices without mandating a particular form, we direct the Consumer Advisory Committee, which is composed of both industry and consumer interests,[433] to formulate a proposed standardized notice format, based on input from a broad range of stakeholders, within six months of the time that its new membership is reconstituted, but, in any event, no later than June 1, 2017. There is strong support in the record for creation of standardized notice, and for use of multi-stakeholder processes.[434] Standardized notices can assist consumers in interpreting privacy policies, and allow them to better compare the privacy policies of different providers, allowing increased competition in privacy protections.[435] Standardized notices can also reduce compliance costs for providers, especially small providers, by ensuring they can easily adopt a compliant form and format for their notices.[436]

154. The CAC has significant expertise in developing standard broadband disclosures and other consumer disclosure issues.[437] We find that the Committee's experience makes it an ideal body to recommend a notice format that will be sufficiently clear and easy to read to allow consumers to easily understand and compare the privacy practices of different providers. To ensure that the notice will be clear and easy to read for all customers, it must also be accessible to persons with disabilities. We delegate authority to the Wireline Competition Bureau, Wireless Telecommunications Bureau, and Consumer & Governmental Affairs Bureau to work with the CAC on the draft standardized notice. If the CAC recommends a form or format that do not meet the Bureaus expectations, the Bureaus may ask the CAC to consider changes and submit a revised proposal for the Bureaus' review within 90 days of the Bureaus' request. The Bureaus may also seek public comment, as they deem appropriate, on any standardized notice the CAC recommends. We also delegate authority to the Bureaus to issue a Public Notice announcing any proposed format or formats that they conclude meet our expectations for the safe harbor for making consumer-facing disclosures.[438]

***13973** 155. Providers that voluntarily adopt a privacy notice format developed by the CAC and approved by the Bureaus will be deemed to be in compliance with the rules' requirements that notices be clear, conspicuous, comprehensible, and not misleading. As with the *Open Internet* BIAS transparency rules, use of the safe harbor notice is a safe harbor with respect to the format of the required disclosure to consumers. A provider meeting the safe harbor could still be found to be in violation of the rules, for example, if the content of that notice is misleading, otherwise inaccurate, or fails to include all mandated information.

4. Advance Notice of Material Changes to Privacy Policies

****46** 156. We require telecommunications carriers to provide advance notice of material changes to their privacy policies to their existing customers, via email or other means of active communication agreed upon by the customer.[439] As with a provider's privacy policy notice, any advance notice of material changes to a privacy policy must be clear, conspicuous, comprehensible, and not misleading. The notice also must be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language. This notice must inform customers of both (1) the changes being made; and (2) customers' rights with respect to the material change as it relates to their customer PI.[440] In doing so, we follow our own precedent and that of the FTC in recognizing the need for consumers to have up-to-date and relevant information upon which to base their choices.[441] This requirement to notify customers of material change finds strong support in the record.[442]

157. The record reflects strong justifications for requiring providers to give customers advance notice of material changes to their privacy policies.[443] In order to ensure that customer approval to use or share customer PI is "informed" consent, customers must have accurate and up-to-date information of what they are agreeing to in privacy policies.[444] The notice of material change requirement that we adopt is consistent with the transparency requirements of the *2015 Open Internet Order*, which require providers to disclose material changes in, among other things, "commercial terms,"[445] which includes privacy policies.[446] Notices of material change are essential to respecting customers' informed privacy choices; if a provider substantially changes

its privacy practices after a customer has agreed to a different set of practices, the customer cannot be said to have given informed consent, consistent with Section 222. This is particularly important when providers are seeking a customer's opt-out consent, since the customer's privacy rights could change whether or not they had actual knowledge of the change in policy. We therefore disagree that such a requirement is outweighed by the risk of notice fatigue;[447] to the extent ***13974** that providers are frequently changing their policies materially, they should alert their customers to that fact, or risk rendering their earlier efforts at transparency fruitless.

158. For the purposes of this rule, we consider a "material change" to be any change that a reasonable customer would consider important to her decisions on her privacy. This parallels the consumer interest-focused definition of ""material change" used in the *2015 Open Internet Order*.[448] Such changes would primarily include any changes to the types of customer PI at issue, how each type of customer PI is used or shared and for what purpose, or the categories of entities with which the customer PI is shared. To provide guidance on the standard above, at minimum, if any of the required information in the initial privacy notification changes, then the carrier must provide the required update notice. We adopt this guidance because the initial notice contains the information on which customers are making their privacy decisions, and changes to that information may alter how consumers grant permissions to their carriers. We also limit carriers' requirements under this section to existing customers, since only existing customers (and not new applicants) would have a current privacy policy that could be materially changed.

****47** 159. *Delivering Notices of Material Changes*. For consumers to understand carriers' privacy practices, carriers must keep them up to date and persistently available, but must also ensure that customers' knowledge of them is up to date. It is not reasonable, for instance, to expect consumers to visit carriers' privacy policies on a daily basis to see if anything has changed. Therefore, we require telecommunications carriers to notify an affected customer of material changes to their privacy policies by contacting the customer with an email or some other form of active communication agreed upon by the customer.

160. We require active forms of communication with the customer because merely altering the text of a privacy policy on the carrier's website alone is insufficient. There is little chance that, absent some form of affirmative contact, a customer would periodically visit and review a provider's notices of privacy policies for any changes.[449] We also recommend, but do not require, providers to solicit customers' contact preferences to enable customers to choose their preferred method of active contact (such as email, text messaging, or some other form of alert), as not all customers have the same contact preferences. This is particularly true for voice services, where it may be less likely that customers will visit a provider's website, and providers may not have a customer's email address.[450] While this does require each provider to have some means of contacting the customer, it does not require gathering more customer information, since, by virtue of providing service, a provider will necessarily be able to contact a customer, whether by email, text message, voice message, or postal mail.[451] Some commenters have expressed concern that requiring carriers to send multiple notices in different formats for each material change would present "significant logistical challenges."[452] The rules do not require multiple formats for ***13975** each notice of material change, but allow carriers to use one method, whether that is email or some other active method agreed upon by the customer.

161. The active notice requirements reflect the rationale behind the transparency requirements of the *2015 Open Internet Order*, which require directly notifying end users if the provider is about to engage in a network practice that will significantly affect a user's use of the service.[453] As explained in that *Order*, the purpose is to "provide the affected [] users with sufficient information ..." to make choices that will affect their usage of the service.[454] Given these existing obligations, we disagree with commenters who suggest that providing more than one notice is overly burdensome.[455]

162. In addition to the active notice required above, we encourage providers to include notices of changes in customers' billing statements, whether a customer has selected electronic billing, paper bills, or some other billing format.[456] Providing notice via bills can help ensure that customers will receive the notice, and makes it more likely that they will correctly attribute the notice as coming from their provider.[457]

**48 163. *Contents of Advance Notice of Material Changes*. As proposed in the *NPRM*, the advance notice of material change must specify and describe the changes made to the provider's privacy policies, including any changes to what customer PI the provider collects; how it uses, discloses, or permits access to such information; and the categories of entities with which it shares that information.[458] This explanation should also include whether any changes are retroactive (i.e., they will involve the use or sharing of past customer PI that the provider can access).[459] The entire notice must be clear and conspicuous, comprehensible, and not misleading. The notice of material change need not contain the entirety of the provider's privacy policies, so long as it accurately conveys the relevant changes and provides easy access to the full policies. Moreover, the notice of material change must not simply provide fully updated privacy policies without specifically identifying the changes—as stated above, the changes must be identified clearly, conspicuously, comprehensibly, and in a manner that is not misleading. For the same reasons that we impose this requirement with respect to the notice of privacy policies, we also require that the notice of material change be translated into a language other than English if the telecommunications carrier transacts business with the customer in that language. As with the initial notice of privacy policies, the notice of material change must also explain the customer's rights with regard to this information. We do not, however, require that carriers use any particular language in these explanations, and encourage carriers to adapt their notices in ways that best suit their customers. We decline to specify how much advance notification providers must give their customers before making material changes to their privacy policies, recognizing that the appropriate amount of time will vary, *inter* *13976 *alia*, based on the scope of the change or the sensitivity of the information at issue. However, BIAS providers and other telecommunications carriers must give customers sufficient advance notice to allow the customers to exercise meaningful choice with respect to those changed policies.

5. Harmonizing Voice Rules

164. As noted above, we apply these rules to all providers of telecommunications services. Harmonizing the rules for broadband and other telecommunications services will allow providers that offer multiple (and frequently bundled)[460] services within this category to operate under a more uniform set of privacy rules, reducing potential compliance costs.[461] For example, our rules will enable providers to provide the necessary notices for both voice and broadband services at the point of sale, allowing the information to be conveyed in one interaction for customers purchasing bundles, minimizing burdens on providers and customers alike.[462] Furthermore, this consistency also enhances the ability of customers purchasing BIAS and other telecommunications services from a single provider to make informed choices regarding the handling of their information.

**49 165. In harmonizing our notice rules across BIAS and other telecommunications services, we are able to reduce burdens on providers by eliminating certain existing requirements that we find are no longer necessary. For instance, because we require that notice of privacy practices be readily available on providers' websites, an already common practice,[463] we eliminate the requirement that notices of privacy practices be re-sent to customers every 2 years.[464] Further, because the record evinces the growing need for flexibility in applying the principles of transparency, we eliminate requirements that notices provide that "the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI"[465] —a requirement that has apparently been interpreted as requiring that language to appear verbatim in privacy policies.[466] Similarly, we eliminate requirements that emails containing notices of material changes contain specific subject lines, leaving to providers the means by which they can meet the general requirements that any communication must be clear and conspicuous, comprehensible, and not misleading. We find that in lieu of these more prescriptive requirements, the common-sense rules we adopt above better ensure that customers receive truly informative notices without unnecessary notice fatigue or unnecessary regulatory burdens on carriers.

D. Customer Approval Requirements for the Use and Disclosure of Customer PI

166. In this section, we adopt rules that give customers of BIAS and other telecommunications services the tools they need to make choices about the use and sharing[467] of their personal information, and to easily adjust those choices over the course of time. Respecting the choice of the individual is *13977 central to any privacy regime,[468] and a fundamental component of

FIPPs.[469] In adopting Section 222, Congress imposed a duty on telecommunications carriers to protect the confidentiality of their customers' information, and specifically required that carriers obtain customer approval for use and sharing of individually identifiable customer information. In adopting rules to implement these statutory requirements, we look to the record, which includes substantial discussion about customers' expectations in the context of the broader Internet ecosystem, as well as existing regulatory, enforcement, and best practices guidance. We are persuaded that sensitivity-based choice rules are the best way to implement the mandates of Section 222, honor customer expectations, and provide carriers the ability to engage their customers.

167. We therefore adopt rules that require express informed consent (opt-in approval) from the customer for the use and sharing of sensitive customer PI. As described in greater detail below, our rules treat the following information as sensitive: precise geo-location, health, financial, and children's information; Social Security numbers; content; and web browsing and application usage histories and their functional equivalents. For voice providers, our rules also treat call detail information as sensitive. With respect to non-sensitive customer PI, carriers must, at a minimum, provide their customers the ability to opt out of the carrier's use or sharing of that non-sensitive customer information. Carriers must also provide their customers with an easy-to-use, persistent mechanism to adjust their choice options.[470]

**50 168. The sensitivity-based choice approach we adopt is not monolithic. We recognize certain congressionally-directed exceptions to customer approval rights. Most obviously, carriers can, and indeed must, use and share customer PI in order to provide the underlying telecommunications service, to bill and collect payment for that service, and for certain other limited purposes by virtue of delivering the service. Congress also recognized that there are other laws and regulations that allow or require carriers to use and share customer PI without consent. Therefore, we adopt exceptions to our choice framework that allow carriers to use and share information for the congressionally directed purposes outlined in the Communications Act, and as otherwise required or authorized by law.

169. In the first part of this section, we discuss our application of a sensitivity-based framework to the use and sharing of customer PI. We explain what we consider to be sensitive customer PI, and how our rules apply the sensitivity-based framework. In the second part of this section, we explain and implement the limitations and exceptions to that choice framework.

170. In the next parts of this section, we discuss the mechanisms for customer approval provided for in our rules. We explain how and when carriers must solicit and obtain customer approval to use and share the customer's PI under the framework we adopt today, and require carriers to provide customers with easy access to a choice mechanism that is simple, easy-to-use, clearly and conspicuously disclosed, persistently available, and made available at no additional cost to the customer. Finally, we eliminate the requirements that telecommunications providers keep particular records of their use of customer PI and periodically report compliance to the Commission.

171. These rules apply both to BIAS and other telecommunications services. The record reflects strong support for consistency between privacy regimes for all telecommunications services, both to reduce possible consumer confusion,[471] and to decrease compliance burdens for all affected *13978 telecommunications carriers, particularly small providers.[472] Therefore, within the scope of our authority over telecommunications carriers, we apply these rules to all BIAS providers and other telecommunications carriers.

1. Applying a Sensitivity-Based Customer Choice Framework

172. Except as otherwise provided by law and subject to the congressionally-directed exceptions discussed below, we adopt a customer choice framework that distinguishes between sensitive and non-sensitive customer information. We adopt rules that require BIAS providers and other telecommunications carriers to obtain a customer's opt-in consent before using or sharing sensitive customer PI.[473] We also adopt rules requiring carriers to, at a minimum, offer their customers the ability to opt out of the use and sharing of non-sensitive customer information. Carriers may also choose to obtain opt-in approval from their customers to use or share non-sensitive customer PI. To ensure that consumers have effective privacy choices, we require

carriers to provide their customers with a persistent, easy-to-access mechanism to opt in to or opt out of their carriers' use or sharing of customer PI.

****51** 173. In adopting a sensitivity-based framework, we move away from the purpose-based framework—in which the purpose for which the information will be used or shared determines the type of customer approval required—in the current rules and in the rules we proposed in the *NPRM*.[474] Having sought comment on a sensitivity-based framework in the *NPRM*,[475] and having received substantial support for it in the record, we find that incorporating a sensitivity element into our framework allows our rules to be more properly calibrated to customer and business expectations. This approach is also consistent with the framework recommended by the FTC in its comments and its 2012 staff report, and ***13979** used by the FTC in its settlements.[476] We make this transition for both BIAS and other telecommunications services because the record demonstrates that a sensitivity-based framework better reflects customer expectations regarding how their privacy is handled by their communications carriers.[477]

174. Some commenters argue that all customer information is sensitive, and that subjecting only certain information to opt-in approval imposes an unnecessary burden on consumers who want to protect the privacy of their information to opt-out.[478] While we appreciate that consumers are not monolithic in their preferences, as discussed below, we think the rule we adopt today strikes the right balance and gives consumers control over the use and sharing of their information. We decline to conclude that all customer PI is sensitive by default, and instead identify specific types of sensitive information, consistent with the FTC.[479] Other commenters express concern that drawing a distinction between sensitive and non-sensitive information requires a broadband provider to analyze a customer's web browsing history and content to identify sensitive information, rendering the point of the distinction moot.[480] Some commenters argue that carriers can use a system of whitelists to determine sensitive versus non-sensitive web sites.[481] This argument mistakenly presumes that the sensitivity of a customer's traffic relies upon the type or contents of the sites visited, and not simply the fact of the customer having visited them. However, this dispute and the concerns underlying it are themselves mooted by our decision to treat content, browsing history, and application usage history as sensitive and subject to opt-in consent. Thus, recognizing customer expectations and the comments reflecting them in the record, we adopt rules that base the level of approval carriers must obtain from customers upon the sensitivity of the customer PI at issue.

175. Adopting this choice framework implements the requirement in Section 222(c)(1) that carriers, subject to certain exceptions, must obtain customer approval before using, sharing, or permitting access to individually identifiable CPNI. Further, we find that except where a limitation or exception discussed below applies, obtaining consent prior to using or sharing customer PI is a necessary component of protecting the confidentiality of customer PI pursuant to Section 222(a). We also observe that drawing distinctions that allow opt-out or opt-in approval is well-grounded in our Section 222 ***13980** precedent and numerous other privacy statutes and regimes.[482] The Commission has long held that allowing a customer to grant partial use of CPNI is consistent with one of the underlying principles of Section 222: to ensure that customers maintain control over their own information.[483]

****52** 176. Below, we explain the framework and its application. First, we define the scope of sensitive customer PI and explain our reasons for requiring opt-in consent to use or share sensitive customer PI. Consistent with FTC enforcement work and best practices guidance, we also require telecommunications carriers that seek to make retroactive material changes to their privacy policies to obtain opt-in consent from customers. Next, we discuss our reasons for allowing carriers to use and share non-sensitive customer PI subject to opt-out approval.

a. Approval Requirements for the Use and Sharing of Sensitive Customer PI

(i) Defining Sensitive Customer PI

177. For purposes of the sensitivity-based customer choice framework we adopt today, we find that sensitive customer PI includes, at a minimum, financial information; health information; Social Security numbers; precise geo-location information; information pertaining to children; content of communications; call detail information; and a customer's web browsing history, application usage history, and their functional equivalents. Although a carrier can be in compliance with our rules by providing customers with the opportunity to opt in to the use and sharing of these specifically identified categories of information, we encourage each carrier to consider whether it collects, uses, and shares other types of information that would be considered sensitive by some or all of its customers, and subject the use or sharing of that information to opt-in consent.

178. In identifying these categories as sensitive and subject to opt-in approval, we draw on the record and consider the context, which is the customer's relationship with his broadband or other telecommunications provider. The record demonstrates strong support for designating these specific categories of information as sensitive: health information,[484] financial information,[485] precise geo-location information,[486] children's information,[487] and Social Security numbers. The FTC explicitly regards these ***13981** categories of information as sensitive, as well.[488] Despite some commenters' assertions to the contrary,[489] the FTC does not claim to define the outer bounds of sensitive information with this list.[490] For example, in its 2009 Staff Report on online behavioral advertising and in its comments to this proceeding, the FTC clearly indicated that its list was non-exhaustive.[491] Furthermore, Commission precedent and consumer expectations demonstrate strong support for certain additional categories of sensitive information. For instance, the Commission has also afforded enhanced protection to call detail information for voice services.[492] Consumer research also supports identifying several types of information as sensitive: the 2016 Pew study, noted by a number of commenters in the record, found that large majorities of Americans considered Social Security numbers, health information, communications content (including phone conversations, email, and texts), physical locations over time, phone numbers called or texted, and web history to be sensitive.[493] Each of these categories has a clear and well attested case in the record and in federal law for being considered sensitive.[494]

****53** 179. Consistent with the FTC and the record, we conclude that precise geo-location information is sensitive customer PI.[495] Congress specifically amended Section 222 to protect the privacy ***13982** of wireless location information as the privacy impacts of it became clear.[496] Real-time and historical tracking of precise geo-location is both sensitive and valuable for marketing purposes due to the granular detail it can reveal about an individual. Such data can expose "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[497] In some cases, a BIAS provider can even pinpoint in which part of a store a customer is browsing.[498] The FTC has found that precise geo-location data "includ[es] but [is] not limited to GPS-based, WiFi-based, or cell-based location information."[499]

180. The record also reflects the historical and widely-held tenet that the content of communications is particularly sensitive.[500] Like financial and health information, Congress recognized communications as being so critical that their content, information about them, and even the fact that they have occurred, are all worthy of privacy protections.[501] This finding is strongly supported by the record, and consistent with FTC guidance.[502] As the FTC explains, "content data can be highly personalized and granular, allowing analyses that would not be possible with less rich data sets."[503] We therefore concur with the large number of commenters who assert that content must be protected[504] and agree with Access Now in finding that "the use or sharing ... of the content of user communications is a clear violation of the right to privacy."[505] As such, we consider communications contents to be sensitive information.[506]

181. We also add to the list of sensitive customer PI a customer's web browsing and application usage history, and their functional equivalents. A customer's web browsing and application ***13983** usage history frequently reveal the contents of her communications,[507] but also constitute sensitive information on their own[508] —particularly considering the comprehensiveness

of collection that a BIAS provider can enjoy and the particular context of the BIAS provider's relationship with the subscriber. The Commission has long considered call detail information sensitive, regardless of whether a customer called a restaurant, a family member, a bank, or a hospital. The confidentiality of that information, and its sensitivity, do not rely upon what category of entity the customer is calling. The same is true of a customer's web browsing and application usage histories.[509] We therefore decline to define a subset of non-sensitive web browsing and application usage history, as a number of commenters urge.[510]

**54 182. Web browsing and application usage history, and their functional equivalents are also sensitive within the particular context of the relationship between the customer and the BIAS provider, in which the BIAS provider is the on-ramp to the Internet for the subscriber and thus sees all domains and IP addresses the subscriber visits or apps he or she uses while using BIAS. This is a different role than even the large online ad networks occupy—they may see many sites a subscriber visits, but rarely see all of them.[511] The notion is that before a BIAS provider tracks the websites or other destinations its customer visits the customer should have the right to decide upfront if he or she is comfortable with that tracking for the purposes disclosed by the provider.

183. As EFF explains, BIAS providers can acquire a lot of information "about a customer's beliefs and preferences—and likely future activities—from Web browsing history or Internet usage history, especially if combined with port information, application headers, and related information about a customer's usage or devices."[512] For instance, a user's browsing history can provide a record of her *13984 reading habits—well-established as sensitive information[513] —as well as information about her video viewing habits,[514] or who she communicates with via email, instant messaging, social media, and video and voice tools. Furthermore, the domain names and IP addresses may contain potentially detailed information about the type, form, and content of a communication between a user and a website. In some cases, this can be extremely revealing: for instance, query strings within a URL may include the contents of a user's search query, the contents of a web form, or other information.[515] Browsing history can easily lead to divulging other sensitive information, such as when and with what entities she maintains financial or medical accounts, her political beliefs, or attributes like gender, age, race, income range, and employment status.[516] More detailed analysis of browsing history can more precisely determine detailed information, including a customer's financial status, familial status, race, religion, political leanings, age, and location.[517] The wealth of information revealed by a customer's browsing history indicates that it, even apart from communications content, deserves the fullest privacy protection.[518]

184. Web browsing, however, is only one form of sensitive information about a customer's online activities.[519] The use of other applications besides web browsers also provides a significant amount *13985 of insight into a user's behavior. Any of the information transmitted to and from a customer via a browser can just as easily be transmitted via a company-specific or use-specific application. Whether on a mobile device or a desktop computer, the user's newsreader application will give indications of what he is reading, when, and how; an online video player's use will transmit information about the videos he is watching in addition to the video contents themselves; an email, video chat, or over-the-top voice application will transmit and receive not only the messages themselves, but the names and contact information of his various friends, family, colleagues, and others; a banking or insurance company application will convey information about his health or finances; even the mere existence of those applications will indicate who he does business with. A customer using ride-hailing applications, dating applications, and even games will reveal information about his personal life merely through the fact that he uses those apps, even before the information they contain (his location, his profile, his lifestyle) is viewed.[520]

**55 185. Considering the particular visibility of this information to telecommunications carriers, we therefore find that web browsing history and application usage history, and their functional equivalents, are sensitive customer PI.[521] Web browsing history and application usage history includes information from network traffic related to web browsing or other applications (including the application layer of such traffic), and information from network traffic indicating the website or party with which the consumer is communicating (e.g., their domains and IP addresses). We include their functional equivalents to ensure that the privacy of customers' online activities (today most frequently encompassed by browsing and application usage history) will be

protected regardless of the specific technology or architecture used. We expect this to be particularly significant as the Internet of Things continues to develop. While a customer may expect that the people and businesses she interacts with will know some things about her—her bookstore will know what she's bought by virtue of having sold it to her—this is distinct from having her voice or broadband provider extract that information from her communications paths and therefore knowing every store she has visited and everything she has purchased.[522] Furthermore, as mentioned above, a carrier not only has the technical ability to access the information about the customer's calls to the bookstore or visits to its website; it could also, unlike the store, associate that information with the customer's other communications.[523] Edge providers, even those that operate ad networks, simply do not have sufficient access to an individual to put together such a comprehensive view of a consumer's online behavior. And, to the extent a customer wants to prevent edge providers from collecting information about her, she can adopt a number of readily available privacy-enhancing technologies.[524] While the knowledge of any one fact from a customer's online history (the use of an online app) may be known to several parties (including the BIAS provider, the app itself, the server of an in-app advertisement),[525] the BIAS provider has the technical ability to access the most complete and most unavoidable picture of that history. We therefore disagree with commenters who believe that browsing history or application usage are not sensitive in the context of the customer/BIAS provider relationship.[526]

***13986** 186. Also, contrary to some commenters' arguments, the existence of encryption on websites or even in apps does not remove browsing history from the scope of sensitive information. As noted above,[527] encryption is far from fully deployed;[528] the volume of encrypted data does not represent a meaningful measure or privacy protection;[529] and carriers have access to a large and broad amount of user data even when traffic is encrypted, including, frequently, the domains and IP addresses that a customer has visited.[530] Comcast argues that because BIAS providers are limited to this information, they have less access to information overall.[531] While the record indicates that BIAS providers have a less granular view of encrypted web traffic than unencrypted, it does not change the breadth of the carrier's view or the fact that it acquires this information by virtue of its privileged position as the customer's conduit to the internet. Nor does it change the fact that this still constitutes a record of the customer's online behavior, which, as noted above, can reveal details of a customer's life even at the domain level.

****56** 187. In deciding to treat broadband customers' web browsing history, application history, and their functional equivalents as sensitive information, we agree with commenters, including technical experts, who explain that attempting to neatly parse customer data flowing through a network connection into sensitive and non-sensitive categories is a fundamentally fraught exercise.[532] As a number of commenters have noted, a network provider is ill-situated to reliably evaluate the cause and meaning of a customer's network usage.[533] We therefore disagree with the suggestion made by some commenters that web browsing is not sensitive, because providers have established methods of sorting data which do not require them to "manually inspect" the contents of packets.[534]

***13987** 188. This remains true even when providers do not attempt to classify customers' browsing and application usage as they use BIAS, but instead employ blacklists or whitelists of sensitive or non-sensitive sites and applications.[535] Although commenters cite various industry attempts to categorize consumer interests, and identify the sensitive categories among those, the definitions vary significantly between them.[536] Even within one set of classifications, the lines between what is and is not considered sensitive information can be difficult to determine. For instance, as Common Sense Kids Action points out, determining when browsing information belongs to a child, teen, or adult customer or user would require more than knowing the user's online destination.[537] Further, as OTI notes, something that is non-sensitive to a majority of people may nevertheless be sensitive to a minority, which may have the unintended consequence of disparately impacting the privacy rights of racial and ethnic minorities and other protected classes.[538] By treating all web browsing data as sensitive, we give broadband customers the right to opt in to the use and sharing of that information, while relieving providers of the obligation to evaluate the sensitivity and be the arbiter of any given piece of information.

189. We also observe that treating web browsing and application usage history as sensitive in the context of the BIAS/customer relationship is consistent with industry norms among BIAS providers. Until recently, for example, to participate in AT&T's GigaPower Premium Offer (i.e., to receive the fixed broadband service GigaPower at a lower cost), customers had to opt in to AT&T Internet Preferences. Under AT&T's Internet Preferences, "you agree to share with us your individual browsing, like the search terms you enter and the webpages you visit, so we can tailor ads and offers to your interests."[539] AT&T explained that "AT&T Internet Preferences works independently of your browser's privacy settings regarding cookies, do-not-track and private browsing" and that "[i]f you opt-in to AT&T Internet Preferences, AT&T will still be able to collect and use your Web browsing information independent of those settings."[540] In short, AT&T appears to have tracked web browsing history only pursuant to customer opt-in. Similarly, participation in Verizon's Verizon Selects program is on an opt-in basis. That opt-in program uses web browsing and application usage data, along with location, to develop marketing information about its customers.[541]

****57 *13988** 190. We disagree with the assertions made by a number of advertising trade associations that web browsing history should not be considered sensitive customer PI because courts have "found that the advertising use of web browsing histories tied to device information does not harm or injure consumers."[542] We find this to be inapposite to the task we confront in applying Section 222 of the Act. These cases deal with a factually different, and significantly narrower, scenarios than we address through web browsing history in this Order.[543]

191. We recognize that there are other types of information that a carrier could add to the list of sensitive information, for example information that identifies customers as belonging to one or more of the protected classes recognized under federal civil rights laws. Commenters also describe as sensitive other forms of governmental identification,[544] biometric identifiers,[545] and electronic signatures.[546] Other privacy frameworks, both governmental and commercial, identify other types of information as particularly sensitive, such as race, religion, political beliefs, criminal history, union membership, genetic data, and sexual habits or sexual orientation.[547] Most of these categories already overlap with our established categories, or the use or sharing of such information would be subject to opt-in requirements pursuant to the requirement to obtain opt-in consent for the use and sharing of content and web browsing and application usage history. Moreover, as explained above, carriers are welcome to give their customers the opportunity to provide opt-in approval for the use and sharing of additional types of information. However, we recognize that as technologies and business practices evolve, the nature of what information is and is not sensitive may change,[548] and as customer expectations or the public interest may require us to refine the categories of sensitive customer PI, we will do so.

***13989 (ii) Opt-In Approval Required for Use and Sharing of Sensitive Customer PI and Retroactive Material Changes in Use of Customer PI**

192. As the FTC recognizes, "the more sensitive the data, the more consumers expect it to be protected and the less they expect it to be used and shared without their consent."[549] We therefore require BIAS providers and other telecommunications carriers to obtain a customer's opt-in consent before using, disclosing, or permitting access to his or her sensitive customer PI, except as otherwise required by law and subject to the other exceptions outlined in Part III.D.2.

193. Consistent with the Commission's existing CPNI rules and wider precedent,[550] opt-in approval requires that the carrier obtain affirmative, express consent from the customer for the requested use, disclosure, or access to the customer PI. Because Section 222(a) requires protection of the confidentiality of all customer PI, we include all types of sensitive customer PI, and not just sensitive, individually identifiable CPNI, within the definition of opt-in approval.[551] The broad support in the record for protecting sensitive information nearly unanimously argues that use and sharing of sensitive customer information be subject to customer opt-in approval.[552] The record demonstrates that customers expect that their sensitive information will not be shared without their affirmative consent, and sensitive information, being more likely to lead to more serious customer harm, requires additional protection.[553] For instance, the FTC recognizes that consumer expectations drive increased protections for sensitive

information.[554] We find that requiring opt-in approval for the use and sharing of sensitive customer PI reasonably balances burdens between carriers and their customers. If a carrier's uses or sharing of customers' sensitive personal information benefits those customers,[555] the customer has every incentive to make that choice, and the carrier has every incentive to make the benefits of that choice clear to the customer.[556] We anticipate that this will increase the amount of clear and informative information that customers will have about the costs and benefits of participation in these programs. Carriers' incentives to encourage customer opt-in will likely be tempered by carriers' desire to avoid alienating customers with too-frequent solicitations to opt in.[557]

**58 194. In contrast, we find that opt-out consent would be insufficient to protect the privacy of sensitive customer PI. Research has shown that default choices can be "sticky," meaning that consumers *13990 will remain in the default position, even if they would not have actively chosen it.[558] Further, opt-in regimes provide additional incentives for a company to invest in making notices clear, conspicuous, comprehensible, and direct.[559] Additionally, empirical evidence shows that relatively few customers opt out even though a larger number express a preference not to share their information, suggesting that they did not receive notice or were otherwise frustrated in their ability to exercise choice.[560] In an opt-in scenario, however, we anticipate that many consumers, solicited by carriers incentivized to provide and improve access to their notice and choice mechanisms, will wish to affirmatively exercise choice options around the use and sharing of sensitive information. Although we recognize that opt-in imposes additional costs, based on these factors we find that opt-in is warranted to maximize opportunities for informed choice about sensitive information.

195. *Material Retroactive Changes*. Notwithstanding the fact that our choice framework generally differentiates between sensitive and non-sensitive information, we agree with the FTC and other commenters that material retroactive changes require a customer's opt-in consent for changes to the use and sharing of both sensitive and non-sensitive information.[561] The record demonstrates widespread conviction that material retroactive changes to privacy policies should require opt-in approval from customers.[562] Retroactive changes in privacy policies particularly risk violating customers' privacy expectations because they result in a carrier using or sharing information already collected from a customer for one purpose or set of purposes for a different purpose. Because of this, we require that telecommunications carriers obtain customers' opt-in approval before making retroactive material changes to privacy policies. It is a "bedrock principle" of the FTC that "companies should provide *13991 prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection."[563] This means that, whether customer PI is sensitive or non-sensitive, a telecommunications carrier must obtain opt-in permission if it wants to use or share data that it collected before the time that the change was made. For instance, if a carrier wanted to change its policy to share a customer's past monthly data volumes with third party marketers, it would need to obtain the customer's opt-in permission. In contrast, if the carrier changes its policy to share the customer's future monthly data volumes with those same marketers, it would only need the customer's opt-out consent.

b. Approval Requirements for the Use and Sharing of Non-Sensitive Customer PI

**59 196. We recognize that customer concerns about the use and sharing of their non-sensitive customer PI will be less acute than sharing of sensitive PI, and that there are significant benefits to customers and to businesses from some use and sharing of non-sensitive customer PI. However, we reject suggestions that consumers should be denied choice about the use and sharing of any of their non-sensitive information.[564] Empowering consumers by providing choice is a standard component of privacy frameworks.[565] Further, ensuring choice is necessary as a part of effectuating the duty to protect the confidentiality of customer PI under Section 222(a) and the duty to obtain the approval of the customer before using, disclosing, or permitting access to individually identifiable CPNI under Section 222(c)(1). Therefore, consistent with the FTC privacy framework, we require BIAS providers and other telecommunications carriers to obtain the customer's opt-out approval to use, disclose, or permit access to non-sensitive customer PI.[566]

197. We define opt-out approval as a means for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information under which a customer is deemed to have consented to the use, disclosure, or access to the customer's covered information if the customer has failed to object thereto after the carrier's request for consent.[567] This definition, based on the existing CPNI voice rules, applies to all non-sensitive customer PI for all covered telecommunications carriers. The current CPNI rules define opt-out approval to require a thirty-day waiting period before a carrier can consider a customer's opt-out approval effective. We eliminate this requirement, and similarly decline to apply it to BIAS providers or other telecommunications carriers. As borne out in the record, we find that requiring carriers to enable customers to opt out at any time and with minimal effort will reduce the likelihood that customers' privacy choices would not be respected. As such, we believe that the 30-day waiting period is no longer necessary and provide additional regulatory flexibility by eliminating it.[568] We make clear, however, that while we do not adopt a specific timeframe for effectuating customers' opt-out approval choices, we do not expect carriers to assume that a customer has granted opt-out consent ***13992** when a reasonable customer would not have had an opportunity to view the solicitation. We conclude that this flexible standard will appropriately account for the faster pace of electronic transactions, while preventing carriers from using customer PI before customers have had the opportunity to opt out.

198. We agree with commenters who assert that non-sensitive information naturally generates fewer privacy concerns for customers, and as such does not require the same level of customer approval as for sensitive customer PI.[569] From this, we conclude that an opt-out approval regime for use and sharing of non-sensitive customer PI would likely meet customers' privacy expectations. We agree with ANA that "[a]n opt-out framework for uses of non-sensitive information also matches consumers' expectations regarding treatment of their data,"[570] and CTIA that "[b]y tying its rules to the sensitivity of the data, the Commission will ensure that they align with consumer expectations and what consumers know to be fair."[571] While an opt-out regime places a greater burden than an opt-in regime upon customers who do not wish for their carrier to use or share their non-sensitive information, research suggests that those same customers will likely be more motivated to actively exercise their opt-out choices.[572] Further, we conclude that permitting carriers to use and share non-sensitive data with customers' opt-out approval—rather than opt-in approval—grants carriers flexibility to make improvements and innovations based on customer PI.[573] For example, ACA notes that an opt-out framework can allow "providers, including small providers, to explore, market, and deploy innovative, value-added services to their consumers, including home security and home automation services that will drive the 'Internet of Things.'"[574] Thus, we reject arguments that "opt-out is not an appropriate mechanism to obtain user approval" in any circumstances.[575]

****60** 199. We disagree with commenters who assert that customer approval to use and share customer PI for the purposes of all first party marketing is generally implied in Section 222.[576] We find that allowing carriers to use or share customer PI for all first party marketing does not comport with Section 222's customer approval and data protection requirements. Section 222(c)(1) explicitly requires customer approval to use and share CPNI for purposes other than providing the telecommunications ***13993** service, and subject to certain other limited exceptions. Likewise, Section 222(a) imposes a duty on carriers to protect the confidentiality of customer PI. We conclude that permitting carriers to use and share customer PI to market all carrier and affiliate services based on inferred customer approval is inconsistent with these statutory obligations.[577] Our conclusion is also consistent with Commission precedent and FTC Staff comments.[578] While some comments assert that customers expect some degree of targeted marketing absent explicit customer approval,[579] the record also indicates that customers expect choice with regard to the privacy of their online communications.[580] Inferring consent for all first-party marketing would leave consumers without the right to opt out of receiving any manner of marketing from their telecommunications carrier—violating that basic precept recognized by Justice Louis Brandeis of the "right of the individual to be let alone."[581] We accordingly adopt an opt-out regime for first-party marketing that relies on non-sensitive customer PI to fulfill Section 222 and provide customers with the choice that they desire without unduly hindering the marketing of innovative services.

200. Giving consumers control of the use and disclosure of their information, even for first-party marketing, is consistent with other consumer protection laws and regulations adopted by the both the FTC and FCC. For instance, the popular and familiar

National Do Not Call registry, created by the FTC, the FCC, and the states empowers consumers to opt out of most telemarketing calls.[582] Consumers have registered over 222 million phone numbers with the Do Not Call Registry in order to stop unwanted marketing calls.[583] Also, pursuant to rules adopted by both the FTC and the FCC, consumers to have the right to opt out of receiving calls even from companies with which they have a prior business relationship, ***13994** with businesses required to place the consumer on a do-not-call list upon the consumer's request.[584] The CAN SPAM Act of 2003,[585] and the rules the FTC adopted under CAN SPAM, also give consumers the right to opt out of the receipt of future commercial email from and require senders of commercial email to provide a working mechanism in their email to facilitate those opt-outs.[586] Our rules follow these many models.

2. Congressionally-Recognized Exceptions to Customer Approval Requirements for Use and Sharing of Customer PI

****61** 201. In this section, we detail the scope of limitations and exceptions to the customer approval framework discussed above. In the first part of this section, based on our review of the record and our analysis of the best way to implement Section 222, we find that no additional customer consent is needed in order for a BIAS provider or other telecommunications carrier to use and share customer PI in order to provide the telecommunications service from which such information is derived or provide services necessary to, or used in, the provision of such telecommunications service. These limitations on customer approval requirements allow a variety of necessary activities beyond the bare provision of services, including research to improve or protect the network or telecommunications, and limited first-party marketing of services that are part of, necessary to, or used in the provision of the telecommunications service. In the second part of this section, we apply the statutory exceptions detailed in Section 222(d) to all customer PI, allowing telecommunications carriers to use and share customer PI to: (1) initiate, render, bill, and collect for telecommunications services; (2) protect the rights or property of the carrier, or to protect users and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, telecommunications services; (3) provide any inbound telemarketing, referral, or administrative services to the customer for the duration of a call; and (4) provide customer location information and non-sensitive customer PI in certain specified emergency situations.[587] We also take this opportunity to clarify that our rules do not prevent use and sharing of customer PI to the extent such use or sharing is allowed or required by other law.

202. The statutory mandate of confidentiality is not an edict of absolute secrecy. The need to use and share customer information to provide telecommunications services, to initiate or render a bill, to protect the network, and to engage in the other practices identified above are inherent in a customer's subscription. While Congress specified this in the context of its more detailed provisions on customer approval for CPNI in Sections 222(c)-(d), it left to the Commission the details of determining the scope of the duty of confidentiality. We therefore exercise our authority to adopt implementing rules in order to harmonize the application in our rules of Section 222(a) as to customer PI with the limitations and exceptions of Sections 222(c)-(d). Doing so ensures that carriers are not burdened with disparate or duplicative approval requirements based upon whether a particular piece of information is classified as CPNI, PII, or both.[588] We disagree with commenters who argue that extending these limitations and exceptions to approval requirements unduly risk customers' privacy.[589] We make clear that carriers using ***13995** or sharing customer PI should remain particularly cognizant of their obligation to comply with the data security standards in Part III.E, below. We also emphasize that carriers should be particularly cautious about using sensitive customer PI, especially the content of communications, and carriers should carefully consider whether its use is necessary before making use of it subject to these limitations and exceptions. Furthermore, we observe that BIAS providers and other telecommunications carriers remain subject to all other applicable laws and regulations that affect their collection, use, or disclosure of communications, including but not limited to, the Electronic Communications Privacy Act (ECPA), the Communications Assistance for Law Enforcement Act (CALEA), Section 705 of the Communications Act, and the Cybersecurity Information Sharing Act (CISA).[590]

a. Provision of Service and Services Necessary to, or Used in, Provision of Service

****62** 203. Section 222 makes clear that no additional customer consent is needed to use customer PI to provide the telecommunications service from which it was derived, and services necessary to, or used in the telecommunications service.[591]

Consent to use customer PI for the provision of service is implied in the service relationship.[592] Customers expect their information to be used in the provision of service—after all, customers fully intend for their communications to be transmitted to and from recipients—and they necessarily give their information to the carrier for that purpose.[593] For instance, a number of commenters objected to our inclusion of IP addresses as forms of customer PI, because they are necessary to route customers' communications, or otherwise provide telecommunications service.[594] This concern is misplaced; while a BIAS provider needs to share its customer's IP address to provide the broadband service, there is no basis to share that information for other non-exempt purposes absent customer consent. Indeed, because of the explicit limitation described by Section 222(c)(1)(A) and implemented here, we do not need to exclude IP addresses or other forms of information from the scope of customer PI in order to allow the provision of telecommunications service, or services necessary to or used in providing telecommunications service. Thus, we import these statutory mandates into our rules and apply them to all customer PI.

204. We continue to find, as did previous Commissions, that telecommunications customers expect their carriers to market them improved service offerings within the scope of service to which they already subscribe, and as such, conclude that such limited first-party marketing is part of the provision of the telecommunications service within the meaning of Section 222(c)(1)(A).[595] As with earlier CPNI orders, we decline to enumerate a definitive list of "services necessary to, or used in, the provision of ... telecommunications service" within the meaning of Section 222(c)(1).[596] However, we provide guidance ***13996** with respect to certain services raised in the record, and specifically find that this exception includes the provision and marketing of communications services commonly bundled together with the subscriber's telecommunications service, customer premises equipment, and services formerly known as "adjunct-to-basic services." We further find that the provision of inside wiring and technical support; reasonable network management; and research to improve and protect the network or the telecommunications either fall within this category or constitute part of the provision of telecommunications service.[597]

205. *Services that are Part of, Necessary to, or Used in the Provision of Telecommunications Service*. The Commission has historically recognized that, as a part of providing service, carriers may, without customer approval, use and share CPNI to market service offerings among the categories of service to which the customer already subscribes.[598] We therefore adopt a variation of our proposal, which mirrored the existing rule, and permit telecommunications carriers to infer approval to use and share non-sensitive customer PI to market other communications services commonly marketed with the telecommunications service to which the customer already subscribes. For example, the carrier could infer consent to market voice (whether fixed and/or mobile) and video service to a customer of its broadband Internet access service.[599] We limit this exception to the use and sharing of non-sensitive information, because we agree with a number of commenters that this type of marketing remains part of what customers expect from their telecommunications carrier when subscribing to a service.[600] For example, under our rules, a BIAS provider can offer customers new or different pricing or plans for the customers' existing subscriptions (e.g., a carrier may, without the customer's approval, use the fact that the customer regularly reaches a monthly usage cap to market a higher tier of service to the customer). This exception also allows carriers to conduct internal analyses of non-sensitive customer PI to develop and improve their products and services and to develop or improve their offerings or marketing campaigns generally, apart from using the customer PI to target specific customers.[601]

****63** 206. The Commission also has historically recognized certain functions offered by telecommunications carriers as inherently part of, or necessary to, or used in, the provision of telecommunications service. Consistent with Commission precedent, we reaffirm that services formerly known as "adjunct-to-basic," including, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain centrex features, are either part of the provision of telecommunications service or are "necessary to, or used in" the provision of that telecommunications service.[602] Similarly, the Commission has, in prior orders, recognized that the provision and marketing of certain other services as being "necessary to, or used in" the provision of service, such as call answering, voice mail or messaging, voice storage and retrieval services, fax storage and retrieval services, and ***13997** protocol conversion, and we continue to do so today.[603] Likewise, we continue to find that CPE, as well as other

customer devices, inside wiring installation, maintenance, and repair, as well as technical support, serve as illustrative examples of services that are either part of the telecommunications service or are " necessary to, or used in" the provision of the underlying telecommunications service for the purposes of these rules.[604] Customers require working inside wiring to receive service, and often depend upon technical support to fully utilize their services.[605] As such, carriers may use and share non-sensitive customer PI, without additional customer approval, to provide and market such services.[606]

207. In importing these historical findings into the rules we adopt today and applying them to the current telecommunications environment, we make clear that our rules no longer permit CMRS providers to use or share customer PI to market all information services without customer approval.[607] In first making these findings, the Commission noted the potential to revisit this decision if it became apparent that customer expectations, and the public interest, changed.[608] The *1999 CPNI Reconsideration Order* interpreted Section 222(c)(1) as permitting CMRS providers to market information services in general to their customers without customer approval, but limited the information services for which wireline carriers could infer approval.[609] That decision was made when the mobile information services market was in its infancy. As the third party mobile application market has developed, we can no longer find that such an exception is consistent with giving consumers meaningful choice over the use and sharing of their information. Moreover, we have a strong interest in our rules being technologically neutral.

208. *Reasonable Network Management*. We agree with commenters asserting that BIAS providers need to use customer PI to engage in reasonable network management.[610] We have previously explained that a network practice is "reasonable if it primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband service."[611] We recognize that reasonable network management plays an ***13998** important role in providing BIAS, and consider reasonable network management to be part of the telecommunications service or "necessary to, or used in" the provision of the telecommunications service.[612] As such, we clarify that BIAS providers may infer customer approval to use, disclose, and permit access to customer PI to the extent necessary for reasonable network management, as we defined that term in the *2015 Open Internet Order*.

****64** 209. *Research to Improve and Protect Networks or Telecommunications*. We also find that certain uses and disclosures of customer PI for the purpose of conducting research to improve and protect[613] networks or telecommunications are part of the telecommunications service or "necessary to, or used in" the provision of the telecommunications service for the purposes of these rules.[614] For instance, Professor Feamster explains that "network research fundamentally depends on cooperative data sharing agreements with ISPs," and that, lack of access to certain types of customer PI, "will severely limit vendors' and developers' ability to build and deploy network technology that functions correctly, safely, and securely."[615] Comcast also emphasizes the need to share customer PI with "trusted vendors, researchers, and academics ... under strict confidentiality agreements ... to improve both the integrity and reliability of the service."[616] NCTA also argues that carriers must be able to use customer data for internal operational purposes such as improving network performance.[617] Some commenters, such as CDT, caution that a research exemption, read too broadly, might permit privacy violations.[618] We share these concerns, and emphasize that in the interest of protecting the confidentiality of customer PI, carriers should seek to minimize privacy risks that may stem from using and disclosing customer PI for the purpose of research, and should ensure that the entities to which they disclose customer PI will likewise safeguard customer privacy.[619] Telecommunications carriers and researchers should design research projects that incorporate principles of privacy-by-design,[620] and agree not to publish or otherwise publicly ***13999** share individually identifiable data without customer consent. In addition, the existing rules permit CMRS providers to infer customer approval to use and share CPNI for the purpose of conducting research on the health effects of CMRS.[621] We retain this limited provision, extending it to all customer PI. We reiterate that that carriers should endeavor to minimize privacy risks to customers.

b. Specific Exceptions

210. In addition to the activities included in the provision of service and services necessary to, or used in, provision of service, carriers do not need to seek customer approval to engage in certain specific activities that represent important policy goals detailed in Section 222(d). We apply those exceptions to the customer approval framework to all customer PI.

211. *Initiate, Render, Bill, and Collect for Service*. We import into our rules and apply to all customer PI the statutory exception permitting carriers to use, disclose, and permit access to CPNI "to initiate, render, bill, and collect for telecommunications services" without obtaining additional customer consent. As the Rural Wireless Association explains, carriers frequently need to share "certain customer information" "with billing system vendors, workforce management system vendors, consultants that assist with certain projects, help desk providers, and system monitoring solutions providers."[622]

****65** 212. *Protection of Rights and Property*. We also import into our rules and apply to all customer PI the statutory provision permitting carriers to use, disclose, and permit access to CPNI "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services" without obtaining specific customer approval.[623] We agree with the broad set of commenters who expressed the opinion that this exception should be incorporated into the rules,[624] and further agree that it should also apply to customer PI beyond CPNI.[625] We also find that these rules comport with the Cybersecurity Information Sharing Act of 2015 (CISA), which permits certain sharing of cyber threat indicators between telecommunications providers and the federal government or private entities, "notwithstanding any other provision of law."[626] ***14000** Moreover, to the extent that other federal laws, such as CISA, permit or require use or sharing of customer PI, our rules expressly do not prohibit such use or sharing.

213. We also agree with commenters that this provision of our rules encompasses the use and sharing of customer PI[627] to protect against spam, malware such as viruses, and other harmful traffic,[628] including fraudulent, abusive, or otherwise unlawful robocalls.[629] We caution that carriers using or sharing customer PI pursuant to this section of the rules should remain vigilant about limiting such use and sharing to the purposes of protecting their networks and users, and complying with their data security requirements.[630] We acknowledge Access Now's concern that an overbroad reading of this exception could result in carriers actively and routinely monitoring and reporting on customers' behavior and traffic,[631] and make clear that the rule does not allow carriers to share their customers' information wholesale on the possibility that doing so would enhance security; use and sharing of customer PI for these purposes must be reasonably tailored to protecting the network and its users.

214. We agree with commenters that recommend that we consider this provision of our rules to encompass not only actions taken to combat immediate security threats, but also uses and sharing to research and develop network and cybersecurity defenses.[632] When combined with the immunity granted by CISA, this exception addresses carriers' concerns about participating in cybersecurity sharing initiatives.[633] Security is an essential part of preventing bad actors from gaining unauthorized access to the system or making abusive use of it with spam, malware, or denial of service attacks. Research and development into new techniques and technologies for addressing fraud and abuse may require internal use of customer PI, but also disclosures to third-party researchers and other collaborators. However, as with other applications of this exception, carriers should not disclose more information than is reasonable to achieve this purpose, and should take reasonable steps to ensure that the parties with which they share information use this information only for the purposes for which it was disclosed.[634]

****66** ***14001** 215. *Providing Inbound Services to Customers*. Customers expect that a carrier will use their customer PI when they initiate contact with the carrier in order to ask for support, referral, or new services in a real-time context. Therefore, within the limited context of the particular interaction, carriers can use customer PI to render the services that the customer requests without receiving additional approval from the customer. This provision represents a more generalized version of the exception in Section 222(d)(3), which specifies that carriers may use customer PI "for the duration of [a support, referral, or request for

new services] call." Under the rule we adopt today, carriers may use customer PI for the duration of any real-time interaction, including voice calls, videoconferencing, and online chats. However, given the less formal nature of such requests, a carrier's authorization to use the customer PI without additional permission should only last as long as that particular interaction does, and not persist longer. We find that this provision will achieve the same purpose as existing Section 64. 2008(f) of our rules, which allows carriers to waive certain notice requirements for one-time usage of customer PI. We believe that carriers' ability to use customer PI for these purposes without additional customer permission obviates the need for streamlined notice and consent requirements in one-time interactions.

216. Some commenters have argued that our rules should permit a carrier to share customer PI with its agents absent customer approval, noting the need to share customer PI with agents to provide customer support, billing, or other tasks.[635] We agree that such sharing is often necessary, and the limitations and exceptions outlined above allow carriers to share customer PI with their agents without additional customer approval. To the extent that a carrier needs to share customer PI with an agent for a non-exempt task, it needs no more customer approval than it would have needed in order to perform that task itself.[636] This is consonant with the Communications Act's requirement that carriers' agents, acting in the scope of their employment, stand in the place of the carrier, both in terms of rights and liabilities.[637]

217. *Providing Certain Customer PI in Emergency Situations*. In adopting Section 222, Congress recognized the important public safety interests in ensuring that carriers can use and share necessary customer information in emergency situations. Section 222(d)(4) specifically allows carriers to provide call location information of commercial mobile service users to: (1) certain specified emergency services, in response to a user's call for emergency services; (2) a user's legal guardian or immediate family member, in an emergency situation that involves the risk of death or serious physical harm; and (3) to providers of information or database management services solely for the purpose of assisting in the delivery of emergency services in the case of an emergency. We adopt rules mirroring these exceptions, and expand the scope of information that may be disclosed under these circumstances to include customer location information and non-sensitive customer PI.

****67** 218. While commercial mobile service users' location may be the information most immediately relevant to emergency services personnel, other forms of customer PI may also be relevant for customers using services other than commercial mobile services, especially if customers are seeking ***14002** emergency assistance through means other than dialing 9-1-1 on a voice line.[638] Expanding the types of information available in an emergency to include non-sensitive information such as other known contact information for the customer or the customer's family or legal guardian will allow carriers the flexibility necessary to keep emergency services informed with actionable information. However, recognizing the concerns that too broad an exception could lead to increased exposure of sensitive information,[639] we extend the exception only to customer location information and non-sensitive customer PI.

219. We recognize that, as with any provision that allows disclosure of a customer's information, this exception can potentially be abused. Various bad actors may use pretexting techniques, pretending to be a guardian, immediate family member, emergency responder, or other authorized entity to gain access to customer PI.[640] As with all of the other provisions of these rules, we expect carriers to abide by the security standards set forth in Part III.E, below. Under these standards, we expect that carriers will reasonably authenticate third parties to whom they intend to disclose or permit access to customer PI. This need to act reasonably also applies to authenticating emergency services and other entities covered under this exception, as well as authenticating customers themselves.

220. We decline suggestions that we allow carriers only to divulge customer PI in emergency situations to emergency contact numbers specified by the customer in advance.[641] While such a safeguard could prevent a certain amount of pretexting, we believe that such a requirement would be overly restrictive and, in the case of call information, contrary to the statute. If such a requirement were in place, customers who failed to supply or update emergency contact information would be denied the ability for guardians or family members from being contacted. Recognizing the permissible nature of Section 222(d), we do not prohibit carriers from using such a safeguard if they so choose.

3. Requirements for Soliciting Customer Opt-Out and Opt-In Approval

221. In this section, we discuss the requirements for soliciting customer approval for the use and sharing of customer PI. First, we require telecommunications carriers to solicit customer approval at the point of sale, and permit further solicitations after the point of sale. Next, we require that carriers actively contact their customers in these subsequent solicitations, to ensure that customers are adequately informed. Finally, we require the solicitations to be clear and conspicuous, to be comprehensible and not misleading, and to contain the information necessary for a customer to make an informed choice regarding her privacy.

****68** 222. *Timing of Solicitation*. Based on the record before us, we conclude that BIAS providers and other telecommunications carriers must solicit customers' privacy choices at the point of sale. We agree with the FTC and other commenters that the point of sale remains a logical time for customers to exercise privacy decisions because it precedes the carriers' uses of customer PI; frequently allows for clarification of terms between customer and carrier; and avoids the need for customers to make privacy decisions when distracted by other considerations, and is the time when customers are making decisions about material terms.[642]

223. We further find that, in addition to soliciting choice at point-of-sale, a carrier seeking customer approval to use customer PI may also solicit that permission at any time after the point after the sale, so long as the solicitation provides customers with adequate information as specified in these rules. ***14003** This allows carriers to supply customers with relevant information at the most relevant time and in the most relevant context.[643] Moreover, a carrier that makes material changes to its privacy policy must solicit customers' privacy choices before implementing those changes. Material retroactive changes require opt-in customer approval as discussed above in Part III.D.1.a(ii). Consistent with our sensitivity-based framework, prospective material changes require opt-in approval if they entail use or sharing of sensitive customer PI, and opt-out approval if they entail use or sharing of non-sensitive customer PI.

224. *Methods of Solicitation*. We agree with commenters who recommend that we not require particular formats or methods by which a carrier must communicate its solicitation of consent to customers. On this point, we agree with NTCA and USTelecom, which request flexibility in determining the means of solicitation, arguing that carriers are best placed to determine the most effective ways of reaching their customers.[644]

225. The existing voice rules contain specific requirements for solicitations sent as email, such as a requirement that the subject line clearly and accurately identify the subject matter of the email.[645] We decline to include such specific requirements and thereby provide carriers with additional flexibility to develop clear notices that best serve their customers. However, the clarity and accuracy of an email subject line are highly relevant to an overall assessment of whether the solicitation as a whole was clear, conspicuous, comprehensible and not misleading.

226. *Contents of Solicitation*. Carriers' solicitations of opt-in or opt-out consent to use or share customer PI must clearly and conspicuously inform customers of the types of customer PI that the carrier is seeking to use, disclose, or permit access to; how those types of customer PI will be used or shared; and the categories of entities with which that information is shared. The solicitations must also be comprehensible and not misleading, and be translated into a language other than English if the telecommunications carrier transacts business with the customer in that language. As with our notice requirements, we decline to specify a particular format or wording for this solicitation, so long as the solicitation meets the standards described above. The solicitation must provide a means to easily access the carrier's privacy policy as well as a means to easily access to a mechanism, described below in Part III.D.4, by which the customer can easily exercise his choice to permit or deny the use or sharing of his customer PI. Access to the choice mechanism may take a variety of forms, including being built into the solicitation, or provided as a link to the carrier's website, an email address that will receive the customer's choice, or a toll-free number that a customer can call to make his choice.[646]

**69 227. As a point of clarification, the distinction between notice and consent solicitation is one of functionality, not necessarily of form. Choice solicitations may be combined with notices of privacy policies or notices of material change in privacy policies, but only to the extent that both the notices and solicitations meet their respective requirements for being clear and conspicuous, comprehensible, and not misleading. For instance, a carrier instituting a new program that uses non-sensitive customer PI prospectively could send an existing customer a notice of material change to the privacy policy that contained the opt-out solicitation (described in this Part) and access to the customer's choice mechanism *14004 (described in Part III.D. 4, *infra*). This communication would, subject to the ease-of-use requirements, satisfy the rules. We further clarify that we are not requiring carriers to have special "customer PI" choice mechanisms that are different and stand alone from other mechanisms that may exist, so long as those mechanisms satisfy the outcomes required by our rules (such as, among other things, that they be clear and conspicuous). Likewise, we are not mandating a "blanket" choice mechanism. A carrier is free to give the customer the ability to pick and choose among which marketing channels the customer will opt out of. At the same time, if a carrier wanted to give the customer the ability to opt out of all marketing with a single click, that would be consistent with our rules.[647]

4. Customers' Mechanisms for Exercising Privacy Choices

228. In soliciting a customer's approval for the use or sharing of his or her customer PI, we require carriers to provide customers with access to a choice mechanism that is simple, easy-to-use clear and conspicuous, in language that is comprehensible and not misleading, and made available at no additional cost to the customer. This choice mechanism must be persistently available on or via the carrier's website; on the carrier's app, if it provides one for account management purposes; and on any functional equivalents of either.[648] If a carrier lacks a website, it must provide a persistently available mechanism by another means such as a toll-free telephone number. However, we decline to specify any particular form or format for this choice mechanism. Carriers must act upon customers' privacy choices promptly.

229. *Format*. As with our requirements for notices and for solicitations of approval, the actual mechanism provided by the carrier by which customers may inform the carrier of their privacy choices must be clear and conspicuous, and in language that is comprehensible and not misleading. Because users' transaction costs, in terms of time and effort expended, can present a major barrier to customers exercising choices, carriers' choice mechanisms must also be easy to use, ensuring that customers can readily exercise their privacy rights.

**70 230. We encourage but do not require carriers to make available a customer-facing dashboard. While a customer-facing dashboard carries a number of advantages, we are mindful of the fact that it may not be feasible for certain carriers, particularly small businesses, and that improved technologies and user interfaces may lead to better options.[649] Preserving this flexibility benefits both carriers and customers by enabling carriers to adopt a mechanism that suits the customer's abilities and preferences and the carrier's technological capabilities. As noted, we are particularly mindful of the needs of smaller carriers. For example, WTA explains that "[a] privacy dashboard as envisioned in the NPRM would require providers to aggregate information that is likely housed today on multiple systems and develop both internal and external user interfaces."[650] ACA adds that creating a privacy dashboard would be a "near-impossible task" for small BIAS providers.[651] Particularly in light of the concerns expressed by small providers and their representatives, we decline to mandate that BIAS providers make available a customer-facing dashboard.

231. *Timing to Implement Choice*. We require carriers to give effect to a customer's grant, denial, or withdrawal of approval "promptly."[652] Aside from the ordinary time that might be required for *14005 processing incoming requests, customers must be confident that their choices are being respected. The flexibility of this standard enables carriers to account for the relative size of the carrier, the type and amount of customer PI being used, and the particular use or sharing of the customer PI.[653] Since the carrier process and technical mechanics of implementing a customer denial of approval for a new use may well differ from implementing a customer's denial of a previously approved practice, we do not expect that the time frames for each will

necessarily be the same.[654] The Commission has long held this interpretation to be consistent with the language and design of Section 222.[655]

232. *Choice Persistence*. As in our existing rules and as proposed in the *NPRM*, we require a customer's choice to grant or deny approval for use of her customer PI to remain in effect until a customer revokes or limits her choice.[656] We find that customers reasonably expect that their choices will persist and not be changed without their affirmative consent (in the case of sensitive customer PI and previously collected non-sensitive customer PI) or at least the opportunity to object (in the case of yet to be collected non-sensitive customer PI).

233. *Small Carriers*. Some small carriers expressed concern on the record that their websites do not allow for customers to manage their accounts, and thus could not offer an in-browser way for customers to immediately exercise their privacy choices on the carriers' websites.[657] Since we decline to require a specific format for accepting customer privacy choices, any carriers, including small carriers, that lack choice mechanisms that customers can operate directly from the carrier's website or app may be able to accept customer preferences by providing on their websites, in their apps, and any functional equivalents, an email address, 24-hour toll-free phone number, or other easily accessible, persistently available means to exercise their privacy choices.

5. Eliminating Periodic Compliance Documentation

****71** 234. We eliminate the specific compliance recordkeeping and annual certification requirements in Section 64.2009 for voice providers. Eliminating these requirements reduces burdens for all carriers, and particularly small carriers, which often may not need to record approval if they do not use or share customer PI for purposes other than the provision of service.[658] We find that carriers are likely to keep records necessary to allow for any necessary enforcement without the need for specific requirements, and that notifications of data breaches to customers and to enforcement agencies (including the Commission) will ensure compliance with the rules and a workable level of transparency for customers.

***14006 E. Reasonable Data Security**

235. In this section, we adopt a harmonized approach to data security that protects consumers' confidential information by requiring BIAS providers and other telecommunications carriers to take reasonable measures to secure customer PI. The record reflects broad agreement with our starting proposition that strong data security practices are crucial to protecting the confidentiality of customer PI.[659] There is also widespread agreement among industry members, consumer groups, academics, and government entities about the importance of flexible and forward-looking reasonable data security practices.[660]

236. In the *NPRM* we proposed rules that included an overarching data security expectation and specified particular types of practices that providers would need to implement to comply with that standard, while allowing providers flexibility in implementing the proposed requirements (e.g., taking into account, at a minimum, the nature and scope of the provider's activities and the sensitivity of the customer PI held by the provider). Based on the record in this proceeding, we have modified the overarching data security standard to more directly focus on the reasonableness of the providers' data security practices. Also based on the record, we decline to mandate specific activities that providers must undertake in order to meet the reasonable data security requirement. We do, however, offer guidance on the types of data security practices we recommend providers strongly consider as they seek to comply with our data security requirement—recognizing, of course, that what constitutes ““reasonable” data security is an evolving concept.

237. The approach we take today underscores the importance of ensuring that providers have robust but flexible data security practices that evolve over time as technology and best practices continue to improve. It is consistent with the FTC's body of work on data security,[661] the NIST Cybersecurity Framework (NIST CSF),[662] the Satellite and Cable Privacy Acts,[663] and the

CPBR,[664] and finds broad support in the record.[665] In harmonizing the rules for BIAS providers and other telecommunications carriers we apply this more flexible and future-focused standard to voice providers as well, replacing the ***14007** more rigid data security procedures codified in the existing rules and thus addressing the potential that these existing procedures are both under- and over-inclusive—with the expectation that strong and flexible, harmonized, forward-looking rules will benefit consumers and industry.

1. BIAS and Other Telecommunications Providers Must Take Reasonable Measures to Secure Customer PI

****72** 238. The rule that we adopt today requires that every BIAS provider and other telecommunications carrier take reasonable measures to protect customer PI from unauthorized use, disclosure, or access. To comply with this requirement, a provider must adopt security practices appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider, and technical feasibility.[666]

239. As we observed in the *NPRM*, privacy and security are inextricably linked.[667] Section 222(a) imposes a duty on telecommunications carriers to "protect the confidentiality of proprietary information of and relating to ... customers."[668] Fulfilling this duty requires a provider to have sound data security practices.[669] A telecommunications provider that fails to secure customer PI cannot protect its customers from identity theft or other serious personal harm, nor can it assure its customers that their choices regarding use and disclosure of their personal information will be honored. As commenters point out, contemporary data security practices are generally oriented toward "confidentiality, integrity, and availability,"[670] three dynamic and interrelated principles typically referred to together as the "CIA" triad.[671] Confidentiality refers specifically in this context to protecting data from unauthorized access and disclosure;[672] integrity refers to protecting information from unauthorized modification or destruction;[673] and availability refers to providing authorized users with access to the information when needed.[674] We ***14008** agree with NTCA that confidentiality, integrity and availability are best understood as " elements of a single duty" to secure data, and their collective purpose is to " illustrate the various considerations that must be engaged when the management of confidential information is considered."[675] The record confirms that these are core principles that underlie the modern-day practice of data security.[676] Thus, we expect providers to take these principles into account when developing, implementing, and monitoring the effectiveness of adopted measures to meet their data security obligation.

240. By requiring providers to take reasonable data security measures, we make clear that providers will not be held strictly liable for all data breaches.[677] Instead, we give providers significant flexibility and control over their data security practices while holding these practices to a standard of reasonableness that respects context and is able to evolve over time. There is ample precedent and widespread support in the record for this approach. FTC best practices guidance advises companies to "make reasonable choices" about data security,[678] and in numerous cases the FTC has taken enforcement action against companies for failure to take "reasonable and appropriate" steps to secure customer data.[679] Many states also have laws that require regulated entities to take "reasonable measures" to protect the personal data they collect.[680] The CPBR reaffirms this standard, directing companies to "establish, implement and maintain safeguards reasonably designed to ensure the security of" personal customer information.[681] Placing the responsibility on companies to develop and manage their own security practices is also a core tenet of the NIST CSF.[682] A diverse range of commenters in this proceeding support adoption of a data security requirement for BIAS providers that is consistent with these ***14009** principles.[683] Indeed, several providers acknowledge the importance of and need for reasonable data security.[684]

****73** 241. By clarifying that our standard is one of "reasonableness" rather than strict liability, we address one of the major concerns that providers— including small providers and their associations—raise in this proceeding.[685] WTA, for instance, argues that a strict liability standard "is particularly inappropriate for small providers that lack the resources to install the

expensive and constantly evolving safeguards necessary to comply with a strict liability regime."[686] We agree with these parties, and others such as the Federal Trade Commission staff,[687] that our rules should focus on the reasonableness of the providers' practices and not hold providers, including smaller providers, to a standard of strict liability.

242. We also agree with those commenters that argue that the reasonableness of a provider's data security practices will depend significantly on context.[688] The rule therefore identifies four factors that a provider must take into account when implementing data security measures: the nature and scope of its activities; the sensitivity of the data it collects; its size; and technical feasibility. Taken together, these factors give considerable flexibility to all providers. No one factor, taken independently, is determinative.

243. We include "size" in part based on the understanding in the record that smaller providers employ more limited data operations in comparison to their larger provider counterparts. While the other contextual factors already account considerably for the varying data collection and usage practices of providers of different sizes, we agree with commenters that size is an independent factor in what practices are reasonable for smaller providers, particularly to the extent that the smaller providers engage in limited data usage practices.[689] For instance, WTA explains that "its members do not currently, and have no plans to, retain customer Internet browsing histories and related information on an individual subscriber basis because the cost ... would significantly outweigh any potential monetary benefit derived from data ***14010** relating to the small subscriber bases of [rural carriers]."[690] Several small provider commenters also point out that many such providers have few employees and limited resources.[691] Accordingly, certain security measures that may be appropriate for larger providers, such as having a dedicated official to oversee data security implementation, are likely beyond the needs and resources of the smallest providers.[692] Our inclusion of "size"" as a factor makes clear that small providers are permitted to adopt reasonable security practices that are appropriate for their businesses.[693] At the same time, we emphasize that all providers must adopt practices that take into account all four contextual factors. For instance, a small provider with very expansive data collection and usage practices could not point to its size as a defense for not implementing security measures appropriate for the "nature and scope" of its operations.[694]

****74** 244. The rule also takes into account the distinction between sensitive and non-sensitive information that underlies our customer approval requirements. Because the protection of both sensitive and non-sensitive customer PI is necessary to give effect to customer choices about the use and disclosure of their information,[695] our data security rule must cover both.[696] At the same time, we decline to require ***14011** "the same, strict data security protections" for all such information.[697] Rather, we direct providers to calibrate their security measures to "the sensitivity of the underlying data."[698] This approach finds broad support in the record[699] and is consistent with FTC guidance and precedent.[700] Similarly, our inclusion of "technical feasibility" as a factor makes clear that reasonable data security practices must evolve as technology advances.[701] Because our rule gives providers broad flexibility to consider costs when determining what security measures to implement over time, we do not find it necessary to include "cost of security measures" as a separate factor as AT&T and other commenters propose.[702] This means that every provider must adopt security measures that reasonably address the provider's data security risks.

245. In their comments, the National Consumers League recommended that we establish data security threshold requirements that providers could build on, but not fall below.[703] We find that unnecessary in light of the rules we adopt today. We believe that the flexible and forward-looking rule we adopt combined with the discussion that follows regarding exemplary practices makes clear that the rule sets a high and evolving standard of data security.[704] A provider that fails to keep current with industry best practices and other relevant guidance in designing and implementing its data security practices runs the risk of both a preventable data breach and that it will be found out of compliance with our data security rule. We also observe that we have already acted in multiple instances to enforce carriers' broad statutory obligations to take reasonable precautions to protect sensitive customer information.[705] In the *TerraCom* proceeding, for instance, we took action against a carrier under Section 222 of the Act for its failure to employ "appropriate security measures" to protect customers' Social Security numbers and other data from exposure on the public Internet.[706] Moreover, in *TerraCom* and other data security enforcement proceedings, parties

have agreed to detailed data security obligations on individual carriers as conditions of settlement.[707] For example, as part of one consent decree entered into ***14012** by AT&T and the Commission's Enforcement Bureau, AT&T agreed to develop and implement a compliance plan aimed at preventing recurrence of a major data security lapse.[708] We have the ability to pursue similar remedial conditions in the context of any enforcement proceeding that may arise under the data security rule we adopt today, based on the facts of the case.

****75** 246. In addition, the flexibility we have built into our rule addresses concerns about potential conflict with the NIST Cybersecurity Framework (NIST CSF) and with other initiatives to confront data security as well as broader cyber threats.[709] The Commission values the NIST CSF and has demonstrated its commitment to promoting its adoption across the communications sector,[710] and we have accordingly fashioned a data security rule that closely harmonizes with the NIST CSF's flexible approach to risk management. The rule gives providers ample flexibility to implement the NIST CSF on a self-directed basis, and it imposes on BIAS providers a standard for data security similar to that which governs edge providers and other companies operating under the FTC's general jurisdiction.[711] We also reject any suggestions that our rule will impinge on BIAS providers' efforts to improve Internet security or protect their customers from malware, phishing attacks, and other cyber threats.[712] Indeed, protecting against such attacks and threats will only bolster a company's claims that it has reasonable data security practices. Moreover, as explained above, the rules adopted in this Report and Order do not prohibit or impose any constraint on cyber threat information sharing that is lawfully conducted pursuant to the Cybersecurity Information Sharing Act of 2015 (CISA).[713] Indeed, we believe that information sharing is a vital part of promoting data security across the industry.

247. Finally, we recognize that there is more to data security than the steps each individual provider takes to secure the data it possesses. For instance, effective consumer outreach and education can empower customers to be pro-active in protecting their own data from inadvertent or malicious disclosures. We also encourage providers to continue to engage constructively with the Commission, including through the CSRIC and related efforts, to develop and refine data security best practices. Also, as carriers develop and manage their security practices, we encourage them to be forward-looking. In particular, carriers should make efforts to anticipate future data security threats and proactively work to mitigate future risk drivers.

2. Practices That Are Exemplary of Reasonable Data Security

248. While we do not prescribe specific practices that a provider must undertake to comply with our data security rule, the requirement to engage in reasonable data security practices is set against a ***14013** backdrop of existing privacy and data security laws,[714] best practices,[715] and public-private initiatives.[716] Each of these is a potential source of guidance on practices that may be implemented to protect the confidentiality of customer PI. For the benefit of small providers, and others, below we discuss in more detail an evolving set of non-exclusive practices that we consider relevant to the question of whether a provider has complied with the requirement to take reasonable data security measures. While certain of these practices were originally proposed as minimum data security requirements,[717] we discuss them here as part of a set of practices that we presently consider exemplary of a reasonable and evolving standard of data security. We agree with commenters that dictating a minimum set of required practices could foster a "compliance mindset" that is at odds with the dynamic and innovative nature of data security.[718] Providers with less established data security programs may interpret such requirements as a checklist of what is required to achieve reasonable data security, an attitude we seek to discourage. We also seek to avoid codifying practices as the state of the art continues to rapidly evolve.[719] Our approach places the responsibility on each provider to develop and implement data security practices that are reasonable for its circumstances and to refine these practices over time as circumstances change.[720] Rather than mandate what these practices must entail, we provide guidance to assist each provider in achieving reasonable data ***14014** security on its own terms. Taking this approach will also allay concerns that overly prescriptive rules would frustrate rather than improve data security.[721]

****76** 249. While providers are not obligated to adopt any of the practices we suggest, we believe that together they provide a solid foundation for data security that providers can modify and build upon as their risks evolve and, as such, the presence and implementation of such practices will be factors we will consider in determining, in a given case, if a provider has complied with the reasonable data security requirement. However, these practices do not constitute a "safe harbor." A key virtue of the flexible data security rule we adopt today is that it permits data security practices to evolve as technology advances and new methods and techniques for data security come to maturity. We are concerned that any fixed set of security practices codified as a safe harbor would fail to keep pace with this evolutionary process.[722] The availability of a safe harbor may also discourage experimentation with more innovative data security practices and techniques. While it may be possible to construct a safe harbor "with concrete requirements backed by vigorous enforcement"[723] that also takes the evolution of data security practices into account, we find no guidance in the record on how to do so in a workable fashion. Accordingly, our approach is to evaluate the reasonableness of any provider's data security practices on a case-by-case basis under the totality of the circumstances, taking into account the contextual factors that are part of the rule. This approach is well-grounded in precedent[724] and will provide sufficient guidance to providers.[725] Our ***14015** approach to data security also mirrors the FTC's, under which the reasonableness of an individual company's data security practices is assessed against a background of evolving industry guidance.[726] The CPBR also takes a similar approach.[727]

250. *Engagement with Industry Best Practices and Risk Management Tools*. We encourage providers to engage with and implement up-to-date and relevant industry best practices, including available guidance on how to manage security risks responsibly. One powerful tool that can assist providers in this respect is the NIST CSF, which many commenters endorse as a voluntary framework for cyber security and data security risk management.[728] We agree that proper implementation of the NIST CSF, as part of a provider's overall risk management, would contribute significantly to reasonable data security, and that use of the NIST CSF can guide the implementation of specific data security practices that are within the scope of that framework.[729] We encourage providers to consider use of the NIST CSF, as the widespread adoption of this common framework permits the Commission to optimize its engagement with the industry. That said, we clarify that use of the NIST CSF is voluntary, and providers retain the option to use whatever risk management approach best fits their needs. In addition, we encourage providers to look to guidance from the FTC,[730] as well as materials that have been issued to guide the implementation of data security requirements under HIPAA, GLBA, and other relevant statutory frameworks.[731] Finally, we note that a Commission multi-stakeholder advisory body, the Communications Security, Reliability, and Interoperability Council (CSRIC), has produced a rich repository of best practices on various aspects of communications security[732] as well as alerting the Commission of useful activities for which Commission leadership can effectively convene stakeholders to address industry-wide risk factors. In particular, CSRIC has developed voluntary mechanisms by which the communications industry can address cyber risk, based upon the NIST CSF. Many providers and ***14016** industry associations that have participated in this proceeding are active contributors to the CSRIC's work.[733] We encourage providers to consider implementation of the CSRIC best practices as appropriate.

****77** 251. *Strong Accountability and Oversight*. Strong accountability and oversight mechanisms are another factor we consider exemplary of reasonable data security. As an initial matter, we agree with the FTC that the development of a written comprehensive data security program is a practice that is a best practice in promoting reasonable data security. As the FTC explains, putting a data security program in writing can "permit internal and external auditors to measure the effectiveness of the program and provide for continuity as staff members leave and join the team."[734] A written security program can also reinforce the specific practices a provider implements to achieve reasonable data security.

252. A second accountability mechanism that helps a company engage in reasonable data security is the designation of a senior management official or officials with personal responsibility over and accountability for the implementation and maintenance of the provider's data security practices as well as an official responsible for its privacy practices.[735] Companies that take this step are advised to couple designation of corporate privacy and security roles and responsibilities with effective interaction with

Boards of Directors (or, for firms without formal Board oversight, such other structure governing the firm's risk management and oversight), to provide a mechanism for including cyber risk reduction expense within overall risk management plans and resource allocations. That said, we do not specify the qualifications or status that such an official would need to possess, and we recognize that for a smaller provider these responsibilities may rest with someone who performs multiple functions or may be outsourced.[736] Another practice that is indicative of reasonable data security is training employees and contractors on the proper handling of customer PI.[737] Employee training is a longstanding component of data security under the Commission's existing rules.[738] We encourage providers to seek out expert guidance and best practices on the design and implementation of efficacious training programs.[739] Finally, accountability and oversight are also relevant in the context of sharing customer PI with third parties. We agree with commenters that providers must take reasonable steps to promote the safe handling of customer PI they share with third parties.[740] Perhaps the most straightforward means of achieving this accountability is to obtain data security commitments from the third party as a condition of the disclosure.[741] We also remind providers that they are directly accountable for the acts and omissions ***14017** of their agents, including independent contractors, for the entirety of the data lifecycle. This means that the acts and omissions of agents will be taken into account in assessing whether a provider has engaged in reasonable data security practices.[742]

253. *Robust Customer Authentication*. The strength of a provider's customer authentication practices also is probative of reasonable data security. We have recognized that there is no single approach to customer authentication that is appropriate in all cases, and authentication techniques and practices are constantly evolving.[743] That said, the record documents some discernable trends in this area that we would currently expect providers to take into account.[744] For instance, we encourage providers to consider stronger alternatives to relying on rudimentary forms of authentication like customer-generated passwords or static security questions.[745] Providers may also consider the use of heightened authentication procedures for any disclosure that would place a customer at serious risk of harm if the disclosure were improperly made.[746] In addition, we encourage providers to periodically reassess the efficacy of their authentication practices and consider possible improvements.[747] Another practice we encourage providers to consider is to notify customers of account changes and attempted account changes. These notifications provide a valuable tool for customers to monitor their own accounts' security.[748] Providers that implement them should consider the potential for "notice fatigue" in determining how often and under what circumstances these notifications are sent.

****78** 254. *Other Practices*. The record identifies other practices that we encourage providers to consider when implementing reasonable security measures. For instance, several commenters cite the importance of "data minimization," which involves thinking carefully about what data to collect, how long to retain it, and how to dispose of it securely.[749] The principle of data minimization is also embodied in FTC guidance,[750] in the CPBR,[751] and in the Satellite and Cable Privacy Acts.[752] We encourage ***14018** providers to look specifically to the FTC's "Disposal Rule" for guidance on the safe destruction and disposal of customer PI.[753] We also encourage providers to consider data minimization practices that apply for the entirety of the data lifecycle, from collection to deletion. In addition, several commenters recommend strong data encryption,[754] another practice that the FTC advises companies to consider.[755] We agree with commenters that technologically sound data encryption can significantly improve data security, in part by minimizing the consequences of a breach.[756] Finally, we believe that the lawful exchange of information regarding cyber incidents and threats is relevant to promoting data security, and encourage providers to consider engagement in established information sharing practices.

255. The exemplary practices discussed above are not an exhaustive list of reasonable data security practices. A provider that implements each of these practices may still fall short of its data security obligation if there remain unreasonable defects in its protection of the confidentiality of customer PI. Conversely, a provider may satisfy the rule without implementing each of the listed practices. The key question is whether a provider has taken reasonable measures to secure customer PI, based on the totality of the circumstances. In taking this approach, we acknowledge that the adoption of more prescriptive, bright-line requirements could offer providers greater certainty as to what reasonable data security requires. Yet virtually all providers

that have addressed the issue—including small providers and their associations—oppose such requirements.[757] Rather, these providers prefer the approach we have taken in this Report and Order, i.e., the adoption of a "reasonableness" standard that mirrors the FTC's.[758] Also like the FTC, we have provided the industry with guidance on how to achieve reasonable data security in compliance with our rule. We anticipate building upon this guidance over time as data security practices evolve and with them the concept of reasonable data security.

3. Extension of the Data Security Rule to Cover Voice Services

256. In light of the record, we conclude that harmonization of the data security requirements that apply to BIAS and other telecommunications services is the best option for providers and consumers alike. Accordingly, we extend to voice services the data security rule we have adopted for BIAS.[759] This data security rule replaces the more inflexible data security requirements presently codified in Part 64 of the rules.[760]

****79** 257. There are many reasons to harmonize the data security requirements that apply to BIAS and voice services. As an initial matter, many providers offer services of both kinds and often sell them together in bundled packages.[761] We agree with commenters that argue that applying different security requirements to the two kinds of services may confuse customers and add unnecessary complexity to ***14019** providers' data security operations, which may be particularly burdensome for smaller providers.[762] In addition, the evidence suggests that the data security requirements of the existing rules no longer provide the best fit with the present and anticipated communications environment. For instance, expert commentary on the topic of robust customer authentication indicates that this is a complex area where providers need flexibility to adapt their practices to new threats.[763] The highly specific procedures outlined in the existing voice rules are incongruous with this approach to customer authentication.[764]

258. Moreover, retaining the prescriptive data security rules that apply to voice services could impede the development and implementation of more innovative data security measures for BIAS. Providers subject to both sets of rules may determine that the easiest and most cost-effective path to compliance is to adopt for both services the more rigid data security practices that the voice rules require.[765] Such an outcome would contravene our intent to establish a robust and flexible standard for BIAS data security that evolves over time.

259. Accordingly, we find that the best course is to replace the data security rules that currently govern voice services with the more flexible standard we are adopting for BIAS. We find that the rule as written is sufficiently broad to cover BIAS and other telecommunications services. We also clarify that the exemplary practices we discuss above may be implemented differently depending on the services an entity provides. For instance, data security best practices that pertain specifically to broadband networks or services may or may not be relevant in the context of providing voice services.

260. In harmonizing the data security rules for voice services and BIAS, we acknowledge that voice providers have operated for many years under the existing rules and have tailored their data security practices accordingly. We do not expect any provider to revamp its data security practices overnight. On the contrary, as explained below, we are adopting an implementation schedule that affords providers ample time to bring their practices into compliance with the new rules.[766]

F. Data Breach Notification Requirements

261. In this section we adopt rules requiring BIAS providers and other telecommunications carriers to notify affected customers, the Commission, the FBI, and the Secret Service of data breaches unless the provider reasonably determines that no harm to customers is reasonably likely to occur.[767] For purposes of these rules, we define a breach as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information. The record clearly demonstrates that data breach notification plays a critical role in protecting the confidentiality of customer

PI. An obligation to notify customers and law enforcement agencies when ***14020** customer data is improperly accessed, used, or disclosed incentivizes carriers to adopt strong data security practices.[768] Breach notifications also empower customers to protect themselves against further harms, help the Commission identify and confront systemic network vulnerabilities, and assist law enforcement agencies with criminal investigations. At the same time, unnecessary notification can cause notice fatigue, erosion of consumer confidence in the communications they receive from their provider, and inflated compliance costs. The approach we adopt today finds broad support in the record and will maximize the benefits of breach notification as a consumer protection and public safety measure while avoiding unnecessary burdens on providers and their customers. Furthermore, our approach is consistent with how federal law enforcement agencies, such as the FBI and Secret Service, conduct and coordinate data breach investigations.

****80** 262. First, we address the circumstances that will obligate BIAS providers and other telecommunications carriers to notify the Commission, federal law enforcement agencies, and customers of data breaches.[769] This includes a discussion of two related elements adopted today: the harm-based notification trigger and the updated definition for "breach." We then address the requirements that BIAS providers and other telecommunications carriers must follow for providing notice to the Commission and other federal law enforcement. Next, we describe the specific notification requirements that BIAS providers and other telecommunications carriers must follow in providing data breach notifications to customers, including: the required timing for sending notification; the necessary contents of the notification; and the permissible methods of notification. We then discuss the data breach record retention requirements. Finally, we explain our decision to adopt rules that harmonize data breach requirements for BIAS providers and other telecommunications carriers.

1. Harm-Based Notification Trigger

263. We require breach notification unless a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. We do so to enable customers to receive the data breach notifications that they need to take steps to protect themselves, and to provide the Commission, the FBI, and Secret Service with the information they need to evaluate the efficacy of data security rules as well as detect systemic threats and vulnerabilities. In the *NPRM* we sought comment on what should trigger data breach notification, and based on the record, we conclude that the trigger most suitable for our purposes is one based on the potential for customer harm.[770] Among its many benefits, this harm-based trigger will avoid burdening providers and customers alike with excessive notifications, and it will allow providers the flexibility to focus limited resources on data security and ameliorating customer harms resulting from data breaches rather than on notifications that have minimal benefit to customers.[771] The record reflects various harms inherent in unnecessary notification, including notice fatigue,[772] erosion of consumer confidence in the communications they receive from their provider,[773] and ***14021** compliance costs.[774] The harm-based notification trigger we adopt addresses these concerns, by limiting the overall volume of notifications sent to customers and eliminating correspondence that provides minimal or no customer benefit.

264. Our harm-based trigger has a strong basis in existing state data breach notification frameworks.[775] The triggers employed in these laws vary from state to state, but in general they permit covered entities to avoid notifying customers of breaches where the entity makes some determination that the breach will not or is unlikely to cause harm.[776] Likewise, the FTC "supports an approach that requires notice unless a company can establish that there is no reasonable likelihood of economic, physical, or other substantial harm."[777] Our rule similarly requires the carrier to reasonably determine that no harm to ***14022** customers is reasonably likely to occur. As such, we disagree with commenters arguing that standards based on determinations of harm leave consumers more vulnerable to that harm.[778] On the contrary, the record, and the many state laws addressing data breach notifications, demonstrate that providers have ample experience determining a likelihood of harm.[779] Additionally, the reasonableness standard that applies to both the carrier's evaluation and the likelihood of harm adds an objective component to these determinations.

**81 265. Further, the harm-based trigger places the burden on a carrier that detects a breach to reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. This responds to concerns such as AAJ's that it is "frequently impossible" for a carrier to immediately discern the full scope and ramifications of a breach.[780] Our harm-based trigger does not relieve a carrier of its notification obligation simply by virtue of its failure or inability to ascertain the harmful effects of a breach. Rather, carriers must take the investigative steps necessary to reach a reasonable determination that no such harm is reasonably likely. Where a carrier's investigation of a breach leaves it uncertain whether a breach may have resulted in customer harm, the obligation to notify remains. By contrast, requiring customer notification *only when* a provider determines the presence of some risk of harm would create perverse incentives not to carefully investigate breaches.[781]

266. In adopting a harm-based trigger, we clarify that its scope is not limited to "easily recognized financial harm."[782] In the *NPRM*, we acknowledged that "harm" is a concept that can be broadly construed to encompass "financial, physical, and emotional harm."[783] We conclude that the same construction of harm is appropriate for our final breach notification rule. This decision is consistent with the fundamental premise of this proceeding that customer privacy is about more than protection from economic harm. The record demonstrates that commenters' privacy concerns stem from more than just avoiding financial harms.[784] As such, we disagree with commenters who assert that financial loss or identity theft should be the primary metrics for determining the level of harm or whether harm exists at *14023 all.[785] Some commenters have called "for the FCC to help determine how organizations can better respond to breaches in which personal, non-financial data is breached."[786] We find that within the meaning of Section 222(a), threats to the "confidentiality" of customer PI include not only identity theft or financial loss but also reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal details.[787]

267. Relatedly, we establish a rebuttable presumption that any breach involving sensitive customer PI presumptively poses a reasonable likelihood of customer harm and would therefore require customer notification. This rebuttable presumption finds a strong basis in the record.[788] Even commenters that favor minimal breach reporting generally concede that customers are entitled to notification when their most sensitive information is misused or disclosed.[789] The presumption also aligns with our decision to base the level of customer approval required for use or disclosure of customer PI on whether the PI is sensitive in nature. As we explain above, this distinction upholds the widespread expectation that customers should be able to maintain particularly close control over their most sensitive personal data.[790] While breaches of sensitive customer PI often present severe risks of concrete economic harm,[791] there is a more fundamental harm that comes from the loss of control over information the customer reasonably expects to be treated as sensitive.

**82 268. We also find that our employing a harm-based trigger will substantially reduce the burdens of smaller providers in reporting breaches of customer PI.[792] We agree with commenters stating that a framework—such as ours—that allows providers to assess the likelihood of harm to their customers will ultimately be less costly and "will not overburden small providers."[793] The record indicates that smaller providers tend to collect and use customer data, including sensitive information, far less *14024 extensively than larger providers.[794] More modest collection and usage of customer PI leaves a provider less prone to breaches that would trigger a data breach notification obligation under our rule.

269. Finally, we clarify that our harm-based notification trigger applies to breaches of data in an encrypted form. Whether a breach of encrypted data presents a reasonable likelihood of harm will depend in significant part on the likelihood that unauthorized third parties reasonably would be expected to be able to decrypt the data.[795] Factors that make decryption more or less likely are therefore relevant in determining whether a reasonable likelihood of customer harm is present in such instances. These factors may include the quality of the encryption and whether third parties can access the encryption key. Ultimately, a provider must notify affected customers if it cannot reasonably determine that a breach poses no reasonable likelihood of harm, regardless of whether the breached data is encrypted.

270. With our adoption of a harm-based trigger, we have removed the need for a separate trigger based on intent. Thus, for purposes of these rules, we adopt the definition of breach that we proposed in the *NPRM* and define a breach as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information. This definition is broader than the definition in our existing rules, which includes an intent element, and only applies to breaches of CPNI, in recognition that the record indicates that the relevant factor for breach reporting is not intent, but effect on the customer.[796]

271. We agree with other commenters that inadvertent breaches can be just as severe and harmful for consumers as intentional breaches,[797] and consumers are likely to care about serious breaches even when they occur by accident or mistake.[798] Moreover, whether or not a breach was intentional may not always be immediately apparent.[799] By defining breach to include unintentional access, use, or disclosure we ensure that in the event of a breach the provider has an incentive to investigate the cause and effect of the breach, and the opportunity to respond appropriately. Some commenters recommend that the definition of breach include an intent element to avoid equating inadvertent disclosure of customer PI to an employee or contractor of a provider with intentional hacking of customer records.[800] ***14025** The adoption of a harm-based trigger—in lieu of a trigger based on intent—creates a consistent obligation to report breaches that may harm consumers, regardless of the source or cause of the breach.

****83** 272. Commenters also argue that including an intent element in the definition of breach would prevent excessive data breach notifications.[801] Commenters making this argument raise the prospect of a flood of notifications for breaches that have no impact on the consumer, including such good-faith errors as an employee inadvertently accessing the wrong database.[802] We share their general concern about the risk of over-notification—it is costly to providers, without corresponding benefit to consumers, and can lead to notice fatigue and possibly consumer de-sensitization. However, in this context the argument is misplaced. Identifying a data breach is only the first step towards determining whether data breach notification is necessary. The harm-based trigger that we adopt today relieves a provider from notifying its customers and government agencies of breaches that result from minor mistakes that create no risk of harm to the affected customers. Based on this analysis, we find eliminating the word "intentionally" from our breach definition equally warranted for all telecommunications carriers.

273. Our adoption of a harm-based trigger also addresses concerns about the breadth of our breach definition. For example our definition includes incidents where a person gains unauthorized access to customer PI but makes no further use of the data.[803] We agree with AAJ that we must account for the difficulties a provider faces in determining when "access translates to acquisition and when acquisition leads to misuse."[804] Our rule appropriately requires providers to issue notifications in cases where a provider is unable to determine the full scope and impact of a breach. However, the definition of breach does not create an obligation to notify customers of an unauthorized gain of access—such as an employee opening the wrong file— once the provider reasonably determines that no harm is reasonably likely to occur. This accords with AT&T, which explains that "not requiring notification where a provider determines that there is no reasonable likelihood of harm to any customer resulting from the breach" will "reduce excessive reporting."[805]

274. Similarly, our harm-based trigger allays the concern that extending breach notification obligations beyond CPNI to customer PI more broadly would vastly expand the range of scenarios where notification is required.[806] This concern is largely premised on the assumption that we would require customer notification of all breaches of customer PI, regardless of the severity of the breach or the sensitivity of the PI at issue. As explained above, we have instead adopted a more targeted obligation that takes into account the potential for customer harm. In addition, we observe that many, if not all, state data breach notification requirements explicitly include sensitive categories of PII within their scope.[807] ***14026** Under our rule, breaches involving such information would presumptively meet our harm trigger and thus require notification. We think it is clear that the unauthorized exposure of sensitive PII, such as Social Security numbers or financial records, is reasonably likely to pose a risk of customer harm, and no commenter contends otherwise. We therefore find it appropriate for our breach notification rule to apply broadly to customer PI, including PII.

2. Notification to the Commission and Federal Law Enforcement

****84** 275. In this section, we describe rules requiring telecommunications carriers to notify the Commission and federal law enforcement of breaches of customer PI, under the harm-based notification trigger discussed above. We also specify the timeframe and methods by which providers must provide this information.

276. *Scope*. As proposed in the *NPRM*, we require notification to the Commission of all breaches that meet the harm-based trigger and, when the breach affects 5,000 or more customers, the FBI and Secret Service. We expect that this notification data will facilitate dialogue between the Commission and telecommunications carriers, and will prove extremely valuable to the Commission in evaluating the efficacy of its data security rules, as well as in identifying systemic negative trends and vulnerabilities that can be addressed with individual providers or the industry as a whole including to further the goal of collaborative improvement and refinement of data security practices.[808] Still, we retain discretion to take enforcement action to ensure BIAS providers and other telecommunications carriers are fulfilling their statutory duties to protect customer information.

277. We adopt an additional trigger of at least 5,000 affected customers for notification to the Secret Service and FBI, in order to ensure that these agencies are not inundated with notifications that are unlikely to have significant law enforcement implications. This threshold finds support in the comments of the FBI and Secret Service[809] and is also consistent with or similar to provisions in various legislative and administration proposals for a federal data breach law.[810] We recognize that there may be circumstances under which carriers want to share breach information that does not meet the harm trigger we adopt today as part of a broader voluntary cybersecurity and threat detection program, and we encourage providers to continue these voluntary efforts.[811]

278. *Timeframe*. The dictates of public safety and emergency response may require that the Commission and law enforcement agencies be notified of a breach in advance of customers and the ***14027** general public.[812] Thus, for breaches affecting 5,000 or more customers, we require carriers to notify the Commission, the FBI, and the Secret Service within seven (7) business days of when the carrier reasonably determines that a breach has occurred, and at least three (3) business days before notifying customers. For breaches affecting fewer than 5,000 customers, carriers must notify the Commission without unreasonable delay and no later than thirty (30) calendar days following the carrier's reasonable determination that a reach has occurred. Both of these thresholds remain subject to the harm-based trigger. We agree with commenters that the timeline for data breach notification should not begin when a provider first identifies suspicious activity.[813] At the same time, we clarify that "reasonably determining" a breach has occurred does not mean reaching a conclusion regarding every fact surrounding a data security incident that may constitute a breach. Rather, a carrier will be treated as having " reasonably determined" that a breach has occurred when the carrier has information indicating that it is more likely than not that there was a breach. To further clarify, the notification timelines discussed herein run from the carrier's reasonable determination that a breach has occurred, not from the determination that the breach meets the harm-based notification trigger.

****85** 279. We agree with the FBI and the Secret Service that advance notification of breaches will enable law enforcement agencies to take steps to avoid the destruction of evidence and to assess the need for further delays in publicizing the details of a breach.[814] We reject arguments that the timeframes for Commission and law enforcement notification that we adopt are too burdensome.[815] Rather, we agree with AT&T and other commenters in the record that allowing carriers seven (7) business days to notify the Commission and law enforcement furnishes those providers with sufficient time to adequately investigate suspected breaches.[816] Further, to address concerns expressed in the record regarding the ***14028** complexity and costs of data breach notification for smaller providers,[817] we relax the notification timeframe for breaches affecting fewer than 5,000 customers. Carriers must notify the Commission of breaches affecting less than 5,000 customers without unreasonable delay and no later than thirty (30) calendar days following the carrier's reasonable determination that a breach has occurred. We find that a 30-day notification timeframe for breaches affecting fewer than 5,000 customers provides the Commission with the data necessary to monitor trends and gain meaningful insight from breach activity across the country, while at the same time reducing and

simplifying the requirements for all carriers, particularly smaller providers, whose limited resources might be better deployed toward remediating and preventing breach activity, particularly in the early days of addressing a relatively small breach.

280. We also recognize that a carrier's understanding of the circumstances and impact of a breach may evolve over time. We expect carriers to supplement their initial breach notifications to the Commission, FBI, and Secret Service, as appropriate.[818] Early notification of breaches will improve the Commission's situational awareness and enable it to coordinate effectively with other agencies, including with the FBI and Secret Service on breaches not reportable directly to these agencies that may nevertheless raise law enforcement concerns. Furthermore, time is of the essence in a criminal investigation.[819] Learning promptly of a significant, large-scale breach gives law enforcement agencies an opportunity "to coordinate their efforts so that any law enforcement response can maximize the resources available to address and respond to the intrusion."[820] Given the vital interests at stake in cases where a data breach merits a law enforcement response, we find that the seven (7) business day reporting deadline for such breaches is necessary as a matter of public safety and national security.

281. To further advance the needs of law enforcement, we permit the FBI or Secret Service to direct a provider to delay notifying customers and the public at large of a breach for as long as necessary to avoid interference with an ongoing criminal or national security investigation.[821] This provision replaces the more prescriptive requirements in the existing rules specifying the timing and methods for law enforcement intervention.[822] Consistent with our overall approach in this proceeding, we adopt rules that incorporate flexibility to account for changing circumstances. Several commenters agree that this provision for law enforcement, which is embodied in the existing rules, remains prudent.[823] We also observe that the laws of several states and the District of Columbia include similar law enforcement delay provisions.[824] We are not persuaded that such a provision unduly interferes with the interests of ***14029** customers in taking informed action to protect themselves against breaches.[825] As the FBI and Secret Service explain, customer notification delays are not routine but are requested as a matter of practice only in "exceptional circumstances" involving a serious threat of harm to individuals or national security.[826] In addition, decisions regarding when to publicly disclose details of a criminal investigation are a matter that lies within the expertise of law enforcement agencies. We therefore find that the best course is to defer to the judgment of the FBI and Secret Service on when the benefits of delaying customer notification outweigh the risks.

****86** 282. *Method*. We will create a centralized portal for reporting breaches to the Commission and other federal law enforcement agencies. The Commission will issue a public notice with details on how to access and use this portal once it is in place. The reporting interface will include simple means of indicating whether a breach meets the 5,000-customer threshold for reporting to the FBI and Secret Service. The creation of this reporting facility will streamline the notification process,[827] reducing burdens for providers, particularly small providers. Any material filed in this reporting facility will be presumed confidential and not made routinely available for public inspection.[828]

3. Customer Notification Requirements

283. In order to ensure that telecommunications customers receive timely notification of potentially harmful breaches of their customer PI, we adopt rules specifying how quickly BIAS providers and other telecommunications carriers must notify their customers of a breach, the information that must be included in the breach notification, and the appropriate method of notification.

a. Timeline for Notifying Customers

284. We require BIAS providers and other telecommunications carriers to notify affected customers of reportable breaches of their customer PI without unreasonable delay, and no later than 30 calendar days following the carriers' reasonable determination that a breach has occurred, unless the FBI or Secret Service requests a further delay.[829] This approach balances affected

customers' need to be notified of potentially harmful breaches of their confidential information with carriers' need to properly determine the scope and impact of the breach, and to the extent necessary, to most immediately focus resources on preventing further breaches. Also, the specific customer notification timeline we adopt has broad record support.[830]

***14030** 285. As an initial matter, we agree with commenters that clear and straightforward notification deadlines are necessary to ensure that customers are timely notified of breaches that affect them.[831] We also agree with commenters that providing more time to notify customers than the 10 days we initially proposed will enable carriers to conduct a more thorough and complete investigation of breaches in advance of the notification.[832] This extra time for investigation will minimize duplicative and incomplete breach notices, avoid customer confusion, allow providers to focus first on stopping further breaches, and minimize burdens on providers.[833] The FBI and Secret Service, which have extensive experience with data breach notification and, more specifically, experience with our existing data breach notification rules, generally support a customer notification timeframe of between 10 and 30 days.[834] FTC staff recommends that breach notifications occur without unreasonable delay, but within an outer limit of between 30-60 days.[835] State data breach laws vary, but most states do not require notification within a specific time frame and the majority of states that do provide 45 days or more to provide notice.[836]

****87** 286. Our adoption of a customer notification period longer than that initially proposed also responds to concerns raised by smaller carriers. For example, the Rural Wireless Association argues that "[s]mall BIAS providers need additional time [beyond ten days] to determine the extent of any breach, as well as to consult with counsel as to the appropriate next steps."[837] The American Cable Association similarly argues that compliance with a compressed notification timeline would require small providers "to divert senior and technical staff solely to data breach response for the duration of the breach response period" and otherwise incur high compliance costs.[838] We are mindful of the compliance burdens that a 10-day period for customer notification would impose on small carriers in particular, and accordingly adopt a more flexible requirement to notify customers of reportable breaches without unreasonable delay and in any event no longer than 30 calendar days. These commenters and others proposed longer notification periods and, alternatively, an open-ended non-specific timeframe for small providers.[839] While we are sensitive to these concerns, we also note, however, that customer exposure to avoidable or ***14031** mitigable risk continues to grow in the aftermath of a breach. We therefore emphasize the value of notifying affected customers as soon as possible to allow the customer to undertake time-sensitive mitigation activities and encourage carriers to notify consumers as soon as practicable.

287. Requiring carriers to notify affected customers without unreasonable delay while adopting a 30 calendar day deadline to do so creates a backstop against excessive delays in notifying customers. Of course, if a telecommunications carrier conducts a good faith, reasonable investigation within 30 calendar days but later determines that the scope of affected customers is larger than initially known, we expect that provider to notify those additional customers as soon as possible.[840] However, based on the record, we find that 30 calendar days is ample time to prepare a customer notification that meets our minimum content requirements, as discussed below.[841] Our prior rules did not specify a precise timeline for customer notice—only that it must occur after the carrier completes law enforcement notification—and we find adoption of the timeline above warranted to ensure timely notification to customers. We recognize that a carrier may identify a breach and later learn that the scope of the breach is larger than initially determined. Under such circumstances a carrier has a continuing obligation to notify without unreasonable delay any additional customers it identifies as having been affected by the breach, to the extent the carrier cannot reasonably determine that no harm is reasonably likely to occur to the newly identified affected customers as a result of the breach.

b. Information Provided as Part of Customer Breach Notifications

****88** 288. To be a useful tool for consumers, breach notifications should include information that helps the customer understand the scope of the breach, the harm that might result, and whether the customer should take any action in response. In the *NPRM*

we proposed that providers include certain types of basic information in their data breach notifications to affected customers, and based on the record, we adopt those same basic requirements,[842] which include the following elements:
· The date, estimated date, or estimated date range of the breach;

· A description of the customer PI that was used, disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed, by a person without authorization or exceeding authorization as a part of the breach of security;

· Information the customer can use to contact the telecommunications carrier to inquire about the breach of security and the customer PI that the carrier maintains about the customer;

· Information about how to contact the Federal Communications Commission and any state regulatory agencies relevant to the customer and the service; and

· If the breach creates a risk of financial harm, information about national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, or credit freezes the telecommunications carrier is offering customers affected by the breach of security.

289. While data breaches are not "one-size-fits-all," creating a measure of consistency across customer breach notifications will benefit customers and providers, particularly smaller providers, by ***14032** removing any need to reinvent the wheel in the event of a data breach. Seventeen states and territories currently mandate that specific content be included in breach notifications and the requirements we adopt today are generally consistent with those statutes.[843] Much of the information we require consists of contact information for the Commission, relevant authorities, credit reporting agencies, and the carrier itself. Based on the record, we also require customer breach notifications to contain information about credit freezes and credit monitoring if the breach creates a risk of financial harm.[844] The foregoing elements should be easy for any provider to ascertain and for customers to understand. The remaining two elements simply define the basic elements of a breach notification—when the breach occurred and what information was breached.[845] Additionally, we hold carriers to a reasonable standard of accuracy and precision in providing this information. Rather than having to provide the exact moment a breach occurred, providers are tasked with giving an "estimated" date or, alternatively, an estimated date "range."" Moreover, while a description of the customer PI involved in the breach should be as detailed, informative, and accurate as possible, the rule allows for a description of the data the telecommunications carrier "reasonably believes"" was used, disclosed, or accessed.

****89** 290. We encourage providers to supplement these minimum elements with additional information that their customers may find useful or informative. For example, FTC Staff recommends that notifications include contact information for the FTC, and a reference to its comprehensive IdentityTheft.gov website.[846] In appropriate cases, providing such additional information could further empower customers to take steps to mitigate their own harm and protect themselves against the effects of any future breaches.

c. Notification Methods

291. As proposed in the *NPRM*, we require that customer notifications occur by means of written notification to the customer's address of record or email address, or by contacting the customer by other electronic means of active communications agreed upon by the customer for contacting that customer for data breach notification purposes. For former customers, we require carriers to issue notification to the customer's last known postal address that can be determined using commonly available sources. These options create flexibility for providers to notify customers in a manner they choose to be contacted by their provider, and they are consistent with methods permitted under other data breach ***14033** notification frameworks.[847] One of the few commenters to address this issue supports the *NPRM* proposal, while also suggesting that providers post "substitute breach notifications" on their websites.[848] While some other breach notification frameworks do include such a requirement,[849]

we are not persuaded it is necessary for our purposes. Telecommunications carriers have direct relationships with their customers through which they are likely to have ready means of contacting them. We believe the options discussed above for direct notification will generally provide a sufficient array of options for reaching customers affected by a breach, and we thus decline also to require a broader, less targeted public disclosure.

4. Record Retention

292. We adopt a streamlined version of the record retention requirement we proposed in the *NPRM*. We require only that providers keep record of the dates on which they determine that reportable breaches have occurred and the dates when customers are notified, and that they preserve written copies of all customer notifications. These records must be kept for two years from the date a breach was reasonably determined to have occurred. The purpose of this limited requirement is to enable Commission oversight of the customer breach notifications our rule requires. This minor recordkeeping requirement will not impose any significant administrative burden on providers.[850] On the contrary, the information that must be retained must be collected anyway, is of limited quantity, and largely comprises information we would expect carriers to retain as a matter of business practice.[851] Moreover, shortening the retention period would weaken the utility of the requirement as an enforcement tool, while not delivering any substantiated cost savings for providers.[852] As a final point, we clarify that we do not require carriers to retain records of breaches that do not rise to the level of a required Commission notification. A large percentage of breaches are therefore likely to be exempted from this requirement.

5. Harmonization

****90** 293. In the *NPRM*, we proposed adoption of a harmonized breach notification rule for BIAS and other telecommunications services that would replace the existing Part 64 rule. Based on the record, we have determined to take this approach. We agree with commenters who argue that creating a harmonized rule will enable providers to streamline their notification processes and will reduce the potential for customer confusion.[853] Moreover, we find that the modifications we have made to the ***14034** proposed rule, particularly the harm trigger we adopt and timeline for notifying customers, ameliorate concerns that applying the new rule to both BIAS and other telecommunications services will unduly increase burdens for voice providers.[854]

G. Particular Practices that Raise Privacy Concerns

294. In this section we prohibit "take-it-or-leave-it" offers in which BIAS providers offer broadband service contingent on customers surrendering their privacy rights as contrary to the requirements of Sections 222, 201, and 202 of the Act. We also adopt heightened disclosure and affirmative consent requirements for BIAS providers that offer customers financial incentives, such as lower monthly rates, in exchange for the right to use the customers' confidential information. Congress has tasked the Commission with protecting the public interest, and we conclude that our two-fold approach to these practices will permit innovative and experimental service offerings and encourage and promote customer choice, while prohibiting the most egregious offerings that would harm the public interest.

1. BIAS Providers May Not Offer Service Contingent on Consumers' Surrender of Privacy Rights

295. We agree with those commenters that argue that BIAS providers should not be allowed to condition or effectively condition the provision of broadband on consenting to use or sharing of a customer's PI over which our rules provide the consumer with a right of approval.[855] Consistent with our proposal in the *NPRM*, we therefore prohibit BIAS providers from conditioning the provision of broadband service on a customer surrendering his or her privacy rights.[856] We also prohibit BIAS providers from terminating service or otherwise refusing to provide BIAS due to a customer's refusal to waive any such privacy rights. By design, such "take-it-or-leave-it" practices offer no choice to consumers. The record supports our finding that such practices will

harm consumers, particularly lower-income customers,[857] and we agree with Atomite that there is a difference between offering consumers "a carrot (i.e., consideration in exchange for property rights) and [] a stick (e.g., no ISP service unless subscribers relinquish their property rights)."[858] We therefore conclude that prohibiting such practices will ensure that consumers will not have to trade their privacy for broadband services.

296. As we discussed above, broadband plays a pivotal role in modern life.[859] We find that a "take-it-or-leave it" approach to the offering of broadband service contingent upon relinquishing customer ***14035** privacy rights is inconsistent with the telecommunications carriers' "duty to protect the confidentiality of proprietary information of, and related to ... customers.""[860] Further, we find that a "take-it-or-leave-it" customer acceptance is not customer "approval" within the meaning of Section 222(c)(1), which prohibits telecommunications carriers from using, disclosing, or permitting access to CPNI without customer approval.[861]

****91** 297. We also conclude that requiring customers to relinquish all privacy rights to their PI to purchase broadband services is an unjust and unreasonable practice within the meaning of Section 201(b).[862] Requiring customers to relinquish privacy rights in order to purchase broadband services, or other telecommunications services, would also constitute unjust and unreasonable discrimination in violation of section 202(a).[863] A take-it-or-leave-it offering would discriminate unreasonably by offering the service to potential customers willing and able to relinquish privacy rights that consumers expect and deserve, and/or that are guaranteed to them under sections 222 and 201, and not offering the service to others. Consumers should not have to face such a choice. In the *2015 Open Internet Order*, we explained that with respect to BIAS services, we will evaluate whether a practice is unjust, unreasonable, or unreasonably discriminatory using the no-unreasonable interference/disadvantage standard (general conduct rule).[864] Under this standard, the Commission can prohibit, on a case-by-case basis, practices that unreasonably interfere with or unreasonably disadvantage the ability of consumers to reach the Internet content, services, and applications of their choosing.[865] In evaluating whether a practice satisfies this rule, we consider a totality of the circumstances, looking to a non-exhaustive list of factors. Among these factors are end-user control, free expression, and consumer protection.

2. Heightened Requirements for Financial Incentive Practices

298. Unlike the "take-it-or-leave-it" offers for BIAS discussed above, the record concerning financial incentives practices is more mixed. There is strong agreement among BIAS providers, some public interest groups, and other Internet ecosystem participants that there are benefits to consumers and ***14036** companies of allowing BIAS providers the flexibility to offer innovative financial incentives.[866] The record does, however, reflect concerns that these programs may be coercive or predatory in persuading consumers to give up their privacy rights.[867] We therefore find that that heightened disclosure and affirmative customer consent requirements will help to ensure that customers' decisions to share their proprietary information in exchange for financial incentives are based on informed consent.[868]

299. As we recognized in the *Broadband Privacy NPRM*, it is not unusual for business to give consumers benefits in exchange for their personal information. For example, customer loyalty programs that track consumer purchasing habits online and in the brick-and-mortar world are commonplace.[869] Moreover, the Internet ecosystem continues to innovate in ways to obtain consumer information such as earning additional broadband capacity, voice minutes, text messages, or even frequent flyer airline miles in exchange for personal information.[870] Discount service offerings can benefit consumers.[871] As MMTC ***14037** explains, for example, such programs "significantly drive online usage"" as well as "help financially challenged consumers."[872]

****92** 300. At the same time, the record includes legitimate concerns that financial incentive practices can also be harmful if presented in a coercive manner, mislead consumers into surrendering their privacy rights, or are otherwise abused.[873] This is particularly true, because as CFC has explained, "consumers have difficulty placing a monetary value on privacy" and

often "have little knowledge of the details or extent of the personally identifiable data that is collected or shared by their BIAS providers and others."[874] Commenters also raise concerns about the potential disproportionate effect on low income individuals.[875] Thirty-eight public interest organizations expressed concern that financial incentives can result in consumers paying up to $800 per year—$62 per month—for plans that protect their privacy.[876]

301. Mindful of the potential benefits and harms associated with financial incentive practices, we adopt heightened disclosure and choice requirements, which will help ensure consumers receive the information they need to fully understand the implications of any such practices and make informed decisions about exchanging their privacy rights for whatever benefits a provider is offering.[877] We therefore require BIAS providers offering financial incentives in exchange for consent to use, disclose, ***14038** and/or permit access to customer PI to provide a clear and conspicuous notice of the terms of any financial incentive program that is explained in a way that is comprehensible and not misleading.[878] That explanation must include information about what customer PI the provider will collect, how it will be used, with what types of entities it will be shared and for what purposes.[879] The notice must be provided both at the time the program is offered and at the time a customer elects to participate in the program. BIAS providers must make financial incentive notices easily accessible and separate from any other privacy notifications and translate such notices into a language other than English if they transact business with customers in that language. When a BIAS provider markets a service plan that involves an exchange of personal information for reduced pricing or other benefits, it must also provide at least as prominent information to customers about the equivalent plan without exchanging personal information.

302. BIAS providers must also comply with all notice requirements in Section 64.2003 of our rules when providing a financial incentive notice.[880] Because of the potential for customer confusion and in keeping with our overarching goal of giving customers control over the use and sharing of their personal information, we further require BIAS providers to obtain customer opt-in consent for participation in any financial incentive program that requires a customer to give consent to use of customer PI.[881] Consistent with the choice framework we adopt today, once customer approval is given, BIAS providers must provide a simple and easy-to-use mechanism that enables customers to change their participation in such programs at any time. This mechanism, which may be the same choice mechanism as the one in Part III.D.4, must be clear and conspicuous and in language that is comprehensible and not misleading. The mechanism must also be persistently available on or through the carrier's website; the carrier's application, if it provides one for account management purposes; and any functional equivalent of either. If a carrier does not have a website, it must provide its customers with a persistently available mechanism by another means such as a toll-free telephone number. We find that the protections outlined herein will encourage consumer choice in evaluating whether to take advantage of financial incentive programs.[882]

****93** 303. We will closely monitor the development of financial incentive practices, particularly if allegations arise that service prices are inflated such that customers are essentially compelled to choose between protecting their personal information and very high prices. We caution that we reserve the right to take action, on a case-by-case basis, under Sections 201 and 222 against BIAS providers engaged in ***14039** financial incentive practices that are unjust, unreasonable, unreasonably discriminatory, or contrary to Section 222. The approach we take today enables BIAS providers the flexibility to experiment with innovative financial incentive practices while ensuring that such practices are neither predatory nor coercive.

H. Other Issues

1. Dispute Resolution

304. In the *Broadband Privacy NPRM* we sought comment on whether our current informal complaint resolution process is sufficient to address customer concerns or complaints with respect to our proposed privacy and data security rules.[883] At present, customers who experience violations of any of our rules may file informal complaints through the Consumer Inquiries and Complaints Division of the Consumer & Governmental Affairs Bureau, and carriers may not require customers to waive, or

otherwise restrict their ability to file complaints with or otherwise contact the Commission regarding violations of their privacy rights.[884] The record does not demonstrate a need to modify our complaint process for purpose of the rules we adopt today.[885]

305. On the question of whether BIAS providers should adopt specific dispute resolution processes, we received significant feedback both in support of[886] and in opposition to[887] limitations on mandatory arbitration agreements. Based on that record, we continue to have serious concerns about the impact on consumers from the inclusion of mandatory arbitration requirements as a standard part of many contracts for communications services. The time has come to address this important consumer protection issue in a comprehensive way. Therefore, we will initiate a rulemaking on the use of mandatory arbitration requirements in consumer contracts for broadband and other communications services, acting on a notice of proposed rulemaking in February 2017. We observe that the Consumer Financial Protection Bureau (CFPB)—which has extensive experience with consumer arbitration agreements and dispute resolution mechanisms—issued a report last year on mandatory arbitration clauses and is currently engaged in a rulemaking on the subject in the consumer finance context.[888] We expect that ***14040** many of the lessons the CFPB learns and the conclusions it draws in its rulemaking will be informative and useful.

2. Privacy and Data Security Exemption for Enterprise Voice Customers

306. Having harmonized the current rules for voice services with the rules we adopt today for BIAS, we revisit and broaden the existing exemption from our Section 222 rules for enterprise voice customers, where certain conditions are met. Specifically, we find that a carrier that contracts with an enterprise customer for telecommunications services other than BIAS need not comply with the other privacy and data security rules under Part 64, Subpart U of our rules if the carrier's contract with that customer specifically addresses the issues of transparency, choice, data security, and data breach; and provides a mechanism for the customer to communicate with the carrier about privacy and data security concerns. As with the existing, more limited business customer exemption from our existing authentication rules, carriers will continue to be subject to the statutory requirements of Section 222 even where this exemption applies.[889]

****94** 307. Our existing voice rules include customer authentication obligations as a required data security practice, but allow business customers to bind themselves to authentication schemes that are different than otherwise provided for by our rules.[890] In adopting an alternative data security option for authenticating business customers, the Commission recognized that the privacy concerns of telecommunications customers are greatest "when using personal telecommunications service,"[891] and "businesses are typically able to negotiate the appropriate protection of CPNI in their service agreements."[892] As Level 3 argues in this rulemaking, business customers have the "knowledge and bargaining power necessary to contract for privacy and data security protections that are tailored to meet their needs."[893] Moreover, business customers may have different privacy and security needs and therefore different expectations.[894] For example, Verizon explains that "many businesses may want their CPNI used in different ways than a typical consumer."[895] Allowing sophisticated enterprise customers to ***14041** negotiate their own privacy and data security protections with their carriers will "allow businesses to tailor how a telecommunications service provider protects their privacy and data specifically to their individual needs""[896] and allow carriers "to compete by offering innovative pro-customer options and contracts that meet business customers' privacy and data security expectations."[897] Although the Commission previously limited the enterprise exemption to authentication, for the reasons above we are convinced to broaden the exemption to encompass all privacy and data security rules under Section 222 for the provision of telecommunications services other than BIAS to enterprise customers.[898]

308. To ensure that business customers have identifiable protections under Section 222, we limit the business customer exemption to circumstances in which the parties' contract addresses the subject matter of the exemption and provides a mechanism for the customer to communicate with the carriers about privacy and data security concerns.[899] The existing exemption applies only if the parties' contract addresses authentication; in light of the broader scope of the exemption we adopt today, we now limit the exemption to circumstances in which the parties' contract addresses transparency, choice, data security,

and breach notification.[900] We reject the contention that we should exempt enterprise services from our rules entirely with regard to the two limitations above.[901] The existence of contractual terms between two businesses addressing privacy ensures that the enterprise customer's privacy is in fact protected without the need for our rules.[902] In this regard, as XO observes, an enterprise carrier would "face significant liability if it violated contractual terms governing privacy and data security."[903] We do not provide a business exemption for BIAS services purchased by enterprise customers, because BIAS services by definition are "mass market retail service[[s]," and as such we do not anticipate that it will be typical for purchasers to negotiate the terms of their contracts.

**95 309. Regardless of whether the exemption applies, we observe that carriers remain subject to the statutory requirements of Section 222. This exemption in our rules is thus not tantamount to forbearance from the statute. We agree with commenters that Section 222 provides a solid legal foundation for carriers and sophisticated business customers to negotiate adequate and effective service terms on matters of privacy and data security.[904]

*14042 **I. Implementation**

310. To provide certainty to customers and carriers alike, in this section we establish a timeline by which carriers must implement the privacy rules we adopt today. Until these rules become effective, Section 222 applies to all telecommunications services, including BIAS, and our current implementing rules continue to apply to telecommunications services other than BIAS and to interconnected VoIP. Below, we explain when the rules we adopt will be effective, and address how carriers should treat customer approvals to use and share customer PI received before the new rules are effective. Finally, we establish an extended implementation period for small providers with respect to the transparency and choice requirements we adopt today.

1. Effective Dates and Implementation Schedule for Privacy Rules

311. Swift implementation of the new privacy rules will benefit consumers. Moreover, carriers that have complied with FTC and industry best practices will be well-positioned to achieve prompt compliance with the privacy rules we adopt today. We recognize, however, that carriers will need some time to update their internal business processes as well as their customer-facing privacy policies and choice mechanisms in order to come into compliance with some of our new rules.[905] Additionally, some of the new rules will require revised information collection approval from the Office of Management and Budget pursuant to the Paperwork Reduction Act (PRA approval), and it is difficult to predict the exact timeline for PRA approval.[906] We therefore adopt a set of effective dates for the new rules that is calibrated to the changes carriers will need to make to come into compliance — providing a minimum timeframe before which the rules could come into effect. In order to provide certainty about effective dates, we also direct the Wireline Competition Bureau (Bureau) to provide advance notice to the public of the precise date after PRA approval when the Commission will begin to enforce compliance with each of the new rules.

312. *Notice and Choice*. The notice and choice rules we adopt today will become effective the later of (1) PRA approval, or (2) twelve months after the Commission publishes a summary of the Order in the Federal Register.[907] We acknowledge that our new notice and choice rules may "represent a significant shift in the status quo" for carriers.[908] Carriers will need to analyze the new, harmonized privacy rules as well as coordinate with various business segments and vendors, and update programs and policies.[909] Carriers will also need to engage in consumer outreach and education. These implementation steps will take time and we find, as supported in the record, that twelve months after publication of the Order in the Federal Register is an adequate minimum implementation period to implement the new notice and approval rules. In order to provide certainty, we also direct the Bureau to release a public notice after PRA approval of the notice and choice rules, indicating that the rules are effective, and giving carriers a time period to come into compliance with those rules that is the later of (1) eight weeks from the date of the public notice, or (2) twelve months after the Commission publishes a summary of the Order in the Federal Register.

**96 313. *Breach Notification Procedures*. The data breach notification rule we adopt today will become effective the later of (1) PRA approval, or (2) six months after the Commission publishes a summary of the Order in the Federal Register.[910] We find that six months is an appropriate minimum *14043 implementation period for data breach implementation. Although providers of telecommunications services other than BIAS are subject to our current breach notification rule[911] and we are confident that carriers are cognizant of the importance of data breach notification in the appropriate circumstances,[912] we recognize that carriers may have to modify practices and policies to implement our new rule, we find the harm trigger we adopt and timeline for notifying customers lessen the implementation requirements.[913] Moreover, harmonization of our data breach rule for BIAS and voice services enable providers to streamline their notification processes, which should also lessen carriers' need for implementation time. Given these steps to minimize compliance burdens, we find six months is an adequate minimum timeframe. We also direct the Bureau to release a public notice after PRA approval of the data breach rule, indicating that the rule is effective, and giving carriers a time period to come into compliance with the rule that is the later of (1) eight weeks from the date of the public notice, or (2) six months after the Commission publishes a summary of the Order in the Federal Register.

314. *Data Security*. The specific data security requirements we adopt today will become effective 90 days after publication of a summary of the Order in the Federal Register.[914] We find this to be an appropriate implementation period for the data security requirements because as discussed above, carriers should already be largely in compliance with these requirements because the reasonableness standard adopted in this Order provides carriers flexibility in how to approach data security and resembles the obligation to which they were previously subject pursuant to Section 5 of the FTC Act.[915] We therefore do not think the numerous steps outlined by commenters that would have been necessary to comply with the data security proposals in the *NPRM* apply to the data security rule that we adopt.[916] Nevertheless, we encourage providers, particularly small providers, to use the adoption of the Order as an opportunity to revisit their data security practices and therefore provide an additional 90 days subsequent to Federal Register publication in which carriers can revisit their practices to ensure that they are reasonable, as provided for in this Order.

315. *Prohibition on Conditioning Broadband Service on Giving up Privacy*. The prohibition on conditioning offers to provide BIAS on a customer's agreement to waive privacy rights will become effective 30 days after publication of a summary of this Order in the Federal Register.[917] We find that unlike the other privacy rules, consumers should benefit from this prohibition promptly. As discussed above, we find that these "take-it-or-leave-it" offers give consumers no choice and require them to trade their privacy for access to the Internet. As supported in the record, these practices would harm consumers, particularly lower-income customers.[918] We therefore find no basis for any delay in the effective date of this important protection. Further, prompt implementation will not create any burdens for carriers that are committed to providing their customers with privacy choices. All other privacy rules adopted in the Order will be effective 30 days after publication of a summary of the Order in the Federal Register.

14044 2. Uniform Timeline for BIAS and Voice Services

**97 316. We adopt a uniform implementation timetable for both BIAS and other telecommunications services. Implementing our rules for all telecommunications services simultaneously will help alleviate potential customer confusion from disparate practices between services or carriers. This approach will support the benefits of harmonization discussed throughout this Order and is strongly supported in the record.[919] We emphasize that until the new privacy rules are effective and implemented with respect to voice services, the existing rules remain in place. Further, we make clear that all carriers, including BIAS providers, remain subject to Section 222 during the implementation period that we establish and beyond.[920]

3. Treatment of Customer Consent Obtained Prior to the Effective and Implementation Date of New Rule

317. We recognize that our new customer approval rule[921] requires carriers to modify the way they obtain consent for BIAS and voice services based on our sensitivity-based framework discussed above.[922] We seek to minimize disruption to carriers' business practices and therefore do not require carriers to obtain new consent from all their customers.[923] Rather, for BIAS, we treat as valid or "grandfather" any consumer consent that was obtained prior to the effective date of our rules and that is consistent with our new requirements. For example, if a BIAS provider obtained a customer's opt-in consent to use that individual's location data to provide coupons for nearby restaurants and provided adequate notice regarding his or her privacy rights, then the customer's consent would be treated as valid. The consent would not be invalidated simply because it occurred before the new customer approval rule became effective. However, if the customer consent was not obtained in the manner contemplated by our new rule, a new opportunity for choice is required. We recognize that consumers whose opt-in or opt-out consent is grandfathered may not be aware of our persistent choice requirement,[924] and therefore we direct the Consumer and Governmental Affairs Bureau to work with the industry to engage in a voluntary consumer education campaign.

318. We decline to more broadly grandfather preexisting consents obtained by small BIAS providers.[925] We find that the parameters set forth above create the appropriate balance to limit ***14045** compliance costs with our new notice and customer approval rules while providing consumers the privacy protections they need. As we explain above, BIAS providers are in a unique position as gateways to the Internet and we need to ensure consumers are aware of their privacy rights and have the ability to choose how their personal information is used and shared.

319. As with BIAS services, customer consent obtained by providers of other telecommunications services subject to the legacy rules remains valid for the time during which it would have remained valid under the legacy rules. As such, opt-out consent obtained before the release date of this order remains valid for two years after it was obtained, after which a carrier must conform to the new rules.[926] Opt-in consent that is valid under the legacy rules remains valid. This approach is consistent with established customer expectations at the time the consent was solicited, and should reduce notice fatigue.[927] Maintaining the validity of customer consent for voice services will also help reduce the up-front cost of compliance of the new rules. We reiterate that a customer's preexisting consent is valid only within its original scope. For instance, if a carrier previously received a customer's opt-in consent to use information about the characteristics of the customer's service to market home alarm services, the carrier could not claim that same consent applies to use of different customer PI (e.g., a Social Security Number) or a different use or form of sharing (e.g., selling to a data aggregator). Similarly, opt-out consent to use and share CPNI to market communications-related services could not be used to support use of different customer PI or different forms of use or sharing (e.g., marketing non-communications-related services).

4. Limited Extension of Implementation Period for Small Carriers

****98** 320. In the *NPRM* we sought comment on ways to minimize the burden of our proposed privacy framework on small providers,[928] and throughout this Order we have identified numerous ways to reduce burdens and compliance costs while providing robust privacy protections to their customers.[929] To further address the concerns raised by small providers in the record, we provide small carriers an additional twelve months to implement the notice and customer approval rules we adopt today.[930]

***14046** 321. We find that an additional one-year phase-in will allow small carriers—both broadband providers and voice providers—time to make the necessary investments to implement these rules.[931] The record reflects that small providers have comparatively limited resources and rely extensively on vendors over which they have limited leverage to compel adoption of new requirements.[932] We recognize our notice and choice framework may entail up- front costs for small providers. We also agree with NTCA that small providers will "be aided by observing and learning from the experience of larger firms who by virtue of their size and scale are better position to absorb the learning curve."[933] As such, we find that this limited extension is appropriate.

322. For purposes of this extension, we define small BIAS providers as providers with 100,000 or fewer broadband connections and small voice providers with 100,000 or fewer subscriber lines as reported on their most recent Form 477, aggregated over all the providers' affiliates. In the *NPRM* we sought comment on whether we should exempt carriers that collect data from fewer than 5,000 customers a year provided they do not share customer data with third parties.[934] Commenters objected that the 5,000 threshold was too narrow to accurately identify small providers and that the limitation on information sharing was too restrictive.[935] We therefore find that given the limited scope of relief granted to small carriers, increasing the numeric scope from the 5,000 to 100,000 is suitable because it will benefit additional providers without excess consumer impact. We also decline to count based on the number of customers from whom carriers collect data, as we recognize that some data collection is necessary to the provision of service.[936] Additionally, we decline to impose any requirement that small providers not share their information with third parties to qualify for the exception. Moreover, cabining the scope of this limited extension to providers serving 100,000 or fewer broadband connections or voice subscriber lines is consistent with the *2015 Open Internet Order*, in which we adopted a temporary exemption from the enhancements to the transparency rule for BIAS providers with 100,000 or fewer broadband subscribers.[937] Therefore for these reasons, and the critical importance of privacy protections to ***14047** consumers, we decline to adopt CCA's recommendation to define small BIAS providers as either companies with up to 1,500 employees or serving 250,000 subscribers or less.[938]

****99** 323. We decline to provide any longer or broader extension periods or exemptions to our new privacy rules.[939] We find that our "reasonableness" approach to data security mitigates small provider concern about specific requirements, such as annual risk assessments and requiring specific privacy credentials.[940] Moreover, as advocated by small carriers, we adopt a customer choice framework that distinguishes between sensitive and non-sensitive customer information, as well as decline to mandate a customer-facing dashboard to help manage their implementation and compliance costs.[941] Furthermore, we find our data breach notification requirements and "take-it-or-leave-it" prohibition do not require an implementation extension as compliance with these protections should not be costly for small carriers that generally collect less customer information and use customer information for narrower purposes. Also, although smaller in company size and market share, small carriers still retain the ability to see and collect customer personal information and therefore, it is appropriate to extend these important protections to all customers on an equal timeframe.

J. Preemption of State Law

324. In this section, we adopt the proposal in the *NPRM* and announce our intent to preempt state privacy laws, including data security and data breach laws, *only* to the extent that they are inconsistent with any rules adopted by the Commission.[942] This limited application of our preemption authority is consistent with our precedent in this area.[943] We have long appreciated and valued the important role states play in upholding the pillars of privacy and protecting customer information.[944] As the Office of the New York Attorney General has explained, the State AGs are "active participants in ensuring that [their] citizens have robust privacy protections" and it is critical that they continue that ***14048** work.[945] As such, we further agree with the New York Attorney General's Office that "it is imperative that the FCC and the states maintain broad authority for privacy regulation and enforcement.""[946] We also agree with those providers and other commenters that argue that neither telecommunications carriers nor customers are well-served by providers expending time and effort attempting to comply with conflicting privacy requirements.[947] We therefore codify a very limited preemption rule that is consistent with our past practice with respect to rules implementing Section 222. By allowing states to craft and enforce their own laws that are not inconsistent with our rules with respect to BIAS providers' and other telecommunications carriers' collection, use, and sharing of customer information, we recognize and honor the important role the states play in protecting the privacy of their customer information.

325. As the Commission has previously explained, we may preempt state regulation of intrastate telecommunications matters "where such regulation would negate the Commission's exercise of its lawful authority because regulation of the interstate

aspects of the matter cannot be severed from regulation of the intrastate aspects."[948] In this case, we apply our preemption authority to the limited extent necessary to prevent such instances of incompatibility. Where state privacy laws do not create a conflict with federal requirements, providers must comply with federal law and state law.

**100 326. As we have in the past, we will take a fact-specific approach to the question of whether a conflict between our privacy rules and state law exists.[949] If a provider believes that it is unable to comply *14049 simultaneously with the Commission's rules and with the laws of another jurisdiction, the provider should bring the matter to our attention in an appropriate petition. Examining specific conflict issues when they arise will best ensure that consumers receive the privacy protections they deserve, whether from a state source or from our rules.

327. The states have enacted many laws aimed at ensuring that their citizens have robust privacy protections.[950] We agree with the Pennsylvania Attorney General that it is important that we not "undermine or override state law providing greater privacy protections than federal law,"[951] or impede the critical privacy protections states continue to implement. Rather, as supported in the record, we encourage the states to continue their important work in the privacy arena, and adopt an approach to preemption that ensures that they are able to do so.[952] In so doing, we reaffirm the Commission's limited exercise of our preemption authority to allow states to adopt consumer privacy protections that are more restrictive than those adopted by the Commission provided that regulated entities are able to comply with both federal and state laws.[953]

328. In taking this approach, we reject ACA's suggestion that we should "preempt state data breach notification laws entirely."[954] As stated above, we continue to provide states the flexibility to craft and enforce their own privacy laws, and therefore we only preempt state laws to the extent that they impose inconsistent requirements. Our privacy rules are designed to promote "cooperative federalism" and therefore unless providers are unable to comply with both the applicable state and Commission requirements, we find it inappropriate to categorically preempt these state data breach laws.[955]

329. Commenters have identified data breach notification as one area where conflicts may arise. We agree with commenters that it is generally best for carriers to be able to send out one customer data breach notification that complies with both state and federal laws,[956] and we welcome state agencies to use our data breach notification rules as a model.[957] However, we recognize that states law may require differently timed notice or additional information than our rules, and we do not view such privacy-protective requirements as necessarily inconsistent with the rules we adopt today since carriers are capable of sending two notices at two different times. However, in the interest of efficiency and *14050 preventing notice fatigue, we invite carriers that find themselves facing requirements to send separate consumer data breach notices to fulfill their federal and state obligations to come to the Commission with a proposed waiver that will enable them to send a single notice that is consistent with the goals of notifying consumers of their data breach. Additionally, as explained by CTIA, a situation could arise where a state law enforcement agency requests a delay in data breach notice due to an ongoing investigation.[958] We encourage both carriers and state law enforcement officials to come to the Commission in such a situation, as we have authority to waive our rules for good cause and recognize the importance of avoiding interference with a state investigation.[959]

**101 330. We clarify that we apply the same preemption standard to all aspects of our Section 222 rules. Although the Commission, in its previous orders, had applied its preemption standard with respect to all of the Section 222 rules, the preemption requirement is currently codified at Section 64.2011 of our rules, which addresses notification of data breaches.[960] Recognizing that states are enacting privacy laws outside of the breach notification context, and consistent with historical Commission precedent, we conclude that the preemption standard should clearly apply in the context of all of the rules we adopt today implementing Section 222. Therefore, as we proposed in the *NPRM*, we remove the preemption provision from that section of our rules, and adopt a new preemption section that will clearly apply to all of our new rules for the privacy of customer proprietary information.[961] In doing so, we enable states to continue their important role in privacy protection.

331. Further, we find that the same preemption standard should apply in both the voice and BIAS contexts to help provide certainty and consistency to the industry.[962] Accordingly, we adopt a harmonized preemption standard across BIAS and other telecommunications services.[963] By applying the same preemption standard to BIAS providers and to other telecommunications carriers, we ensure that states continue to serve a role in tandem with the Commission, regardless of the specific service at issue.

IV. LEGAL AUTHORITY

332. In this Report and Order, we implement Congress's mandate to ensure that telecommunications carriers protect the confidentiality of proprietary information of and relating to customers. As explained in detail below, the privacy and security rules that we adopt are well-grounded in our statutory authority, including but not limited to Section 222 of the Act.[964]

A. Section 222 of the Act Provides Authority for the Rules

333. Section 222 of the Act governs telecommunications carriers in their use, disclosure, and protection of proprietary information that they obtain in their provision of telecommunications services. The fundamental duty this section imposes on each carrier, as stated in Section 222(a), is to "protect the ***14051** confidentiality of proprietary information of, and relating to" customers, fellow carriers, and equipment manufacturers.[965] Section 222(c) imposes more specific requirements with regard to a subset of customers' proprietary information, namely customer proprietary *network* information.[966] This Report and Order implements Section 222 as to customer PI, a category that includes individually identifiable CPNI and other proprietary information that is "of, and relating to" customers of telecommunications services. As explained below, the rules we adopt today are faithful to the text, structure, and purpose of Section 222.

1. Section 222 Applies to BIAS Providers Along With Other Telecommunications Carriers

****102** 334. We begin by reaffirming our conclusion in the *2015 Open Internet Order* that Section 222 applies to BIAS providers.[967] In so doing, we reject the view that Section 222 applies only to voice telephony.[968] The *2015 Open Internet Order* reclassified BIAS as a telecommunications service, making BIAS providers "telecommunications carriers" insofar as they are providing such service.[969] Section 222(a) imparts a general duty on "[e] very telecommunications carrier," while other subsections specify the duties of "a telecommunications carrier" in particular situations. The term ""telecommunications carrier" has long included providers of services distinct from telephony, including at the time of Section 222's enactment. Thus, in construing the term for purposes of Section 222, we see no reason to depart from the definition of "telecommunications carrier" in Section 3 of the Act.[970] To the contrary, deviating from this definition without a clear textual basis in Section 222 would create uncertainty as to the scope of numerous provisions in the Act, regulatory imbalance between various telecommunications carriers, and a gap in Congress's multi-statute privacy regime. Moreover, commenters cite no evidence that the term "telecommunications carrier" is used more restrictively in Section 222 than elsewhere in the Act.

335. We similarly reject the claim that in reclassifying BIAS we have improperly exercised our "definitional authority" to expand the scope Section 222.[971] The relevant term that defines the scope of Section 222 is ""telecommunications carrier,"[972] and we simply are applying the holding of the *2015 Open Internet Order* that this statutory term encompasses BIAS.[973] Nor does the fact that Section 230 of ***14052** the Act uses the term Internet, while Section 222 does not, compel us to disregard the clear uses of ""telecommunications carrier" in Section 222.[974]

336. We also reject arguments that "telephone-specific references" contained in Section 222 serve to limit the scope of the entire section to voice telephony or related services.[975] This argument misconstrues the structure of Section 222. As explained in more detail below, Section 222(a) imposes a broad general duty to protect proprietary information while other provisions impose more-specific duties. Some of these more-specific duties concerning CPNI are indeed relevant only in the context of voice

telephony.[976] But their purpose is to specify duties that apply in that limited context, not to define the outer bounds of Section 222.[977] The definition of CPNI found in Section 222(h)(1) illustrates this point. While the term is defined in Section 222(h)(1)(B) to include "the information contained in the bills pertaining to telephone exchange service or telephone toll service"[978] and to exclude ""subscriber list information"[979] —categories that have no relevance for BIAS—pursuant to Section 222(h)(1)(A) the term CPNI also includes a broader category of information that carriers obtain by virtue of providing a telecommunications service.[980] This broader category articulated in Section 222(h)(1)(A) pertains to "telecommunications service[s]" in general, not only to telephony. As we have explained above, BIAS providers collect significant amounts of information that qualifies as CPNI under the broad, functional definition articulated in Section 222(h)(1)(A).[981] Whether BIAS providers also issue telephone bills or publish directories makes no difference. The reference to "call[s]" in Section 222(d)(3) is similarly inapposite as to the scope of Section 222 as a whole.[982] The "call[s]" at issue in this provision are customer service calls initiated by the customer; a customer of any service, including BIAS, can make such a call.

****103** 337. If anything, the placement of references to telephony in Section 222 supports our reading of that section as reaching *beyond* telephony. Such terms are used to define narrow provisions or exceptions, but not the outer contours of major components of the statute. Most significantly, the broad term "telecommunications carrier" is used in defining the general duty under subsection (a); the ***14053** obligation to seek customer approval for use, disclosure, or permission of access to individually identifiable CPNI under paragraph (c)(1); the obligation to disclose CPNI upon request under paragraph (c)(2); and the grant of permission to use and disclose "aggregate customer information" under paragraph (c) (3).

338. Where a component of Section 222 applies only to a subset of telecommunications carriers, Congress used a term to apply such a limit. For instance, Section 222(c)(3) permits all telecommunications carriers to use and disclose aggregate customer information, but "local exchange carrier[s]" can do so only on the condition that they make the information available to others on reasonable and nondiscriminatory terms.[983] The inclusion of a pro-competitive condition in Section 222(c)(3) that applies only to local exchange carriers is consistent with other provisions of the 1996 Act directed at opening local telephone markets to competition.[984] But the limited scope of this condition does not serve to limit the applicability of Section 222 as a whole.[985] Indeed, not even Section 222(c)(3) *itself* is limited in scope to providers of local exchange service. Rather, its primary purpose is to clarify that telecommunications carriers may use and disclose customer information when it takes the form of "aggregate customer information." BIAS providers commenting in this proceeding have expressed a strong interest in being able to use and disclose such information.[986] As telecommunications carriers, their ability to do so is made clear under Section 222(c)(3).

339. Similarly, the limited scope of providers covered by the duty to share ""subscriber list information" under Section 222(e) is commensurate with the scope of the problem being addressed, namely in the publication of telephone directories.[987] In particular, the "telephone exchange service" providers subject to unbundling and nondiscrimination requirements by the provision are those that would have the "subscriber list information" needed to produce these directories.[988] The fact that Section 222 includes provisions to address such telephone-specific concerns does not change its overall character as a privacy protection statute for telecommunications, one that has as much relevance for BIAS as it does for telephone service.

340. We disagree with the view that Congress confirmed Section 222 as a telephone-specific statute when it amended subsections 222(d)(4), (f)(1) and (g) as part of the New and Emerging Technologies 911 Improvement Act of 2008 (NET 911 Act).[989] These provisions of Section 222 establish rights and obligations regarding carrier disclosure of customer information to assist in the delivery of emergency services. The NET 911 Act brought "IP-enabled voice service[s]" within their scope. Amending Section 222 in this manner addressed a narrow but critical public safety concern: IP-enabled voice services were emerging as a platform for delivery of 911 service, yet providers of these services were not classified as "telecommunications carriers" subject to Section 222.[990] The NET 911 Act ***14054** amendments ensure that all IP-enabled voice services, even to the extent they are *not* telecommunications services, are treated under Section 222 much the same as traditional telephony services for purposes

related to E911 service. This treatment has nothing to do with the extent to which telecommunications services that are not voice services are subject to Section 222.[991]

**104 341. In addition, we observe that none of the references to telephone-specific services in Section 222 that commenters identify are found in Section 222(a). As explained below, we construe Section 222(a) as a broad privacy protection mandate that extends beyond the specific duties articulated in Sections 222(b) and (c). Thus, even if commenters could establish that these more specific parts of Section 222 are qualified in ways that limit their scope to voice telephony or related services, or that exclude BIAS from their scope, we would still find that a BIAS provider—like "[e]very telecommunications carrier"[992]—has customer privacy obligations under Section 222(a). And if we accept commenters' view that the role of Section 222(a) in the statute is to identify "which entities" have duties thereunder,[993] it follows that subsections (b) and (c) apply not only to telephony or voice providers but to ""every telecommunications carrier."

342. Finally, we dismiss efforts to conflate Section 222 with its implementing rules.[994] When we forbore from application of the existing implementing rules to BIAS, we made clear that the statute itself still applies.[995] Commenters do not present any compelling reason to revisit this decision.[996]

2. Section 222(a) Provides Authority for the Rules as to Customer PI

343. We next conclude that Section 222(a) provides legal authority for our rules. As explained below, Section 222(a) imposes an enforceable duty on telecommunications carriers that is more expansive than the combination of duties set forth subsections (b) and (c). We interpret these subsections as defining the contours of a carrier's general duty under Section 222(a) as it applies in particular contexts, but not as coterminous with the broader duty under Section 222(a). On the contrary, we construe Section 222(a) as imposing a broad duty on carriers to protect customer PI that extends beyond the narrower scope of information specified in Section 222(c). We also find that the rules adopted in this Report and Order to ensure the protection of customer PI soundly implement Section 222(a).

*14055 **a. Section 222(a) Imposes on Telecommunications Carriers an Enforceable Duty to "Protect the Confidentiality" of "Proprietary Information"**

344. Section 222(a) states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to" customers, fellow carriers, and equipment manufacturers.[997] In this Report and Order we adopt the most straightforward interpretation of this text by finding that Section 222(a) imposes a "duty," on "every telecommunications carrier." A "duty" is commonly understood to mean an enforceable obligation.[998] It is well-established that the Commission may adopt rules to implement and enforce an obligation imposed by the Act, including Section 222(a).[999] The substance of the duty is to "protect the confidentiality of proprietary information"—all "proprietary information" that is "of, and relating to," the specified entities, namely "other telecommunications carriers, equipment manufacturers, and customers."[1000] This Report and Order implements Section 222(a) with respect to "customers," defining the term "customer PI" to mean that which is "proprietary information of, and relating to ... customers."[1001] The term is thus firmly rooted in the language of Section 222(a).[1002]

**105 345. The duty set forth in Section 222(a) concerns information "of, and relating to" customers and other covered entities. The Supreme Court has held that "the ordinary meaning of [the phrase 'relat[ing] to'] is a broad one," and in certain contexts it has described the phrase as "deliberately expansive" and "conspicuous for its breadth."[1003] The record contains no evidence that Congress intended the phrase "relating to" to be construed more narrowly for purposes of Section 222(a) than it would be ordinarily. Thus, the most natural reading of Section 222(a) is that it imposes a broad duty on telecommunications carriers

to protect proprietary information, one that is informed by but not necessarily limited to the more specific duties laid out in subsections (b) and (c).[1004]

346. The treatment of "equipment manufacturers" under Section 222 provides further evidence for this interpretation. This term is used only once: Section 222(a) includes "equipment manufacturers" ***14056** among the classes of entities owed confidentiality protections as part of a carrier's "general" duty.[1005] While Sections 222(b) and (c) specify in greater detail how this duty applies with respect to customers and fellow carriers—the other entities protected under Section 222(a)—there is no further statutory guidance on what carriers must do to protect the proprietary information of equipment manufacturers. Thus, the duty imposed on carriers under Section 222 with regard to equipment manufacturers must have its sole basis in Section 222(a). This would not be possible unless Section 222(a) were read to confer enforceable obligations that are independent of, and that exceed, the requirements of subsections (b) and (c).[1006]

347. Nothing in the statutory text or structure of Section 222 contradicts this interpretation. To the contrary, this plain language interpretation is further supported by the structure of Section 222 and consistent with approaches used in other parts of the Act. Section 222(a)'s heading "In General" suggests a general "duty," to be followed by specifics as to particular situations. Section 222(a) is not given a heading such as "Purpose" or "Preamble" that would indicate that the "duty" it announces is merely precatory or an inert "statement of purpose." Section 251 of the Act is structured similarly in this regard, and there is no argument that the duty announced in Section 251(a) is merely precatory.[1007] In addition, there is no textual indication that Sections 222(b) and (c) define the outer bounds of Section 222(a)'s scope.[1008] For instance, Section 222(a) does not include language such as "as set forth below" or "as set forth in subsections (b) and (c)." We also dismiss as irrelevant CTIA's observation that some provisions of the 1996 Act "can be interpreted as general statements of policy, rather than as grants of additional authority."[1009] That fact alone would have no bearing on how to interpret Section 222(a), which employs "regulatory terminology" in imparting a general "duty" on telecommunications carriers.[1010] Finally, our interpretation of subsection (a) does not render subsection (b) or (c) superfluous.[1011] The latter subsections directly impose specific requirements on telecommunications carriers to address concerns that ***14057** were particularly pressing at the time of Section 222's enactment. Our reading of Section 222(a) preserves the role of each of these provisions within the statute, while also allowing the Commission to adopt broader privacy protections to keep pace with the evolution of telecommunications services.

****106** 348. As Public Knowledge argues, the breadth of the duty announced in Section 222(a) is consistent with a broad understanding of the purpose of Section 222. We agree that this subsection endows the Commission with a continuing responsibility to protect the privacy customer information as telecommunications services evolve.[1012] Congress's inclusion in Section 222 of more specific provisions to address issues that were "front-and-center" at the time of the 1996 Act's enactment in no way detracts from this broader purpose.[1013]

349. Our interpretation of Section 222(a) is far from novel. Other provisions of the Act set forth a general rule along with specific instructions for applying the rule in particular contexts.[1014] We agree with Public Knowledge that, in addition to Section 251, another provision that bears a particularly close resemblance to Section 222 in this regard is Section 628.[1015] Subsection (b) of this provision imposes a general "prohibition" on cable operators from interfering with competitors' ability to provide satellite cable or satellite broadcast programming.[1016] Subsection (c) in turn directs the Commission to adopt rules to implement this prohibition and specifies their "minimum contents."[1017] As a general matter, the "minimum" regulations required under Section 628(c) are aimed at preventing cable operators from denying their competitors access to programming.[1018] In 2009, the D.C. Circuit upheld Commission rules adopted under Section 628(b) that prevented cable operators from entering exclusivity agreements with ***14058** owners of multi-unit buildings, an anti-competitive practice that is only tenuously related to the "minimum" regulations implemented under Section 628(c).[1019] Taking note of Section 628(b)'s "broad and sweeping terms,"" the court ruled that "nothing in the statute unambiguously limits the Commission to regulatingpractices" related

to the "principal evil that Congress had in mind" when enacting Section 628, as expressed in subsection (c).[1020] Rather, it held that the Commission's "remedial powers" to enforce subsection (b) reached beyond circumstances that Congress "specifically foresaw."[1021] Similarly, we agree with OTI that the "principal"" focus of Section 222 on regulating CPNI to promote competition and consumer protection in emerging telecommunications markets must be read in harmony with the "broad and sweeping" mandate of Section 222(a).[1022] In construing the latter we must give effect to the "actual words" of the provision.[1023] These words plainly impose a "duty" on "every telecommunications carrier."

350. Even if there were some ambiguity in the text, commenters that oppose our interpretation of Section 222(a) have failed to offer a compelling alternative interpretation. One proposed alternative is that Section 222(a) merely confirms Congress's intent that the newly enacted Section 222 would apply to "every telecommunications carrier," including not only the legacy carriers subject to then-existing CPNI requirements but also "the new entrants that the 1996 Act envisioned."[1024] Similar arguments in the record are that Section 222(a) "identifies which entities have responsibility to protect information, and informs the reading of subsequent subsections, which articulate how these entities must protect information,"[1025] or that the provision "merely identifies the categories of information to which Section 222 applies."[1026] These arguments are unconvincing. First, subsections (b) and (c) themselves are written broadly to apply to "telecommunications carrier[[s]." There is no textual basis for interpreting either provision as applying only to a legacy subset of carriers, such as the Bell Operating Companies, AT&T, and GTE. Subsections (b) and (c) also specify the categories of information to which each applies, without reference to subsection (a). Thus, commenters' proposals for interpreting Section 222(a) ***14059** would render that provision superfluous, contrary to the canon against such interpretations.[1027] Moreover, the statute does not expressly link the duty announced in Section 222(a) with the subsections that follow. That is, the statute does not direct "every telecommunications carrier" to protect proprietary information "in accordance with subsections (b) and (c)" or anything similar.

****107** 351. Nor does our interpretation of Section 222(a) vitiate any other elements of Section 222. On the contrary, we read Section 222(a) as imposing a broad duty that can and must be read in harmony with the more specific mandates set forth elsewhere in the statute.[1028] Accordingly, we need not and do not construe Section 222(a) so broadly as to prohibit any sharing of subscriber information that subsection (e) or (g) would otherwise require.[1029] That is, subsection (a)'s duty to protect the confidentiality of customer PI is in no way inconsistent with subsection (e)'s duty to share SLI, which by definition[1030] is *published* and therefore is not confidential.[1031] Nor is it inconsistent with subsection (g)'s duty to share subscriber information "solely for purposes of delivering or assisting in the delivery of emergency services."[1032] Indeed, far from "render[ing] null" subsections (e) and (g), our reasoned interpretation of Section 222(a) preserves the full effect of both of these provisions.[1033] We thus reject the argument that subsection (a)'s absence from the "notwithstanding" clauses of subsections (e) and (g) should be taken as evidence that the former provision confers no ""substantive regulatory authority."[1034] Rather, there was simply no need for Congress to have included subsection (a) in these clauses.[1035] Also, the mere omission of Section 222(a) from the these clauses would have been an exceedingly oblique and indirect way of settling upon an interpretation of Section 222(a) that runs counter to its plain meaning.[1036] Relatedly, there is no conflict because our understanding of Section 222(a) does not override any of the exceptions to Section 222(c) set forth in Section 222(d). For example, a carrier need not fear that its disclosure of CPNI "to initiate, render, bill [or] collect for telecommunications services" as subsection (d) permits might independently violate Section 222(a), because such disclosure is not inconsistent with the carrier's ***14060** duty to protect the confidentiality of such information.[1037] Nor do we construe Section 222(a) as negating a carrier's right under Section 222(c)(1) to use, disclose or permit access to CPNI for the specific purposes set forth in subclauses (A) and (B).[1038]

352. We also disagree with the argument that our construction of Section 222(a) enlists a "vague or ancillary" provision of the statute to "alter [its] fundamental details."[1039] Section 222(a) appears, of course, at the beginning of Section 222. The first thirteen words of Section 222(a)—and thus, of Section 222—read: "Every telecommunications carrier has a duty to protect

the confidentiality of proprietary information ....”[1040] Congress could not have featured this language any more prominently within the statute, nor could the duty it propounds be any more clearly and directly expressed. As discussed above, a statutory structure of establishing a general duty and then addressing subsets of that duty in greater detail is not unique, even within the Communications Act.

**108 353. Finally, we reject the view that our interpretation of Section 222(a) locates in “a long-extant statute an unheralded power to regulate a significant portion of the American economy.”[1041] The Commission has exercised regulatory authority under Section 222(c) for approximately two decades and oversaw certain carriers' handling of customer PI for over two decades before that.[1042] Even assuming a contrary reading of Section 222(a), subsection (c) would still invest the Commission with substantial regulatory authority over personal information that BIAS providers and other telecommunications carriers collect from their customers, and Sections 201 and 202 would apply to carriers' practices in handling customers' information.[1043] Thus, our interpretation of Section 222(a) is a far cry from the ““transformative” act of statutory interpretation struck down in *Utility Air Regulatory Group v. EPA*.[1044] There, the agency's broad construction of the term “air pollutant” would have completely upended the “structure and design” of a permitting scheme established by statute and extended that regime to broad swaths of the economy.[1045] By contrast, the net effect of our interpreting Section 222(a) as governing all customer PI is to make clear the Commission's authority over carriers' treatment of customer proprietary information that may not qualify as CPNI, such as Social Security numbers or financial records. This represents a modest but critical recognition of our regulatory purview beyond CPNI to cover additional “proprietary” information that Section 222(a) plainly reaches. Moreover, BIAS providers' treatment of such information fell squarely within the jurisdiction of the FTC prior to the Commission's reclassification of BIAS. The scope of regulatory authority we are asserting under Section 222(a) is thus far from novel or “unheralded.”

b. The Broad Duty of Section 222(a) Extends to All “Proprietary Information” That Is “Of” or “Relating to” Customers

354. Having determined that Section 222(a) imposes on carriers an enforceable duty, we also *14061 conclude that this duty extends to all “proprietary information”” that is “of, or relating to” customers, regardless of whether the information qualifies as CPNI. That is, we reject the argument that Section 222(c) exhausts the duty set forth in Section 222(a) as it applies with respect to customers.

355. Once again, our interpretation follows from the plain language of Section 222. While subsection (c) establishes obligations with respect to ““customer proprietary network information,” subsection (a) omits the word ““network.” The concept of the “network” lies at the heart of CPNI: the information defined as CPNI in Section 222(h)(1) is of the sort that carriers obtain by virtue providing service over their networks. However, as we have explained above, this sort of information is not the only “proprietary information” that telecommunications carriers can and do obtain from their customers by virtue of the carrier-customer relationship.[1046] We therefore find that “proprietary information of, and relating to ... customers” is best read as broader than CPNI. Moreover, we are convinced that the term “network” should not be read into Section 222(a), contrary to what some commenters appear to argue.[1047] We dismiss the idea that the syntax of Section 222(a) would have made it awkward to include the term “network” as an express limitation on the general duty as it applies with regard to customer proprietary information.[1048] Congress is not bound to any particular formula when drafting legislation. Section 222(a) could easily have been written to include the term “customer proprietary network information” in full, had Congress chosen to do so.[1049]

**109 356. Even if there were some ambiguity in the text of the statute, we would conclude that the best interpretation is that Section 222(a) applies to customer proprietary information that is not CPNI. Some argue that the legislative history of Section 222 precludes this interpretation because of a statement from the Conference Report that attended passage of the 1996 Act, which reads: “In general, Section 222 strives to balance both competitive and consumer privacy interests with respect to CPNI.”[1050] Commenters appear to interpret this statement as evidence that Section 222 was intended to apply *only* to CPNI.[1051] But this is clearly not so. Section 222(a) concerns not only customer information but also information “of, and relating to” fellow

carriers and equipment manufacturers. Section 222(b) in turn is focused exclusively on "carrier information."[1052] Therefore, Section 222 *in general* cannot be concerned solely with CPNI. We are similarly unmoved by evidence that Congress considered but ultimately rejected a more expansive definition of CPNI than that which is codified in Section 222(h)(1).[1053] Such evidence cannot decide the question whether Section 222(a) governs a category of customer information that is *broader than* CPNI. As explained above, our interpretation follows from the plain language of the ***14062** provision, and the legislative history of Section 222 is not to the contrary. At the very least, any contrary evidence that may be derived from the legislative history is far from sufficient to override our reasoned interpretation of the provision.[1054]

357. We acknowledge that prior Commission orders implementing Section 222 have focused largely on CPNI rather than customer PI more broadly.[1055] Yet we do not believe this precedent should constrain our efforts in this proceeding to develop robust privacy protections for consumers under Section 222(a). In fact, the Commission made clear as early as 2007 that Section 222(a) requires carriers to "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."[1056] Our express determination in the *TerraCom* proceeding that subsection (a) covers customer proprietary information beyond CPNI merely "affirm[ed]" what the Commission had strongly implied seven years earlier.[1057] Moreover, earlier orders adopting and revising rules under Section 222 were focused so narrowly on the protection of individually identifiable CPNI that the question whether Section 222(a) covers additional customer information was never squarely addressed.[1058] This early focus on CPNI makes sense: Section 222 was adopted against the background of existing Commission regulations concerning CPNI,[1059] and the first Section 222 proceeding was instituted in response to a petition from industry seeking clarity about the use of CPNI.[1060] However, the Commission has never expressly endorsed the view that Section 222(a) fails to reach customer information beyond CPNI.[1061] We ***14063** therefore disagree that interpreting the provision in a contrary manner will have the effect of unsettling "18 years" of Commission precedent in this area.[1062]

****110** 358. Finally, construing Section 222(a) as reaching customer information other than CPNI avoids the creation of a regulatory gap that Congress could not reasonably have intended. While the FTC has broad statutory authority to protect against "unfair or deceptive" commercial practices, its enabling statute includes a provision that exempts common carriers subject to the Communications Act.[1063] This leaves the Federal Communications Commission as the only federal agency with robust authority to regulate BIAS providers and other telecommunications carriers in their treatment of sensitive customer information obtained through the provision of BIAS and other telecommunications services. If that authority failed to reach customer PI other than CPNI, substantial quantities of highly sensitive information that carriers routinely collect and use would fall outside of the purview of either this Commission or the FTC. The facts of *TerraCom* make clear the dangers of this outcome. In that proceeding we enforced Section 222(a) against a carrier that neglected to take even minimal security measures to protect Social Security numbers and other sensitive customer data from exposure on the public Internet.[1064] Commenters that advocate a narrow construction of Section 222(a) would have us divest ourselves of authority to take action in circumstances such as these. We need not and will not leave consumers without the authority to decide under what circumstances, if any, their BIAS providers are allowed to use and share their Social Security numbers, financial and health information, and other personal information.

c. The Rules We Adopt as to "Customer PI" Reasonably Implement the Mandate of Section 222(a) That Carriers "Protect the Confidentiality" of Such Information

359. The rules we adopt in this Report and Order apply with respect to customer PI, which we have defined to include three overlapping categories of information: individually identifiable CPNI; personally identifiable information (PII); and the content of communications. As explained above, the information we define as customer PI is "proprietary information of, [or] relating to ... customers" for purposes of Section 222(a).[1065] The rules we adopt in this Report and Order faithfully implement this statutory provision. As a general matter, we are adopting a uniform regulatory scheme to govern all customer PI, regardless of whether the information qualifies as CPNI. We have achieved this unity by replicating the basic structure of Section 222(c), including the exceptions set forth in Section 222(d), under Section 222(a). In doing so, we uphold the specific statutory terms

that govern CPNI, while ***14064** adapting these to the broader category of customer PI. This approach is lawful under the statute and well-supported as a matter of policy.

360. As discussed above, we understand Section 222(a) to impose a broad duty on carriers to protect customer PI that extends beyond the narrower scope of information specified in Section 222(c).[1066] Section 222(c) sets forth binding rules regarding application of the general duty to carriers' handling of CPNI. In support of this view, we note the common focus of these subsections on "confidentiality." While subsection (a) directs carriers to "protect the confidentiality of proprietary information" in general,[1067] subsection (c) concerns the confidentiality of "individually identifiable customer proprietary network information" in particular.[1068] Under our interpretation, subsection (c) provides one possible way of implementing the broad duty set forth in subsection (a). That is, subsection (c) settles what it means for a carrier to "protect the confidentiality of proprietary information" when the information at issue is individually identifiable CPNI. Given this reading of the two provisions, we find no reason that the basic scheme set forth in Section 222(c) to govern individually identifiable CPNI cannot not be replicated under Section 222(a) to govern customer PI more broadly. In adopting Section 222(c), Congress identified a scheme for "protecting the confidentiality of proprietary information" that it deemed valid at least in the context of CPNI.[1069] The statute is silent on the implementation of this general duty as it applies to customer PI more broadly. In the absence of clear statutory guidance on the matter, we must exercise our judgment to determine a regulatory scheme that is appropriate for customer PI other than individually identifiable CPNI.

****111** 361. We have good reason to adopt a single set of rules for all customer PI under Section 222(a) that is based on the scheme set forth for individually identifiable CPNI in Sections 222(c) and (d). First, the record indicates that customer expectations about the use and handling of their personal information do not typically depend on whether the information at issue is CPNI or some other kind of proprietary information. Rather, customers are far more likely to recognize distinctions based on the sensitivity of the data.[1070] The rules we adopt today uphold this widespread customer expectation.[1071] In addition, a common set of rules for all customer PI subject to 222(a) will be easier for customers to understand and for providers to implement than two distinct sets of rules.[1072] These considerations go to the very heart of Section 222: the ability of customers to make informed decisions and of providers to apply a harmonized regime to all customer data will each contribute to the protection of "confidentiality" that the statute requires. Moreover, equalizing treatment of CPNI and other customer PI more closely aligns our rules with the FTC's time-tested privacy approach.[1073]

362. We agree with Comcast that "protect[ing] confidentiality" of proprietary information involves, among other things, "preventing [such information] from being exposed without authorization."[1074] This is among the core purposes of our rules. The requirement to obtain customer ***14065** approval before using, disclosing, or permitting access to customer PI directly ensures that such information is not "expose[d]" without the "authorization" of the customer.[1075] The notice requirement advances this purpose further by providing customers the information they need to make informed choices regarding such use, disclosure, and access.[1076] As for the data security rule we adopt, its essential purpose is to safeguard customer PI from inadvertent or malicious "expos[ure]."[1077] The data breach notification rule reinforces these other requirements by providing customers, the Commission, and law enforcement agencies with notice of instances in which customer PI was "exposed without authorization."[1078] Finally, we uphold customers' ability to make decisions about the "expos[ure]" of their data by prohibiting carriers from conditioning service on the surrender of privacy rights.[1079]

363. Yet "protecting the confidentiality" of customer PI involves more than protecting it from unauthorized exposure. AT&T draws a false distinction in arguing that certain aspects of the rules "have nothing to do with confidentiality concerns and instead address only the *uses* of information within an ISP's possession."[1080] On the contrary, upholding customer expectations and choices regarding the use of their proprietary information is an integral part of "protecting the confidentiality of" that information for purposes of Section 222.[1081] In support of this view, we note that restrictions on the use of individually identifiable CPNI

are part of the scheme enacted under Section 222(c) to address the "confidentiality of [[CPNI],"[1082] and use is the *sole* conduct regulated to address the ""confidentiality of carrier information" under subsection (b).[1083] We thus believe the most natural reading of the term "confidentiality" as used in Section 222 is that it encompasses the use of information, not only "disclos[[ure]" and permissions of "access." As a coalition of consumer advocacy groups explain, in creating Section 222 "Congress most explicitly directed the Commission to ensure that users are not merely protected from exposure to third parties, but can actively control how the telecommunications provider itself *uses* the information" it collects.[1084] We agree with Verizon that "'protect' and 'use' are different words [that] must have different meanings" within the statute,[1085] but our view is that these meanings differ in terms of breadth. The "protect[ion] of confidentiality" is a concept that is broad enough to cover the different kinds of conduct regulated under Section 222(c): use, disclosure, and permission of access. A carrier that uses, discloses, or permits access to individually identifiable CPNI without customer approval violates its duty under ***14066** Section 222(c) to protect the ""confidentiality" of that CPNI. The same analysis applies under Section 222(a) with regard to customer PI more broadly. Accordingly, we find Section 222(a)'s duty to "protect the confidentiality" of proprietary information supports our rules in full.

3. Section 222(c) Provides Authority for the Rules as to CPNI

****112** 364. In addition to our Section 222(a) authority discussed above, we have authority under Section 222(c) to adopt the rules articulated in this Order as to individually identifiable CPNI. Subsection (c) obligates carriers to obtain customer approval for any use or disclosure of individually identifiable CPNI, except to provide the underlying telecommunications service or related services.[1086] Our rules implement this mandate.

365. First, our rules establish three methods for obtaining the customer approval required under Section 222(c): inferred consent, opt-in and opt-out. There exists longstanding Commission precedent for requiring the use of these methods,[1087] and commenters generally support some combination of the three.[1088] Under the rules we adopt in this Order, whether a carrier must seek an affirmative "opt-in" depends primarily on whether the information at issue is sensitive.[1089] This distinction is permissible under Section 222(c), which requires customer approval in general for most uses and disclosures of individually identifiable CPNI but does not specify the form this approval must take in any particular circumstance. Second, we require carriers to provide their customers with notice of their privacy policies, both at the point of sale and through posting on their websites and in mobile apps.[1090] This is an essential part of customer approval, as only informed customers can make meaningful decisions about whether and how extensively to permit use or disclosure of their information. The need for this notice to be given at the point of sale is particularly acute in circumstances where approval may take the form of an "opt-out." In such cases, the notice itself is integral to the "approval": customers are presumed to approve of the use or disclosure unless and until they affirmatively "opt out" of such activity. We also prohibit carriers from conditioning the provision of service on consent to the use or disclosure of information protected under Section 222.[1091] We believe that this prohibition is necessary to give effect to the customer approval that subsection (c) requires.[1092]

366. We next require carriers to take reasonable measures to secure the individually identifiable CPNI they collect, possess, use and share.[1093] Such a requirement is necessary to uphold customer decisions regarding use and disclosure of their information and to give effect to the terms of carriers' privacy policies. These other privacy protections would be vitiated if customers lacked any assurance that their information would be secured against unauthorized or inadvertent disclosures, cyber incidents, or other threats to the confidentiality of the information. Finally, we require carriers to report data breaches to their customers, the Commission, and law enforcement, except when a carrier reasonably determines that there is no reasonable likelihood of harm to customers.[1094] The Commission has long required such reporting as part of a carrier's duty to protect the confidentiality of its customers' ***14067** information.[1095] Among other purposes, data breach notifications can meaningfully inform customer decisions regarding whether to give, withhold, or retract their approval to use or disclose their information.

**113 367. In adopting these rules, we are respectful of other parts of the statute that limit or condition the scope of Section 222(c). For instance, our rules preserve the statutory distinction between individually identifiable ""CPNI" and "aggregate customer information."[1096] As explained above, we have not modified the definition of either of these terms in a way that would impermissibly narrow the scope of Section 222(c)(3).[1097] In addition, our rules include provisions that implement the exceptions to Section 222(c) that are set forth in Section 222(d).[1098] Finally, our rules are consistent with and pose no obstacle to compliance with the requirements of Sections 222(e) and (g) that subscriber information be disclosed in certain defined circumstances.[1099]

B. Sections 201(b) and 202(a) Provide Additional Authority to Protect Against Privacy Practices That Are "Unjust or Unreasonable" or "Unjustly or Unreasonably Discriminatory"

368. While Section 222 provides sufficient authority for the entirety of the rules we adopt in this Order, we conclude that Sections 201(b) and 202(a) also independently support the rules, because they authorize the Commission to prescribe rules to implement carriers' statutory duties not to engage in conduct that is "unjust or unreasonable" or "unjustly or unreasonably discriminatory."[1100] Our enforcement of Sections 201(b) and 202(a) in the context of BIAS finds expression in the "no unreasonable interference/disadvantage" standard adopted in the *2015 Open Internet Order*.[1101] As we explained in the *2015 Open Internet Order*, "practices that fail to protect the confidentiality of end users' proprietary information" are among the potential carrier practices that are "unlawful if they unreasonably interfere with or disadvantage end-user consumers' ability to select, access, or use broadband services, applications, or content."[1102] Above, we noted that financial incentives to surrender privacy rights in connection with BIAS are one sort of practice that could potentially run afoul of this standard, and we will accordingly monitor such practices closely. Yet, aside from prohibiting "take-it-or-leave-it" offerings, we do not engage in any *ex ante* prohibition of such practices.[1103]

369. In addition, Sections 201(b) and 202(a) provide backstop authority to ensure that no gaps are formed in Congress's multi-statute regulatory framework governing commercial privacy and data security practices. As explained above, the FTC's enabling statute grants the agency broad authority with respect to such practices, but denies it authority over common carrier activities of common carriers.[1104] *14068 That leaves this Commission as the sole federal agency with authority to regulate telecommunications carriers' treatment of personal and proprietary customer data obtained in the provision of BIAS and other telecommunications services. While we believe Section 222 endows the Commission with ample authority for the rules we adopt today to protect such data, both as to CPNI and other customer PI, Sections 201(b) and 202(a) provide an independent legal basis for the rules. Indeed, both this Commission and the FTC have long recognized that similar conduct would tend to run afoul of Section 201(b) and of Section 5 of the FTC Act, the statutory linchpin of the FTC's privacy and data security enforcement work.[1105] Thus, asserting Sections 201(b) and 202(a) as a basis for our rules merely preserves consistent treatment of companies that collect sensitive customer information—including Social Security numbers and financial records— regardless of whether the company operates under the FCC's or FTC's authority.

**114 370. Accordingly, for these reasons and others discussed throughout this Report and Order, we find that Sections 201(b) and 202(a) by their own terms, consistent the *2015 Open Internet Order*'s interpretation of those provisions in the context of BIAS, provide authority for the adoption of these rules. Also, while we recognize that telecommunications services other than BIAS are beyond the reach of the open Internet rules, providers of such services remain subject to enforcement directly under Sections 201(b) and 202(a), and those provisions authorize adoption of these rules.

C. Title III of the Communications Act Provides Independent Authority

371. With respect to mobile BIAS and other mobile telecommunications services, the rules we adopt in this Order are also independently supported by our authority under Title III of the Act to protect the public interest through spectrum licensing.[1106] Section 303(b) directs the Commission, consistent with the public interest, to "[p]rescribe the nature of the service to be rendered

by each class of licensed stations and each station within any class."[1107] These rules do so.[1108] They lay down rules about "the nature of the service to be rendered" by licensed entities providing mobile telecommunications service; making clear that this service may not be offered in ways that harm the interests of consumers is protecting the confidentiality of their personal information.[1109] Today's rules specify the form this service must take for those who offer it pursuant to license. In providing such licensed service, carriers must adhere to the rules we adopt today. Section 303(r) also supplements the Commission's authority to carry out its mandates through rulemaking,[1110] and Section 316 authorizes the Commission to adopt new conditions on existing licenses if it determines that such action "will promote the public interest, convenience, and necessity."[1111] Throughout this Order, we determine that the rules adopted here will promote the public interest.

***14069 D. The Rules Are Also Consistent With the Purposes of Section 706 of the 1996 Act**

372. We also believe that our rules are consistent with Section 706 of the 1996 Act and will help advance its objective of promoting "the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[1112] We agree with commenters that strong broadband privacy and data security practices tend to promote consumer trust and confidence, which can increase demand for broadband and ultimately spur additional facilities deployment.[1113] Moreover, we have adopted a flexible set of rules that are largely consistent with the FTC's approach to privacy regulation, creating a measure of consistency across the telecommunications ecosystem. We thus reject any argument that the rules will impose novel costs or burdens on BIAS providers and other telecommunications carriers that would discourage further deployment of advanced services.[1114]

E. We Have Authority to Apply the Rules to Interconnected VoIP Services

****115** 373. In 2007, the Commission exercised ancillary jurisdiction to extend its Part 64 CPNI rules to interconnected VoIP services.[1115] Since then, interconnected VoIP providers have operated under these rules. Today, we exercise the same authority[1116] to apply to interconnected VoIP services the harmonized set of rules we are adopting for BIAS and other telecommunications services. Interconnected VoIP services remain within the Commission's subject matter jurisdiction, and we continue to find that the application of customer privacy requirements to these services is "reasonably ancillary to the effective performance" of our statutory responsibilities.[1117] As the Commission explained in 2007, "American consumers [can reasonably] expect that their telephone calls are private irrespective of whether the call is made using the service of a wireline carrier, a wireless carrier, or an interconnected VoIP provider."[1118] ***14070** Furthermore, " extending Section 222's protections to interconnected VoIP service customers is necessary to protect the privacy of wireline or wireless customers that place calls to or receive calls from interconnected VoIP providers."[1119] These rationales hold equally true today. In addition, in 2008, Congress ratified the Commission's decision to apply Section 222's requirements to interconnected VoIP by adding language to Section 222 that expressly covers "IP-enabled voice service,"[1120] defined expressly to incorporate the Commission's definition of "interconnected VoIP service."[1121]

374. We believe that the rules we adopt today are no less suitable for interconnected VoIP service, and are in fact better tailored to that service, than the rules adopted in 2007. As explained above, we have adopted a harmonized set of rules for voice services and BIAS. There is considerable flexibility built into these rules to permit providers of different services and with different business models to adopt privacy practices appropriate for their businesses.[1122] Moreover, while the Order expands on existing obligations in some respects, it also streamlines or removes several of the more prescriptive requirements codified in the existing rules.[1123] We have also broadened the enterprise customer exemption[1124] and taken measures to address the potential for disproportionate impacts on smaller providers, including those that provide interconnected VoIP service.[1125] We therefore are not persuaded that our rules will overburden interconnected VoIP providers in particular with "expand[ed] privacy obligations" that would "forestall competition."[1126]

F. Constitutional Considerations

1. Our Sensitivity-Based Choice Framework Is Supported by the Constitution

375. In adopting section 222, Congress identified a substantial government interest in protecting the privacy of customers of telecommunications services. In adopting and revising rules pursuant to section 222 we have recognized and honored that same substantial interest. Nonetheless, because our rules require carries to provide their customers with tools to grant or deny the carriers approval to use customer information for marketing and other purposes, they can be said to restrict certain types of commercial speech by telecommunications carriers, and therefore must be narrowly tailored to further that substantial government interest.[1127] In the *Central Hudson* case, the Supreme Court found that in order to meet the requirement that rules implicating commercial speech are narrowly tailored to meet a substantial government interest, the government must conduct a threshold inquiry regarding whether the commercial speech concerns lawful activity and is not misleading.[1128] If this threshold requirement is met, as it is here, the government may restrict the speech only if (1) the government interest advanced by the regulation is substantial; (2) the regulation directly and materially advances that interest; and (3) the regulation is not more extensive than necessary to serve the interest.[1129] By adopting a sensitivity-based ***14071** framework for giving customers tools to make decisions about their telecommunications carriers' use and sharing of their information, the rules we adopt today meet that three part test.

a. Substantial Government Interest

****116** 376. We agree with the D.C. Circuit that Section 222 seeks to promote a substantial public interest in protecting consumer privacy.[1130] The record indicates broad agreement on this point,[1131] which is further reinforced by the wealth of case law reiterating the substantial state interest in protecting privacy.[1132] Section 222 is designed to protect the interest of telecommunications consumers in limiting unexpected and unwanted use and disclosure of their personal information by carriers that must collect such information in order to provide the telecommunications service,[1133] and the record further indicates that customers' ability to know and control the information gathered by virtue of their relationships with their telecommunications providers also comprises a substantial government interest.[1134]

377. The failure to adequately protect customer PI can have myriad negative consequences for customers and society at large. Revelations of private facts have been recognized as harms since at least the time of Justices Warren and Brandeis.[1135] Failure to protect the privacy of consumer information can, of course create a risk of financial harm, identity theft and physical threat.[1136] The Commission has also found that emotional and dignitary harms are privacy harms, in other contexts.[1137] The FTC similarly recognized that harms beyond the economic, physical, and intrusive are nonetheless real and ***14072** cognizable,[1138] and the Administration's CPBR defines "privacy risk"" to include the potential to cause "emotional distress, or physical, financial, professional, or other harm to an individual."[1139]

378. Some commenters argue that the Commission can only demonstrate an interest in addressing the *disclosure* of customer PI and not in how carriers' *use* customer PI.[1140] We disagree. The Supreme Court has recognized that an important part of privacy is the right to know and have an effective voice in how one's information is being used, holding that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[1141] The D.C. Circuit has similarly held that "it is widely accepted that privacy deals with determining for oneself when, how, and to whom personal information will be disclosed to others."[1142] This conception of privacy is embedded within the history of the Fair Information Practice Principles[1143] (which form the broadly-supported[1144] basis for our privacy rules), and within the long

history of communications privacy as well.[1145] Scholarly literature on privacy also finds that misuse by the collecting entity can harm individuals' privacy, even apart from disclosure.[1146]

379. Direct surveys confirm consumers' recognition of these harms. According to the 2016 Consumer Privacy Index by TRUSTe and the National Cybersecurity Alliance, 68 percent of consumers were more concerned about not knowing how personal information was collected online than losing their principal income.[1147] The Consumer Privacy Index also indicated that large numbers of consumers want control over who has access to personal information (45 percent), how that information is used (42 percent), and the type of information collected (41 percent).[1148] Consumers also object to their data being ***14073** used, and not only disclosed, in the service of targeted advertising.[1149] These studies demonstrate empirically that consumers find loss of control over their information harmful, even apart from potential monetary loss.

****117** 380. The risk of privacy harms directly affects behavior and activity by eroding trust in and use of communications networks. As the Commission has found, if "consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand."[1150] There is evidence that unexpected uses of private customer information can increase fear, uncertainty, powerlessness, and vulnerability.[1151] This is not a purely academic concern; the National Telecommunications and Information Administration (NTIA) recently found that fear of privacy violations chills online activity, to the point where privacy concerns prevented 45 percent of online households from conducting financial transactions, buying goods or services, or posting on social networks.[1152] The Consumer Privacy Index found that 74 percent of respondents limited their activity in the past year due to privacy concerns, including 36 percent who stopped using certain websites and 29 percent stopped using an app.[1153] In contrast, when companies protect consumers' privacy, consumers' adoption of their products, services, and technologies increases.[1154]

381. We therefore conclude that the government's interest in protecting customer privacy is a substantial one—a fact recognized widely by consumers, the courts, and the Communications Act.

b. Direct and Material Advancement

382. The choice framework that we adopt directly and materially advances the substantial government interests discussed above.[1155] We find that requiring customer approval for use and disclosure of customer PI prevents information uniquely collected and collated by telecommunications carriers from being used or disclosed against a customer's wishes, consistent with customer expectations, and as such directly and materially advances the government's substantial government interest in protecting customers' privacy.[1156] Customers have an important interest in ensuring that their personal ***14074** information is not used by their BIAS providers or other telecommunications carrier without their prior approval in a way that the customers do not or cannot reasonably expect.[1157]

383. In addition, requiring telecommunications carriers to obtain opt-in approval for the use and sharing of sensitive customer PI materially advances the government's interest in protecting telecommunications customers' privacy and in enabling customer to avoid unwanted and unexpected use and disclosure of sensitive customer PI. The opt-in requirements we adopt today provide telecommunications customers control over how their sensitive customer PI can be used for purposes besides those essential to the delivery of service. Likewise, we conclude that opt-out directly and materially advances the government's interest that a customer be given an opportunity to approve (or disapprove) uses of his non-sensitive customer PI by mandating that carriers provide prior notice to customers along with an opportunity to decline the carriers' requested use.

c. The Rules Are No More Burdensome than Necessary to Advance the Government's Substantial Interest

**118 384. *Central Hudson* requires that regulations on commercial speech be no more extensive than necessary to advance the substantial interest.[1158] This does not mean that a regulation must be as narrow as possible, however. The Supreme Court has held that "[t]he government is not required to employ the least restrictive means conceivable ... a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is in proportion to the interest served."[1159] As explained below, our framework satisfies this test.

385. *Non-Sensitive Customer PI*. In most cases involving what we categorize as non-sensitive customer PI, we find opt-in approval unnecessary to ensure adequate customer choice. We therefore find that the opt-out framework for use and sharing of non-sensitive customer PI is a narrowly tailored means to directly and materially advance the government's interest in protecting consumers from unapproved use of non-sensitive customer PI by telecommunications carriers. The record reflects that non-sensitive information naturally generates fewer privacy concerns for customers, and as such does not require the same level of customer approval as for sensitive customer PI.[1160] Further, the record reflects that customers expect their providers to use their non-sensitive information to market improved services, lower-priced service offerings, promotional discounts for new services, and other offers of value from telecommunications carriers and their affiliates. The record also demonstrates that customers can reap significant benefits in the form of more personalized service offerings and possible cost saving from their carriers providing services based on the non-sensitive customer PI that carriers collect.[1161] Requiring carriers to obtain opt-out consent from customers to use and share their non-sensitive information grants carriers flexibility to make improvements and innovations based on customer PI, while still ensuring that customers can control the use and sharing of their non-sensitive customer PI.

386. *Sensitive Customer PI*. We require opt-in approval only for the most important *14075 information to customers—sensitive customer PI. We find that requiring opt-in approval for the use and sharing of sensitive customer PI is a narrowly-tailored means of advancing the Commission's interests in protecting the privacy of sensitive customer PI, and in enabling customers meaningful choice on the use and sharing of such sensitive customer PI. As discussed above in detail, the record reflects that customers reasonably expect that their sensitive information will not be shared without their affirmative consent.[1162] Furthermore, it has been our experience implementing Section 222 that sensitive information, being more likely to lead to more serious customer harm, requires additional protection,[1163] and the record here supports that view.[1164] Commenters nearly unanimously argue that use and sharing of sensitive customer information be subject to customer opt-in approval.[1165] Although we recognize that opt-in imposes additional costs, we find that opt-in is warranted to maximize opportunities for informed choice about sensitive information.

**119 387. In contrast, we find that opt-out consent would be insufficient to protect the privacy of sensitive customer PI.[1166] As we explain above, research has shown that default choices can be "sticky," meaning that consumers will remain in the default position, even if they would not have actively chosen it.[1167] From this, we conclude that an opt-out regime for use and sharing of sensitive customer PI would not materially and directly advance the government's interest in protecting customer privacy because it would not adequately address customers' expectations that their sensitive customer PI is not used without their affirmative consent.

2. Other First Amendment Arguments

388. *Strict Scrutiny Under* Sorrell. The customer choice rules we adopt today do not impermissibly target particular speech or speakers, and thus a strict scrutiny analysis under *Sorrell v. IMS Health Inc.*[1168] is unwarranted. In *Sorrell*, the state of Vermont specifically targeted "drug detailers" and their marketing speech, which the state disfavored, in a framework that otherwise permitted communications about medical prescriptions.[1169] By contrast, the rules adopted here do not disfavor any particular activity. While a large number of commenters are particularly concerned with the limitations that the rules may place upon marketing, customers' privacy interests reach far beyond targeted marketing, to include for instance risk of identity theft or other fraud, stalking, and revelations of private communications, as well as the harms inherent in lacking control over the uses of their proprietary information.

389. The fact that Section 222 and our rules thereunder apply to certain types of information and certain providers is a function of their tailoring, not indications that they are content-based. As explained above, our rules are tailored to address unique characteristics of telecommunications services and of the relationship between telecommunications carriers and their customers.[1170] Were we to interpret *Sorrell* to hold sector-specific privacy laws such as Section 222 and our rules to be content-based simply ***14076** because they do not apply to all entities equally, it would stand to invalidate nearly every federal privacy law, considering the sectoral nature of our federal privacy statutes.[1171] However, *Sorrell* stands for no such thing, itself citing HIPAA—limited to covering certain specific entities and types of information—as an example of a constitutionally sound privacy protection.[1172]

390. *Compelled Speech*. Some commenters argue that the notice requirements unconstitutionally compel speech from carriers.[1173] We disagree. Requirements to include purely factual and uncontroversial information in commercial speech are constitutional so long as they are reasonably related to the government's substantial interest in protecting consumers.[1174] The notice requirements we adopt here, just like the notice requirements in the CPNI rules before them and like numerous notice and labeling requirements before,[1175] require only that companies provide factual and uncontroversial information to consumers.

****120** 391. *Constitutional Avoidance*. Some commenters raise arguments citing the canon of constitutional avoidance.[1176] We do not believe this is applicable. Constitutional avoidance is a canon of statutory interpretation that states that a court should not resolve a case "by deciding a constitutional question if it can be resolved in some other fashion."[1177] As the Supreme Court has held, "[t]he so-called canon of constitutional avoidance is an interpretive tool, counseling that ambiguous statutory language be construed to avoid serious constitutional doubts."[1178] The Court further found "no precedent for applying it to limit the scope of authorized executive action."[1179] The canon of constitutional avoidance therefore does not apply to this proceeding, does not require that we adopt an opt-out framework, and does not mandate that we avoid regulating in this space.

392. Finally, to the extent that parties argue that today's rules deny carriers a First Amendment right of editorial control or impose prior restraints that implicate the First Amendment,[1180] we note that it is well established that common carriers transmitting speech through communications networks are not speakers for First Amendment purposes.[1181]

***14077 G. Severability**

393. In this Report and Order, we adopt a unified scheme of privacy protections for customers of BIAS and other telecommunications services. While the unity and comprehensiveness of this scheme maximizes its utility, we clarify that its constituent elements each operate independently to protect consumers. Were any element of this scheme stayed or invalidated by a reviewing court, the elements that remained in effect would continue to provide vital consumer protections. For instance, telecommunications customers have long benefitted from Commission rules governing the treatment CPNI. The rules we adopt today would continue to ensure that such information is protected even if they did not extend to all of the information we define as customer PI. Similarly, the different forms of conduct regulated under Section 222—use, disclosure, and permission of access—each pose distinct threats to the confidentiality of customer PI. Finally, the benefit of the rules for customers of any particular telecommunications service does not hinge on the same rules applying to other telecommunications services. Accordingly, we consider each of the rules adopted in this Report and Order to be severable, both internally and from the remaining rules. In the event of a stay or invalidation of any part of any rule, or of any rule as it applies as to certain services, providers, forms of conduct, or categories of information, the Commission's intent is to otherwise preserve the rule to the fullest possible extent.

V. PROCEDURAL MATTERS

A. Regulatory Flexibility Analysis

394. As required by the Regulatory Flexibility Act of 1980 (RFA),[1182] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Broadband Privacy NPRM*.[1183] The Commission sought written public comment on the possible significant economic impact on small entities regarding the proposals address in the *2016 Broadband Privacy NPRM*, including comments on the IRFA. Pursuant to the RFA, a Final Regulatory Flexibility Analysis is set forth in Appendix B.

B. Paperwork Reduction Act

****121** 395. This document contains new information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other federal agencies are invited to comment on the new information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

396. In this present document, we require telecommunications carriers to: 1) disclose their privacy practices to customers; 2) provide customers a mechanism for opting in or out of the use or sharing of their customer PI; 3) notify customers of any unauthorized disclosure or use of their customer PI; and 4) provide customers clear and conspicuous notice regarding any financial incentive programs related to the use or disclosure of their customer PI. We have assessed the effects of these changes and find that the burdens on small businesses will be addressed through the implementation plan adopted in this Order, as well as accommodations made in response to small carriers concerns on the record. The privacy policy notice rules, for example, afford carriers significant flexibility on how to comply with the notice requirement. They mandate neither a specific format nor specific content to be contained in the notice. We have also directed the Commission's Consumer Advisory Committee to develop a standardized notice format that will serve as a safe harbor once adopted. Similarly, the choice rules do ***14078** not prescribe a specific format for accepting a customer's privacy choices. The choice rules are also significantly harmonized with existing rules, with which most small providers currently comply. Additionally, the heightened requirements for financial incentive programs allow all providers considerable latitude to develop their programs within the parameters of the rule. Finally, the data breach notification rules incorporate both a harm trigger and notification timeline that significantly lessen the implementation requirements for small providers.

C. Congressional Review Act

397. The Commission will send a copy of this Report and Order in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act (CRA), see 5 U.S.C. § 801(a)(1)(A).

D. Accessible Formats

398. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to fcc504 @fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

VI. ORDERING CLAUSES

****122** 399. Accordingly, IT IS ORDERED that, pursuant to Sections 1, 2, 4(i)-(j), 201, 202, 222, 303(b), 303(r), 316, 338(i), 631, and 705 of the Communications Act of 1934, as amended, and Section 706 of the Telecommunications Act of 1996, as amended, 47 U.S.C. §§ 151, 152, 154(i)-(j), 201, 202, 222, 303(b), 303(r), 316, 338(i), 551, 605, 1302, this Report and Order IS ADOPTED.

400. IT IS FURTHER ORDERED that part 64 of the Commission's rules IS AMENDED as set forth in Appendix A.

401. IT IS FURTHER ORDERED that the data security requirements set forth in new 47 CFR § 64.2005 SHALL BE effective 90 days after publication in the Federal Register.

402. IT IS FURTHER ORDERED that, except as set forth in the prior paragraph, this Report and Order SHALL BE effective 30 days after publication of a summary in the Federal Register, except that the amendments to 47 CFR §§ 64.2003, 64.2004, 64.2006, and 64.2011(b), which contain new or modified information collection requirements that require approval by the Office of Management and Budget under the Paperwork Reduction Act, WILL BECOME EFFECTIVE after the Commission publishes a notice in the Federal Register announcing such approval and the relevant effective date. It is our intention in adopting the foregoing Report and Order that, if any provision of the Report and Order or the rules, or the application thereof to any person or circumstance, is held to be unlawful, the remaining portions of such Report and Order and the rules not deemed unlawful, and the application of such Report and Order and the rules to other person or circumstances, shall remain in effect to the fullest extent permitted by law.

403. IT IS FURTHER ORDERED that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. § 801(a)(1)(A).

**123 404. IT IS FURTHER ORDERED that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

*14079 Marlene H. Dortch
Secretary

*14080 **APPENDIX A**

Final Rules

**124 The Federal Communications Commission proposes to amend 47 CFR part 64 to read as follows:

PART 64 — MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

1. The authority citation for Part 64 is revised to read as follows:

AUTHORITY: 47 U.S.C. 154, 254(k), 403, Pub. L. 104-104, 110 Stat. 56. Interpret or apply 47 U.S.C. 201, 202, 218, 222, 225, 226, 227, 228, 254(k), 301, 303, 332, 338, 551, 616, 620, 705, 1302, and the Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. 112-96, unless otherwise noted.

2. Revise Subpart U to read as follows:

Subpart U — Protecting Customer Information

§ 64.2001 Basis and Purpose.

(a) *Basis*. The rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.

(b) *Purpose*. The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222.

§ 64.2002 Definitions.

(a) Broadband Internet access service (BIAS). The term "broadband Internet access service" or "BIAS" has the same meaning given to such term in section 8.2(a) of this chapter.

(b) Broadband Internet Access service provider. The term "broadband Internet access service provider" or "BIAS provider" means a person engaged in the provision of BIAS.

(c) Breach of security. The terms "breach of security," "breach," or "data breach," mean any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information.

(d) Call detail information. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

****125** (e) Customer. A customer of a telecommunications carrier is (1) a current or former subscriber to a telecommunications service; or (2) an applicant for a telecommunications service.

(f) Customer proprietary information. The term "customer proprietary information" or "customer PI" means any of the following a carrier acquires in connection with its provision of telecommunications service:

(1) Individually identifiable customer proprietary network information (CPNI);

(2) Personally identifiable information (PII); and

(3) Content of communications.

(g) Customer proprietary network information (CPNI). The term "customer proprietary network information" or "CPNI" has the same meaning given to such term in section 222(h)(1) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(1).

***14081** (h) Interconnected Voice over Internet Protocol (VoIP) Service. The term "interconnected VoIP service" has the same meaning given to such term in subsection (h) of this section.

(i) Material change. The term "material change" means any change that a customer, acting reasonably under the circumstances, would consider important to his or her decisions regarding his or her privacy, including any change to information required by the privacy notice described in section 64.2003.

(j) Opt-in approval. A method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the customer proprietary information after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

(k) Opt-out approval. A method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's proprietary information if the customer has failed to object thereto after the customer is provided appropriate notification of the carrier's request for consent consistent with the requirements set forth in this subpart.

(l) Person. The term "person" has the same meaning given such term in section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153.

(m) Personally identifiable information (PII). The term "personally identifiable information" or "PII" means any information that is linked or reasonably linkable to an individual or device.

(n) Sensitive customer proprietary information. The terms "sensitive customer proprietary information" or "sensitive customer PI" include:
**126 (1) financial information;

(2) health information;

(3) information pertaining to children;

(4) Social Security numbers;

(5) precise geo-location information;

(6) content of communications;

(7) call detail information; and

(8) web browsing history, application usage history, and the functional equivalents of either.

(o) Telecommunications carrier or carrier. The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153. For the purposes of this subpart, the term "telecommunications carrier" or "carrier" shall include a person engaged in the provision of interconnected VoIP service, as that term is defined in subsection (h) of this section.

(p) Telecommunications service. The term "telecommunications service" has the same meaning given to such term in section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153. For the purposes of this subpart, the term ""telecommunications service" shall include interconnected VoIP service, as that term is defined in subsection (h) of this section.

§ 64.2003 Notice Requirements for Telecommunications Carriers.
(a) A telecommunications carrier must notify its customers of its privacy policies. Such notice must be clear and conspicuous, and in language that is comprehensible and not misleading.

(b) *Contents*. A telecommunications carrier's notice of its privacy policies under subsection (a) must:

*14082 (1) Specify and describe the types of customer proprietary information that the telecommunications carrier collects by virtue of its provision of telecommunications service and how it uses that information;

(2) Specify and describe under what circumstances the telecommunications carrier discloses or permits access to each type of customer proprietary information that it collects;

(3) Specify and describe the categories of entities to which the carrier discloses or permits access to customer proprietary information and the purposes for which the customer proprietary information will be used by each category of entities;

(4) Specify and describe customers' opt-in approval and/or opt-out approval rights with respect to their customer proprietary information, including:

(i) That a customer's denial or withdrawal of approval to use, disclose, or permit access to customer proprietary information will not affect the provision of any telecommunications services of which he or she is a customer; and

(ii) That any grant, denial, or withdrawal of approval for the use, disclosure, or permission of access to the customer proprietary information is valid until the customer affirmatively revokes such grant, denial, or withdrawal, and inform the customer of his or her right to deny or withdraw access to such proprietary information at any time.

****127** (5) Provide access to a mechanism for customers to grant, deny, or withdraw approval for the telecommunications carrier to use, disclose, or provide access to customer proprietary information as required by section 64.2004 of this subpart;

(6) Be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

(c) *Timing*. Notice required under subsection (a) must:

(1) Be made available to prospective customers at the point of sale, prior to the purchase of service, whether such point of sale is in person, online, over the telephone, or via another means; and

(2) Be made persistently available through: a clear and conspicuous link on the telecommunications carrier's homepage; the carrier's application (app), if it provides one for account management purposes; and any functional equivalent to the carrier's homepage or app. If a carrier does not have a website, it must provide notice to customers in paper form or another format agreed upon by the customer.

(d) *Material changes to a telecommunications carrier's privacy policies*. A telecommunications carrier must provide existing customers with advance notice of one or more material changes to the carrier's privacy policies. Such notice must be clear and conspicuous, and in language that is comprehensible and not misleading, and must:

(1) Be provided through email or another means of active communication agreed upon by the customer;

(2) Specify and describe:

(i) The changes made to the telecommunications carrier's privacy policies, including any changes to what customer proprietary information the carrier collects, and how it uses, discloses, or permits access to such information, the categories of entities to which it discloses or permits access to customer proprietary information, and which, if any, changes are retroactive; and

***14083** (ii) Customers' opt-in approval and/or opt-out approval rights with respect to their customer proprietary information, including the material specified in subsection (b)(4) of this section;

(3) Provide access to a mechanism for customers to grant, deny, or withdraw approval for the telecommunications carrier to use, disclose, or permit access to customer proprietary information as required by section 64.2004 of this subpart; and

(4) Be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

§ 64.2004 Customer Approval.

Except as described in subsection (a), a telecommunications carrier may not use, disclose, or permit access to customer proprietary information except with the opt-out or opt-in approval of a customer as described in this section.

(a) *Limitations and Exceptions*. A telecommunications carrier may use, disclose, or permit access to customer proprietary information without customer approval for the following purposes:

****128** (1) In its provision of the telecommunications service from which such information is derived, or in its provision of services necessary to, or used in, the provision of such service.

(2) To initiate, render, bill, and collect for telecommunications service.

(3) To protect the rights or property of the telecommunications carrier, or to protect users of the telecommunications service and other providers from fraudulent, abusive, or unlawful use of the service.

(4) To provide any inbound marketing, referral, or administrative services to the customer for the duration of a real-time interaction, if such interaction was initiated by the customer.

(5) To provide location information and/or non-sensitive customer proprietary information to:

(i) A public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's request for emergency services;

(ii) Inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(iii) Providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(6) As otherwise required or authorized by law.

(b) *Opt-Out Approval Required*. Except as otherwise provided in this section, a telecommunications carrier must obtain opt-out approval from a customer to use, disclose, or permit access to any of the customer's non-sensitive customer proprietary information. If it so chooses, a telecommunications carrier may instead obtain opt-in approval from a customer to use, disclose, or permit access to any of the customer's non-sensitive customer proprietary information.

(c) *Opt-In Approval Required*. Except as otherwise provided in this section, a telecommunications carrier must obtain opt-in approval from a customer to:

(1) use, disclose, or permit access to any of the customer's sensitive customer proprietary information; or

***14084** (2) make any material retroactive change—i.e., a material change that would result in a use, disclosure, or permission of access to any of the customer's proprietary information previously collected by the carrier for which the customer did not previously grant approval, either through opt-in or opt-out consent, as required by subsections (b) and (c) of this section.

(d) *Notice and Solicitation Required*.

(1) Except as described in subsection (a) of this section, a telecommunications carrier must at a minimum solicit customer approval pursuant to subsection (b) and/or (c), as applicable, at the point of sale and when making one or more material changes to privacy policies. Such solicitation may be part of, or the same communication as, a notice required by section 64.2003 of these rules.

****129** (2) A telecommunications carrier's solicitation of customer approval must be clear and conspicuous, and in language that is comprehensible and not misleading. Such solicitation must disclose:

(i) The types of customer proprietary information for which the carrier is seeking customer approval to use, disclose, or permit access to;

(ii) The purposes for which such customer proprietary information will be used;

(iii) The categories of entities to which the carrier intends to disclose or permit access to such customer proprietary information; and

(iv) A means to easily access the notice required by section 64.2003(a) of this subpart and a means to access the mechanism required by subsection (e).

(3) A telecommunications carrier's solicitation of customer approval must be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

(e) *Mechanism for Exercising Customer Approval*. A telecommunications carrier must make available a simple, easy-to-use mechanism for customers to grant, deny, or withdraw opt-in approval and/or opt-out approval at any time. Such mechanism must be clear and conspicuous, in language that is comprehensible and not misleading, and made available at no additional cost to the customer. Such mechanism must be persistently available on or through the carrier's website; the carrier's application (app), if it provides one for account management purposes; and any functional equivalent to the carrier's homepage or app. If a carrier does not have a website, it must provide a persistently available mechanism by another means such as a toll-free telephone number. The customer's grant, denial, or withdrawal of approval must be given effect promptly and remain in effect until the customer revokes or limits such grant, denial, or withdrawal of approval.

§ 64.2005 Data Security.

(a) A telecommunications carrier must take reasonable measures to protect customer PI from unauthorized use, disclosure, or access.

(b) The security measures taken by a telecommunications carrier to implement the requirement set forth in this section must appropriately take into account each of the following factors:
(1) The nature and scope of the telecommunications carrier's activities;

(2) The sensitivity of the data it collects;

(3) The size of the telecommunications carrier; and

(4) Technical feasibility.

***14085** (c) A telecommunications carrier may employ any lawful security measures that allow it to implement the requirement set forth in this section.

§ 64.2006 Data Breach Notification.

(a) *Customer Notification*. A telecommunications carrier shall notify affected customers of any breach without unreasonable delay and in any event no later than 30 calendar days after the carrier reasonably determines that a breach has occurred, subject to law enforcement needs, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach.

****130** (1) A telecommunications carrier required to provide notification to a customer under this subsection must provide such notice by one or more of the following methods:

(i) Written notification sent to either the customer's email address or the postal address of record of the customer, or, for former customers, to the last postal address ascertainable after reasonable investigation using commonly available sources; or

(ii) Other electronic means of active communications agreed upon by the customer for contacting that customer for data breach notification purposes.

(2) The customer notification required to be provided under this subsection must include:

(i) The date, estimated date, or estimated date range of the breach of security;

(ii) A description of the customer PI that was breached or reasonably believed to have been breached;

(iii) Information the customer can use to contact the telecommunications carrier to inquire about the breach of security and the customer PI that the telecommunications carrier maintains about that customer;

(iv) Information about how to contact the Federal Communications Commission and any state regulatory agencies relevant to the customer and the service; and

(v) If the breach creates a risk of financial harm, information about the national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, credit freezes, or other consumer protections the telecommunications carrier is offering customers affected by the breach of security.

(b) *Commission Notification*. A telecommunications carrier must notify the Commission of any breach affecting 5,000 or more customers no later than seven business days after the carrier reasonably determines that a breach has occurred and at least three business days before notification to the affected customers, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. A telecommunications carrier must notify the Commission of any breach affecting fewer than 5,000 customers without unreasonable delay and no later than thirty (30) calendar days after the carrier reasonably determines that a breach has occurred, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. Such notification shall be made through a central reporting system made available by the Commission.

(c) *Federal Law Enforcement Notification*. A telecommunications carrier must notify the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Secret Service) of a breach that affects 5,000 or more customers no later than seven business days after the carrier reasonably determines that such a breach has occurred and at least three business days before notification to the affected customers, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. Such notification shall be made through a central reporting system made available by the Commission.

****131** (d) *Recordkeeping*. A telecommunications carrier shall maintain a record, electronically or in some ***14086** other manner, of any breaches and notifications made to customers, unless the telecommunications carrier can reasonably determine

that no harm to customers is reasonably likely to occur as a result of the breach. The record must include the dates on which the carrier determines that a reportable breach has occurred and the dates of customer notification. The record must include a written copy of all customer notifications. Carriers shall retain the record for a minimum of two years from the date on which the carrier determines that a reportable breach has occurred.

§ 64.2010 Business Customer Exemption for Provision of Telecommunications Services other than BIAS.

Telecommunications carriers may bind themselves contractually to privacy and data security regimes other than those described in this subpart for the provision of telecommunications services other than BIAS to enterprise customers if the carrier's contract with that customer specifically addresses the issues of transparency, choice, data security, and data breach and provides a mechanism for the customer to communicate with the carriers about privacy and data security concerns.

§ 64.2011 BIAS Offers Conditioned on Waiver of Privacy Rights.

(a) A BIAS provider must not condition, or effectively condition, provision of BIAS on a customer's agreement to waive privacy rights guaranteed by law or regulation, including this subpart. A BIAS provider must not terminate service or otherwise refuse to provide BIAS as a direct or indirect consequence of a customer's refusal to waive any such privacy rights.

(b) A BIAS provider that offers a financial incentive, such as lower monthly rates, in exchange for a customer's approval to use, disclose, and/or permit access to the customer's proprietary information must do all of the following:

(1) Provide notice explaining the terms of any financial incentive program that is clear and conspicuous, and in language that is comprehensible and not misleading. Such notice must be provided both at the time the program is offered and at the time a customer elects to participate in the program. Such notice must:

(i) Explain that the program requires opt-in approval to use, disclose, and/or permit access to customer PI;

(ii) Include information about what customer PI the provider will collect, how it will be used, and with what categories of entities it will be shared and for what purposes;

(iii) Be easily accessible and separate from any other privacy notifications, including but not limited to any privacy notifications required by this subpart;

(iv) Be completely translated into a language other than English if the BIAS provider transacts business with the customer in that language; and

(v) Provide at least as prominent information to customers about the equivalent service plan that does not necessitate the use, disclosure, or access to customer PI beyond that required or permitted by law or regulation, including under this subpart.

****132** (2) Obtain customer opt-in approval in accordance with section 64.2004(c) of this subpart for participation in any financial incentive program.

(3) If customer opt-in approval is given, the BIAS provider must make available a simple, easy-to-use mechanism for customers to withdraw approval for participation in such financial incentive program at any time. Such mechanism must be clear and conspicuous, in language that is comprehensible and not misleading, and must be persistently available on or through the carrier's website; the carrier's application (app), if it provides one for account management purposes; and any functional equivalent to the carrier's homepage or app. If a carrier does not have a website, it must provide a persistently available mechanism by another means such as a toll-free telephone number.

***14087 § 64.2012 Effect on State Law.**

The rules set forth in this subpart shall preempt any State law only to the extent that such law is inconsistent with the rules set forth herein and only if the Commission has affirmatively determined that the State law is preempted on a case-by-case basis. The Commission shall not presume that more restrictive State laws are inconsistent with the rules set forth herein.

***14088 APPENDIX B**

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Broadband Privacy NPRM* for this proceeding.[2] The Commission sought written public comment on the proposals in the *Broadband Privacy NPRM*, including comment on the IRFA. The Commission received comments on the IRFA, which are discussed below.[3] This present Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[4]

A. Need for, and Objectives of, the Rules

2. In the Order, we adopt privacy requirements for providers of broadband Internet access service (BIAS) and other telecommunications services.[5] In doing so, we build upon the Commission's long history of protecting customer privacy in the telecommunications sector. Section 222 of the Communications Act provides statutory protections to the privacy of the data that all telecommunications carriers collect from their customers. Section 222(a) imposes a duty on all telecommunications carriers to protect the confidentiality of their customers' "proprietary information," or PI. Section 222(c) imposes restrictions on telecommunications carriers' use and sharing of customer proprietary network information (CPNI) without customer approval, subject to certain exceptions, including as necessary to provide the telecommunications service (or services necessary to or used in providing that telecommunications service), and as required by law.[6]

3. Over the last two decades, the Commission has promulgated, revised, and enforced privacy rules for telecommunications carriers that are focused on implementing the CPNI requirements of Section 222. As practices have changed, the Commission has refined its Section 222 rules. The current Section 222 rules focus on transparency, choice, data security, and data breach notification.

****133** 4. Prior to 2015, BIAS was classified as an information service, which excluded such services from the ambit of Title II of the Act, including Section 222, and the Commission's CPNI rules. Instead, broadband providers were subject to the FTC's unfair and deceptive acts and practices authority. In the *2015 Open Internet Order*, we reclassified BIAS as a telecommunications service subject to Title II of the Act, an action upheld by the D.C. Circuit in *United States Telecom Ass'n v. FCC*. While we granted BIAS forbearance from many Title II provisions, we concluded that application and enforcement of the privacy protections in Section 222 to BIAS is in the public interest and necessary for the protection of consumers. However, we questioned "whether the Commission's current rules implementing section 222 necessarily would be well suited to broadband Internet access service," and forbore from the application of these rules to broadband service, "pending the adoption of rules to govern broadband Internet access service in a separate rulemaking proceeding."[7]

5. In March 2016, we adopted the *Broadband Privacy NPRM*, which proposed a framework ***14089** for applying the longstanding privacy requirements of the Act to BIAS.[8] In the *NPRM*, we proposed rules protecting customer privacy using the three foundations of privacy—transparency, choice, and security—and also sought comment on, among other things, whether we should update rules that govern the application of Section 222 to traditional telephone service and interconnected VoIP service in order to harmonize them with the results of this proceeding.[9]

6. Based on the record gathered in this proceeding, today we adopt a harmonized set of rules applicable to BIAS providers and other telecommunications carriers. The privacy framework we adopt focuses on transparency, choice, and data security, and provides heighted protection for sensitive customer information, consistent with customer expectations. Our need to extend such privacy requirements to BIAS providers is based, in part, on their particular role as network providers and the context of the consumer/BIAS provider relationship. Based on our review of the record, we reaffirm our earlier finding that a broadband provider "sits at a privileged place in the network, the bottleneck between the customer and the rest of the Internet"[10] —a position that we have referred to as a gatekeeper.[11] As such, BIAS providers can collect "an unprecedented breadth" of electronic personal information.[12]

7. In adopting these rules we honor customers' privacy rights and implement the statutory requirement that carriers protect the confidentiality of customer proprietary information. These rules do not prohibit carriers from using or sharing customer information, but rather are designed to protect consumer choice while giving carriers the flexibility they need to continue to innovate. By bolstering customer confidence in carriers' treatment of confidential customer information, we also promote the virtuous cycle of innovation in which new uses of the network lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses, business growth and innovation.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

****134** 8. In response to the *Broadband Privacy NPRM*, five entities filed comments, reply comments, and/or *ex parte* letters that specifically addressed the IRFA to some degree: Alaska Telephone Association, Competitive Carriers Association, NTCA, Rural Wireless Association, and Wireless Internet ***14090** Service Providers Association (WISPA).[13] Some of these, as well as other entities, filed comments, reply comments, and/or *ex parte* letters that more generally considered the small business impact of our proposals.[14]

9. Some commenters recommend that the Commission adopt specific exemptions or provisions to alleviate burdens on small carriers. In particular, commenters recommend that the Commission (1) exempt small carriers from some or all of the rules based on their size and/or practices;[15] (2) give small carriers additional time to comply with the rules;[16] (3) harmonize notice and choice requirements with the preexisting voice CPNI rules;[17] (4) exempt small carriers from any privacy dashboard requirements and otherwise give them flexibility in the structure of their privacy notices;[18] (5) grandfather existing customer approvals for use and disclosure of customer information;[19] (6) exempt small carriers from any opt-in approval requirements;[20] (6) not impose specific data security requirements on small providers;[21] (7) not impose specific data breach reporting deadlines on small providers, and instead allow them to report breaches as soon as practicable;[22] and (8) not hold small carriers liable for misuse of customer PI by third parties with whom they share the information.[23] We considered these proposals and concerns when composing the Order and the accompanying rules.[24]

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

10. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[25]

11. The SBA filed comments in response to the IRFA encouraging the Commission to examine measures, exemptions, and alternatives that would ease compliance by small ***14091** telecommunications carriers with our rules.[26] SBA observed that compliance costs to small providers may include "consulting fees, attorney's fees, hiring or training in-house privacy personnel, customer notification costs, and opportunity costs."[27] In particular, SBA recommends giving small providers more time to comply with the rules and it supports granting small providers an exemption from the rules "wherever practicable.""[28]

12. As explained in detail below, we have taken numerous measures in this Order to alleviate burdens for small providers, consistent with the comments of the SBA. In particular, we have adopted SBA's proposal that we give small providers additional time to comply.[29] Also, while we do not exempt small providers from any of our rules, we have taken alternative measures to address several of the concerns with specific rule proposals that the SBA identifies. For instance, the data security rule we adopt focuses on the "reasonableness" of a carrier's security practices and does not prescribe any minimum required practices a provider must undertake to achieve compliance.[30] The rule also specifically recognizes that the size of the provider is one of the factors to be considered in determining whether a provider has engaged in reasonable data security practices. By formulating the rule in this way, we have addressed small provider concerns regarding the costs of implementing prescriptive requirements.[31] We also note that among other accommodations directly responsive to small provider concerns, we decline to require a consumer-facing dashboard.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

****135** 13. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules.[32] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and ""small governmental jurisdiction."[33] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[34] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[35]

14. For the purposes of these rules, we define small providers as providers with 100,000 or fewer broadband connections as reported on their most recent Form 477, aggregated over all the providers' affiliates. We decline to count based on the number of customers from whom carriers collect ***14092** data, as we recognize that some data collection is necessary to the provisions of service. Cabining the scope of small providers to those serving 100,000 or fewer subscribers is consistent with the *2015 Open Internet Order*.[36]

15. The rules apply to all telecommunications carriers, including providers of BIAS. Below, we describe the types of small entities that might provide these services.

1. Total Small Entities

16. Our rules may, over time, affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three comprehensive, statutory small entity size standards.[37] First, as of 2013, the SBA estimates there are an estimated 28.8 million small businesses nationwide—comprising some 99.9% of all businesses.[38] In addition, a ""small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[39] Nationwide, as of 2007, there were approximately 1,621,315 small organizations.[40] Finally, the term "small governmental jurisdiction" is defined generally as "governments of cities, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[41] Census Bureau data for 2011 indicate that there were 90,056 local governmental jurisdictions in the United States.[42] We estimate that, of this total, as many as 89,327 entities may qualify as "small governmental jurisdictions."[43] Thus, we estimate that most governmental jurisdictions are small.

2. Broadband Internet Access Service Providers

17. The Economic Census places BIAS providers, whose services might include Voice over Internet Protocol (VoIP), in either of two categories, depending on whether the service is provided over the provider's own telecommunications facilities (e.g.,

cable and DSL ISPs), or over client-supplied telecommunications connections (e.g., dial-up ISPs). The former are within the category of Wired Telecommunications Carriers,[44] which has an SBA small business size standard of 1,500 or fewer ***14093** employees.[45] These are also labeled "broadband." The latter are within the category of All Other Telecommunications,[46] which has a size standard of annual receipts of $32.5 million or less.[47] These are labeled non-broadband. According to Census Bureau data for 2012, there were 3,117 firms in the first category, total, that operated for the entire year.[48] Of this total, 3,083 firms had employment of 999 or fewer employees.[49] For the second category, the data show that 1,442 firms operated for the entire year.[50] Of those, 1,400 had annual receipts below $25 million per year. Consequently, we estimate that the majority of broadband Internet access service provider firms are small entities.

****136** 18. The broadband Internet access service provider industry has changed since this definition was introduced in 2007. The data cited above may therefore include entities that no longer provide broadband Internet access service, and may exclude entities that now provide such service. To ensure that this FRFA describes the universe of small entities that our action affects, we discuss in turn several different types of entities that might be providing broadband Internet access service, which also overlap with entities providing other telecommunications services. We note that, although we have no specific information on the number of small entities that provide broadband Internet access service over unlicensed spectrum, we include these entities in our Final Regulatory Flexibility Analysis.

3. Wireline Providers

19. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[51] The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[52] Census data for 2012 shows that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[53] Thus, under this size standard, the majority of firms in this industry can be considered small.

20. *Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers as defined in this FRFA. Under ***14094** the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[54] According to Commission data, census data for 2012 shows that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[55] The Commission therefore estimates that most providers of local exchange carrier service are small entities that may be affected by the rules adopted.

21. *Incumbent Local Exchange Carriers* (*Incumbent LECs*). Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers as defined in this FRFA. Under that size standard, such a business is small if it has 1,500 or fewer employees.[56] According to Commission data, 3,117 firms operated in that year. Of this total, 3,083 operated with fewer than 1,000 employees.[57] Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by the rules and policies adopted. Three hundred and seven (307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers.[58] Of this total, an estimated 1,006 have 1,500 or fewer employees.[59]

****137** 22. *Competitive Local Exchange Carriers (Competitive LECs), Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate NAICS Code category is Wired Telecommunications Carriers, as defined in this FRFA. Under that size standard, such a business is small if it has 1,500 or fewer employees.[60] U.S. Census data for 2012 indicate that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees.[61] Based on this data, the Commission concludes that the majority of Competitive LECS, CAPs, Shared-Tenant Service Providers, and Other Local Service Providers, are small entities. According to Commission data, 1,442 carriers reported that they were engaged in the provision of either competitive local exchange services or competitive access provider services.[62] Of these 1,442 carriers, an estimated 1,256 have 1,500 or fewer employees.[63] In addition, 17 carriers have reported that they are Shared-Tenant Service Providers, and all 17 are estimated to have 1,500 or fewer employees.[64] Also, 72 carriers have reported that they are Other Local Service Providers.[65] Of this total, 70 have 1,500 or fewer employees.[66] Consequently, based on internally researched FCC data, the Commission estimates that ***14095** most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities.

23. We have included small incumbent LECs in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small business size standard (e.g., a telephone communications business having 1,500 or fewer employees), and "is not dominant in its field of operation."[67] The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent LECs are not dominant in their field of operation because any such dominance is not "national" in scope.[68] We have therefore included small incumbent LECs in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

24. *Interexchange Carriers*. Neither the Commission nor the SBA has developed a definition for Interexchange Carriers. The closest NAICS Code category is Wired Telecommunications Carriers as defined in this FRFA. The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[69] U.S. Census data for 2012 indicates that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees.[70] According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.[71] Of this total, an estimated 317 have 1,500 or fewer employees.[72] Consequently, the Commission estimates that the majority of interexchange service providers are small entities that may be affected by the rules adopted.

****138** 25. *Operator Service Providers* (*OSPs*). Neither the Commission nor the SBA has developed a small business size standard specifically for operator service providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[73] According to Commission data, 33 carriers have reported that they are engaged in the provision of operator services. Of these, an estimated 31 have 1,500 or fewer employees and two have more than 1,500 employees.[74] Consequently, the Commission estimates that the majority of OSPs are small entities that may be affected by these rules.

26. *Prepaid Calling Card Providers*. Neither the Commission nor the SBA has developed a small business definition specifically for prepaid calling card providers. The most appropriate NAICS code-based category for defining prepaid calling card providers is Telecommunications Resellers. This industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual ***14096** networks operators (MVNOs) are included in this industry.[75] Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[76] U.S. Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[77] Thus, under this category and the associated small business size standard, the majority of these prepaid calling

card providers can be considered small entities. According to Commission data, 193 carriers have reported that they are engaged in the provision of prepaid calling cards.[78] All 193 carriers have 1,500 or fewer employees.[79] Consequently, the Commission estimates that the majority of prepaid calling card providers are small entities that may be affected by the rules adopted.

27. *Local Resellers*. Neither the Commission nor the SBA has developed a small business size standard specifically for Local Resellers. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[80] Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[81] Under this category and the associated small business size standard, the majority of these local resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services.[82] Of this total, an estimated 211 have 1,500 or fewer employees.[83] Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by the rules adopted.

****139** 28. *Toll Resellers*. The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers, and the SBA has developed a small business size standard for the category of Telecommunications Resellers.[84] Under that size standard, such a business is small if it has 1,500 or fewer employees.[85] Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[86] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[87] Of this total, an estimated 857 have 1,500 or fewer employees.[88] Consequently, the Commission estimates that the majority of toll resellers are small entities.

***14097** 29. *Other Toll Carriers*. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. The closest applicable NAICS Code category is for Wired Telecommunications Carriers as defined in paragraph 6 of this FRFA. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[89] Census data for 2012 shows that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[90] Thus, under this category and the associated small business size standard, the majority of Other Toll Carriers can be considered small. According to internally developed Commission data, 284 companies reported that their primary telecommunications service activity was the provision of other toll carriage.[91] Of these, an estimated 279 have 1,500 or fewer employees.[92] Consequently, the Commission estimates that most Other Toll Carriers are small entities.

4. Wireless Providers — Fixed and Mobile

30. The telecommunications services category covered by these rules may cover multiple wireless firms and categories of regulated wireless services. In addition, for those services subject to auctions, we note that, as a general matter, the number of winning bidders that claim to qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Also, the Commission does not generally track subsequent business size unless, in the context of assignments and transfers or reportable eligibility events, unjust enrichment issues are implicated.

31. *Wireless Telecommunications Carriers (except Satellite*). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[93] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees. For this industry, Census data for 2012 show that there were 967 firms that operated for the entire year. Of this total, 955 firms had fewer than 1,000 employees. Thus under this category and the associated size standard, the Commission

estimates that the majority of wireless telecommunications carriers (except satellite) are small entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) services.[94] Of this total, an estimated 261 have 1,500 or fewer employees.[95] Thus, using available data, we estimate that the majority of wireless firms can be considered small.

****140** 32. *Wireless Communications Services*. This service can be used for fixed, mobile, radiolocation, and digital audio broadcasting satellite uses. The Commission defined "small business" for the wireless communications services (WCS) auction as an entity with average gross revenues of $40 million for each of the three preceding years, and a "very small business" as an entity with average gross ***14098** revenues of $15 million for each of the three preceding years.[96] The SBA has approved these definitions.[97]

33. *1670-1675 MHz Services*. This service can be used for fixed and mobile uses, except aeronautical mobile.[98] An auction for one license in the 1670-1675 MHz band was conducted in 2003. One license was awarded. The winning bidder was not a small entity.

34. *Wireless Telephony*. Wireless telephony includes cellular, personal communications services, and specialized mobile radio telephony carriers. As noted, the SBA has developed a small business size standard for Wireless Telecommunications Carriers (except Satellite).[99] Under the SBA small business size standard, a business is small if it has 1,500 or fewer employees.[100] According to Commission data, 413 carriers reported that they were engaged in wireless telephony.[101] Of these, an estimated 261 have 1,500 or fewer employees and 152 have more than 1,500 employees.[102] Therefore, a little less than one third of these entities can be considered small.

35. *Broadband Personal Communications Service*. The broadband personal communications services (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission initially defined a "small business" for C- and F-Block licenses as an entity that has average gross revenues of $40 million or less in the three previous calendar years.[103] For F-Block licenses, an additional small business size standard for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years.[104] These small business size standards, in the context of broadband PCS auctions, have been approved by the SBA.[105] No small businesses within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that claimed small business status in the first two C-Block auctions. A total of 93 bidders that claimed small business status won approximately 40 percent of the 1,479 licenses in the first auction for the D, E, and F Blocks.[106] On April 15, 1999, the Commission completed the reauction of 347 C-, D-, E-, and F-Block licenses in Auction No. 22.[107] Of the 57 winning bidders in that auction, 48 claimed small business status and won 277 licenses.

***14099** 36. On January 26, 2001, the Commission completed the auction of 422 C and F Block Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in that auction, 29 claimed small business status.[108] Subsequent events concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant. On February 15, 2005, the Commission completed an auction of 242 C-, D-, E-, and F-Block licenses in Auction No. 58. Of the 24 winning bidders in that auction, 16 claimed small business status and won 156 licenses.[109] On May 21, 2007, the Commission completed an auction of 33 licenses in the A, C, and F Blocks in Auction No. 71.[110] Of the 12 winning bidders in that auction, five claimed small business status and won 18 licenses.[111] On August 20, 2008, the Commission completed the auction of 20 C-, D-, E-, and F-Block Broadband PCS licenses in Auction No. 78.[112] Of the eight winning bidders for Broadband PCS licenses in that auction, six claimed small business status and won 14 licenses.[113]

****141** 37. *Specialized Mobile Radio Licenses*. The Commission awards "small entity" bidding credits in auctions for Specialized Mobile Radio (SMR) geographic area licenses in the 800 MHz and 900 MHz bands to firms that had revenues of no more than $15 million in each of the three previous calendar years.[114] The Commission awards "very small entity" bidding credits to firms that had revenues of no more than $3 million in each of the three previous calendar years.[115] The SBA has approved these small business size standards for the 900 MHz Service.[116] The Commission has held auctions for geographic area licenses in the 800 MHz and 900 MHz bands. The 900 MHz SMR auction began on December 5, 1995, and closed on April 15, 1996. Sixty bidders claiming that they qualified as small businesses under the $15 million size standard won 263 geographic area licenses in the 900 MHz SMR band. The 800 MHz SMR auction for the upper 200 channels began on October 28, 1997, and was completed on December 8, 1997. Ten bidders claiming that they qualified as small businesses under the $15 million size standard won 38 geographic area licenses for the upper 200 channels in the 800 MHz SMR band.[117] A second auction for the 800 MHz band was held on January 10, 2002 and closed on January 17, 2002 and included 23 BEA licenses. One bidder claiming small business status won five licenses.[118]

***14100** 38. The auction of the 1,053 800 MHz SMR geographic area licenses for the General Category channels began on August 16, 2000, and was completed on September 1, 2000. Eleven bidders won 108 geographic area licenses for the General Category channels in the 800 MHz SMR band and qualified as small businesses under the $15 million size standard.[119] In an auction completed on December 5, 2000, a total of 2,800 Economic Area licenses in the lower 80 channels of the 800 MHz SMR service were awarded.[120] Of the 22 winning bidders, 19 claimed small business status and won 129 licenses. Thus, combining all four auctions, 41 winning bidders for geographic licenses in the 800 MHz SMR band claimed status as small businesses.

39. In addition, there are numerous incumbent site-by-site SMR licenses and licensees with extended implementation authorizations in the 800 and 900 MHz bands. We do not know how many firms provide 800 MHz or 900 MHz geographic area SMR service pursuant to extended implementation authorizations, nor how many of these providers have annual revenues of no more than $15 million. One firm has over $15 million in revenues. In addition, we do not know how many of these firms have 1,500 or fewer employees, which is the SBA-determined size standard.[121] We assume, for purposes of this analysis, that all of the remaining extended implementation authorizations are held by small entities, as defined by the SBA.

40. *Lower 700 MHz Band Licenses*. The Commission previously adopted criteria for defining three groups of small businesses for purposes of determining their eligibility for special provisions such as bidding credits.[122] The Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years.[123] A "very small business" is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years.[124] Additionally, the lower 700 MHz Service had a third category of small business status for Metropolitan/Rural Service Area (MSA/RSA) licenses—"entrepreneur"—which is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years.[125] The SBA approved these small size standards.[126] An auction of 740 licenses (one license in each of the 734 MSAs/RSAs and one license in each of the six Economic Area Groupings (EAGs)) commenced on August 27, 2002, and closed on September 18, 2002. Of the 740 licenses available for auction, 484 licenses were won by 102 winning bidders. Seventy-two of the winning bidders claimed small business, very small business or entrepreneur status and won a total of 329 licenses.[127] A second auction commenced on May 28, 2003, closed on June 13, 2003, and included 256 licenses: 5 EAG licenses and 476 Cellular Market Area licenses.[128] Seventeen winning bidders claimed small or very small business status and won 60 licenses, and nine ***14101** winning bidders claimed entrepreneur status and won 154 licenses.[129] On July 26, 2005, the Commission completed an auction of 5 licenses in the Lower 700 MHz band (Auction No. 60). There were three winning bidders for five licenses. All three winning bidders claimed small business status.

**142 41. In 2007, the Commission reexamined its rules governing the 700 MHz band in the *700 MHz Second Report and Order*.[130] An auction of 700 MHz licenses commenced January 24, 2008 and closed on March 18, 2008, which included, 176 Economic Area licenses in the A Block, 734 Cellular Market Area licenses in the B Block, and 176 EA licenses in the E Block.[131] Twenty winning bidders, claiming small business status (those with attributable average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years) won 49 licenses. Thirty three winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) won 325 licenses.

42. *Upper 700 MHz Band Licenses*. In the *700 MHz Second Report and Order*, the Commission revised its rules regarding Upper 700 MHz licenses.[132] On January 24, 2008, the Commission commenced Auction 73 in which several licenses in the Upper 700 MHz band were available for licensing: 12 Regional Economic Area Grouping licenses in the C Block, and one nationwide license in the D Block.[133] The auction concluded on March 18, 2008, with 3 winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) and winning five licenses.

43. *700 MHz Guard Band Licensees*. In 2000, in the 700 MHz Guard Band Order, the Commission adopted size standards for "small businesses" and "very small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments.[134] A small business in this service is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years.[135] Additionally, a very small business is an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years.[136] SBA approval of these definitions is not required.[137] An auction of 52 Major Economic Area licenses commenced on September *14102 6, 2000, and closed on September 21, 2000.[138] Of the 104 licenses auctioned, 96 licenses were sold to nine bidders. Five of these bidders were small businesses that won a total of 26 licenses. A second auction of 700 MHz Guard Band licenses commenced on February 13, 2001, and closed on February 21, 2001. All eight of the licenses auctioned were sold to three bidders. One of these bidders was a small business that won a total of two licenses.[139]

44. *Air-Ground Radiotelephone Service*. The Commission has previously used the SBA's small business size standard applicable to Wireless Telecommunications Carriers (except Satellite), i.e., an entity employing no more than 1,500 persons.[140] There are approximately 100 licensees in the Air-Ground Radiotelephone Service, and under that definition, we estimate that almost all of them qualify as small entities under the SBA definition. For purposes of assigning Air-Ground Radiotelephone Service licenses through competitive bidding, the Commission has defined "small business" as an entity that, together with controlling interests and affiliates, has average annual gross revenues for the preceding three years not exceeding $40 million.[141] A "very small business" is defined as an entity that, together with controlling interests and affiliates, has average annual gross revenues for the preceding three years not exceeding $15 million.[142] These definitions were approved by the SBA.[143] In May 2006, the Commission completed an auction of nationwide commercial Air-Ground Radiotelephone Service licenses in the 800 MHz band (Auction No. 65). On June 2, 2006, the auction closed with two winning bidders winning two Air-Ground Radiotelephone Services licenses. Neither of the winning bidders claimed small business status.

**143 45. *AWS Services (1710-1755 MHz and 2110-2155 MHz bands (AWS-1); 1915-1920 MHz, 1995-2000 MHz, 2020-2025 MHz and 2175-2180 MHz bands (AWS-2); 2155-2175 MHz band (AWS-3))*. For the AWS-1 bands,[144] the Commission has defined a "small business" as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a "very small business" as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. For AWS-2 and AWS-3, although we do not know for certain which entities are likely to apply for these frequencies, we note that the AWS-1 bands are comparable to those used for cellular service and personal communications service. The Commission has not yet adopted size standards for the AWS-2 or AWS-3 bands but proposes to treat both AWS-2 and AWS-3

similarly to broadband PCS service and AWS-1 service due to the comparable capital requirements and other factors, such as issues involved in relocating incumbents and developing markets, technologies, and services.[145]

***14103** 46. *3650-3700 MHz band*. In March 2005, the Commission released a *Report and Order and Memorandum Opinion and Order* that provides for nationwide, non-exclusive licensing of terrestrial operations, utilizing contention-based technologies, in the 3650 MHz band (i.e., 3650-3700 MHz). As of April 2010, more than 1270 licenses have been granted and more than 7433 sites have been registered. The Commission has not developed a definition of small entities applicable to 3650-3700 MHz band nationwide, non-exclusive licensees. However, we estimate that the majority of these licensees are Internet Access Service Providers (ISPs) and that most of those licensees are small businesses.

47. *Fixed Microwave Services*. Microwave services include common carrier,[146] private-operational fixed,[147] and broadcast auxiliary radio services.[148] They also include the Local Multipoint Distribution Service (LMDS),[149] the Digital Electronic Message Service (DEMS),[150] and the 24 GHz Service,[151] where licensees can choose between common carrier and non-common carrier status.[152] At present, there are approximately 36,708 common carrier fixed licensees and 59,291 private operational-fixed licensees and broadcast auxiliary radio licensees in the microwave services. There are approximately 135 LMDS licensees, three DEMS licensees, and three 24 GHz licensees. The Commission has not yet defined a small business with respect to microwave services. For purposes of the IRFA, we will use the SBA's definition applicable to Wireless Telecommunications Carriers (except satellite)—i.e., an entity with no more than 1,500 persons.[153] Under the present and prior categories, the SBA has deemed a wireless business to be small if it has 1,500 or fewer employees.[154] The Commission does not have data specifying the number of these licensees that have more than 1,500 employees, and thus is unable at this time to estimate with greater precision the number of fixed microwave service licensees that would qualify as small business concerns under the SBA's small business size standard. Consequently, the Commission estimates that there are up to 36,708 common carrier fixed licensees and up to 59,291 private operational-fixed licensees and broadcast auxiliary radio licensees in the microwave services that may be small and may be affected by the rules and policies adopted herein. We note, however, that the common carrier microwave fixed licensee category includes some large entities.

****144** 48. *Broadband Radio Service and Educational Broadband Service*. Broadband Radio Service systems, previously referred to as Multipoint Distribution Service (MDS) and Multichannel ***14104** Multipoint Distribution Service (MMDS) systems, and "wireless cable," transmit video programming to subscribers and provide two-way high speed data operations using the microwave frequencies of the Broadband Radio Service (BRS) and Educational Broadband Service (EBS) (previously referred to as the Instructional Television Fixed Service (ITFS)).[155] In connection with the 1996 BRS auction, the Commission established a small business size standard as an entity that had annual average gross revenues of no more than $40 million in the previous three calendar years.[156] The BRS auctions resulted in 67 successful bidders obtaining licensing opportunities for 493 Basic Trading Areas (BTAs). Of the 67 auction winners, 61 met the definition of a small business. BRS also includes licensees of stations authorized prior to the auction. At this time, we estimate that of the 61 small business BRS auction winners, 48 remain small business licensees. In addition to the 48 small businesses that hold BTA authorizations, there are approximately 392 incumbent BRS licensees that are considered small entities.[157] After adding the number of small business auction licensees to the number of incumbent licensees not already counted, we find that there are currently approximately 440 BRS licensees that are defined as small businesses under either the SBA or the Commission's rules.

49. In 2009, the Commission conducted Auction 86, the sale of 78 licenses in the BRS areas.[158] The Commission offered three levels of bidding credits: (i) a bidder with attributed average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years (small business) received a 15 percent discount on its winning bid; (ii) a bidder with attributed average annual gross revenues that exceed $3 million and do not exceed $15 million for the preceding three years (very small business) received a 25 percent discount on its winning bid; and (iii) a bidder with attributed average annual gross revenues that do not exceed $3 million for the preceding three years (entrepreneur) received a 35 percent discount on its winning

bid.[159] Auction 86 concluded in 2009 with the sale of 61 licenses.[160] Of the ten winning bidders, two bidders that claimed small business status won 4 licenses; one bidder that claimed very small business status won three licenses; and two bidders that claimed entrepreneur status won six licenses.

50. In addition, the SBA's Cable Television Distribution Services small business size standard is applicable to EBS. There are presently 2,436 EBS licensees. All but 100 of these licenses are held by educational institutions. Educational institutions are included in this analysis as small entities.[161] Thus, we estimate that at least 2,336 licensees are small businesses. Since 2007, Cable Television Distribution Services have been defined within the broad economic census category of Wired Telecommunications Carriers; that category is defined as follows: "This industry comprises ***14105** establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies."[162] The SBA has developed a small business size standard for this category, which is: all such firms having 1,500 or fewer employees. To gauge small business prevalence for these cable services we must, however, use the most current census data that are based on the previous category of Cable and Other Program Distribution and its associated size standard; that size standard was: all such firms having $13.5 million or less in annual receipts.[163] According to Census Bureau data for 2007, there were a total of 996 firms in this category that operated for the entire year.[164] Of this total, 948 firms had annual receipts of under $10 million, and 48 firms had receipts of $10 million or more but less than $25 million.[165] Thus, the majority of these firms can be considered small.

5. Satellite Service Providers

****145** 51. *Satellite Telecommunications Providers*. Two economic census categories address the satellite industry. The first category has a small business size standard of $30 million or less in average annual receipts, under SBA rules.[166] The second has a size standard of $30 million or less in annual receipts.[167]

52. The category of Satellite Telecommunications "comprises establishments primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[168] For this category, Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[169] Of this total, 299 firms had annual receipts of under $25 million.[170] Consequently, we estimate that the majority of Satellite Telecommunications firms are small entities that might be affected by our action.

53. The second category of Other Telecommunications comprises, *inter alia*, ""establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems."[171] For this category, census data for 2012 show that there ***14106** were 1,442 firms that operated for the entire year. Of these firms, a total of 1,400 had gross annual receipts of less than $25 million.[172] Thus, a majority of "All Other Telecommunications" firms potentially affected by the rules adopted can be considered small.

6. Cable Service Providers

54. *Cable and Other Program Distributors*. Since 2007, these services have been defined within the broad economic census category of Wired Telecommunications Carriers; that category is defined as follows: "This industry comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities

may be based on a single technology or a combination of technologies."[173] The SBA has developed a small business size standard for this category, which is: all such firms having 1,500 or fewer employees. To gauge small business prevalence for these cable services we must, however, use current census data that are based on the previous category of Cable and Other Program Distribution and its associated size standard; that size standard was: all such firms having $13.5 million or less in annual receipts.[174] According to Census Bureau data for 2007, there were a total of 2,048 firms in this category that operated for the entire year.[175] Of this total, 1,393 firms had annual receipts of under $10 million, and 655 firms had receipts of $10 million or more.[176] Thus, the majority of these firms can be considered small.

****146** 55. *Cable Companies and Systems*. The Commission has also developed its own small business size standards, for the purpose of cable rate regulation. Under the Commission's rules, a "small cable company" is one serving 400,000 or fewer subscribers, nationwide.[177] Industry data shows that there were 1,141 cable companies at the end of June 2012.[178] Of this total, all but ten cable operators nationwide are small under this size standard.[179] In addition, under the Commission's rules, a " small ***14107** system" is a cable system serving 15,000 or fewer subscribers.[180] Current Commission records show 4,945 cable systems nationwide.[181] Of this total, 4,380 cable systems have less than 20,000 subscribers, and 565 systems have 20,000 or more subscribers, based on the same records. Thus, under this standard, we estimate that most cable systems are small entities.

56. *Cable System Operators*. The Communications Act also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1 percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000."[182] There are approximately 52,403,705 cable video subscribers in the United States today.[183] Accordingly, an operator serving fewer than 524,037 subscribers shall be deemed a small operator if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate.[184] Based on available data, we find that all but nine incumbent cable operators are small entities under this size standard.[185] We note that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[186] Although it seems certain that some of these cable system operators are affiliated with entities whose gross annual revenues exceed $250 million, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

7. All Other Telecommunications

57. "All Other Telecommunications" is defined as follows: This U.S. industry is comprised of establishments that are primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[187] The SBA has developed a small business size standard for "All Other Telecommunications," which consists of all such firms with gross annual receipts of $32.5 million or less.[188] For this category, census data for 2012 show that there were 1,442 firms that operated for the entire year. Of these firms, a total of 1,400 had gross annual receipts of less than $25 million.[189] Thus, a majority of "All Other Telecommunications" firms potentially affected by the rules adopted can be considered small.

***14108 E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities**

****147** 58. The Order adopts requirements concerning (1) the provision of meaningful notice of privacy policies; (2) customer approval for the use and disclosure of customer PI; (3) reasonable data security; (4) data breach notification; and (5) particular

practices that raise privacy concerns. The rules we adopt in the Order will apply to all telecommunications carriers, including BIAS and voice service providers.

59. *Providing Meaningful Notice of Privacy Policies*. We adopt privacy policy notice requirements for all telecommunications carriers, including small providers. We require telecommunications carriers to provide notices of privacy policies at the point of sale prior to the purchase of service, and also to make notices clearly, conspicuously, and persistently available on carriers' websites and via carriers' apps that are used to manage service, if any. These notices must clearly inform customers about what customer proprietary information the providers collect, how they use it, and under what circumstances they share it. We also require that providers inform their customers about customers' rights to opt in to or out (as the case may be) of the use or sharing of their proprietary information. We require that privacy notices be clear, conspicuous, comprehensible, and not misleading; and written in the language with which the carrier transacts business with the customer; but we do not require that they be formatted in any specific manner. Finally, we require providers to give their customers advance notice of material changes to their privacy policies.[190] We have declined to require periodic notice on an annual or bi-annual basis, similar to what the preexisting CPNI rules require.

60. *Customer Approval Requirements for the Use and Disclosure of Customer PI*. We require carriers to obtain express, informed customer consent (i.e., opt-in approval) for the use and sharing of sensitive customer PI. With respect to non-sensitive customer PI, carriers must, at a minimum, provide their customers the ability to opt out of the carrier's use or sharing of that non-sensitive customer information. Carriers must also provide customers with easy access to a choice mechanism that is simple, easy-to-use, clearly and conspicuously disclosed, persistently available, and made available at no additional cost to the customer.[191] We require telecommunications carriers to solicit customer approval at the point of sale, and permit further solicitations after the point of sale. We also require that carriers actively contact their customers in these subsequent solicitations, to ensure that customers are adequately informed. Finally, we require the solicitations to be clear and conspicuous, comprehensible, not misleading, and to contain the information necessary for a customer to make an informed choice. This means the solicitations must inform customers of the types of customer proprietary information that the carrier is seeking to use, disclose, or permit access to, how those types of information will be used or shared, and the categories of entities with which that information is shared. In order to maintain flexibility, we do not require particular formats or methods by which a carrier must communicate its solicitation of consent to customers.[192]

****148** 61. Our rules allow providers to use and disclose customer data without approval if the data is properly de-identified. This option gives providers carriers, including small providers, a way to use customer information that avoids both the risks associated with identifiable information and any compliance costs associated with obtaining customer approval.[193]

62. *Reasonable Data Security*. We require telecommunications carriers to take reasonable measures to secure customer PI. We decline to mandate specific activities that providers must undertake in order to meet this reasonableness requirement. We do, however, offer guidance on the types of data ***14109** security practices we recommend carriers strongly consider as they seek to comply with our data security requirement, while recognizing that what constitutes "reasonable" data security is an evolving concept. When considering whether a carrier's data security practices are reasonable, we will weigh the nature and scope of the carrier's activities, the sensitivity of the underlying data, the size of the carrier, and technical feasibility. We recognize that the resources and data practices of small carriers are likely to be different from large carriers, and therefore what constitutes "reasonable" data security for a small carrier and a large carrier may differ. The totality of the circumstances, and not any individual factor, is determinative of whether a carrier's practices are reasonable. By requiring providers to take reasonable data security measures, we make clear that providers will not be held strictly liable for all data breaches.[194]

63. *Data Breach Notification Requirements*. We require BIAS providers and other telecommunications carriers to notify affected customers, the Commission—and, when a breach affects 5,000 or more customers, the FBI and Secret Service—of data breaches that meet a harm-based trigger. In particular, a carrier must report the breach unless it reasonably determines that no harm to customers is reasonably likely to occur. Customer breach notifications must include the date, estimated date, or estimated date

range of the breach; a description of the customer PI that was breached; contact information for the carrier; contact information for the FCC and any relevant state agencies; and information about credit-reporting agencies and steps customers can take to avoid identity theft.[195] We also require providers to keep records, for two years, of the dates of breaches and the dates when customers are notified.

64. When a reportable breach affects 5,000 or more customers, a provider must notify the Commission and the FBI and Secret Service within seven (7) business days of when the carrier reasonably determines that such a breach has occurred, and at least three (3) business days before notifying customers. The Commission will create a centralized portal for reporting breaches to the Commission and other federal law enforcement agencies.[196] Carriers must notify affected customers without unreasonable delay, and no later than 30 calendar days following the carriers' reasonable determination that a breach has occurred, unless the FBI or Secret Service requests a further delay. When a reportable breach does not meet the 5,000-customer threshold for reporting to the FBI and Secret Service, the Commission may be notified of the breach within the same no-more-than-30-days timeframe as affected customers.

****149** 65. *Particular Practices That Raise Privacy Concerns*. The Order prohibits BIAS providers from conditioning the provision of service on a customer's consenting to use or sharing of the customer's proprietary information over which our rules provide the consumer with a right of approval.[197] However, the Order does not prohibit BIAS providers from offering financial incentives to permit the use or disclosure of such information.[198] The Order requires BIAS providers offering such incentives to provide clear notice explaining the terms of any financial incentive program and to obtain opt-in consent. The notice must be clear and conspicuous and explained in a way that is comprehensible and not misleading. The explanation must include information about what customer PI the provider will collect, how it will be used, with what types of entities it will be shared, and for what purposes.[199] BIAS providers must make financial incentive notices easily accessible and separate from any other privacy notifications.[200] When a ***14110** BIAS provider markets a service plan that involves an exchange of personal information for reduced pricing or other benefits, it must also provide at least as prominent information to customers about an equivalent plan that does not include such an exchange. BIAS providers must also comply with all notice requirements of our rules when providing a financial incentive notice.[201]

F. Steps Take to Minimize the Significant Economic Impact on Small Entities and Significant Alternatives Considered

66. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): ""(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[202]

67. The Commission considered the economic impact on small providers, as identified in comments filed in response to the *NPRM* and IRFA, in reaching its final conclusions and taking action in this proceeding. Moreover, in formulating these rules, we have sought to provide flexibility for small providers whenever possible, including by avoiding prescription of the specific practices carriers must follow to achieve compliance.[203] Additionally, harmonizing our rules across all telecommunications services will reduce and streamline compliance costs for small carriers.[204] We have also adopted a phased-in implementation schedule, under which small providers are given an extra twelve months to come into compliance with the notice and approval requirements we adopt today. As discussed below, we have designed the rules we adopt today with the goal of minimizing burdens on all carriers, and particularly on small carriers.

****150** 68. *Providing Meaningful Notice of Privacy Policies*. Recognizing the importance of flexibility in finding successful ways to communicate privacy policies to consumers, we decline to adopt any specific form or format for privacy notices. We

adopt rules that require providers to disclose their privacy practices, but decline to be prescriptive about either the format or specific content of privacy policy notices in order to provide flexibility to providers and to minimize the burden of compliance levied by this requirement. In the interest of further minimizing the burden of transparency, particularly for small providers, we also direct the Consumer Advisory Committee to develop a model privacy policy notice that will serve as a safe harbor for our notice requirements.[205] We also decline to adopt specific notice requirements in mobile formats and we decline to require periodic notices of privacy practices.[206]

69. *Customer Approval Requirements for the Use and Disclosure of Customer PI*. In formulating customer approval requirements we have taken specific actions to reduce burdens on small carriers. First, as requested by small carriers and other commenters, we harmonize the voice and BIAS customer approval regimes into one set of rules.[207] Second, we do not require carriers to provide a ""privacy dashboard" for customer approvals; carriers may use any choice mechanism that is easy to use, persistently available, and clearly and conspicuously provided. This reduces the need for small carriers to ***14111** develop specific customer service architecture.[208] Third, we decline to require a specific format for accepting customer privacy choices and therefore allow carriers, particularly small carriers, that lack sophisticated websites or apps to accept customer choices through other means, such as by email or phone, so long as these means are persistently available. Fourth, we eliminate the periodic compliance documentation and reporting requirements that create recordkeeping burdens in our pre-existing CPNI rules.[209] To further reduce compliance burdens, we have clarified that choice solicitations may be combined a carrier's other privacy policy notices.

70. *Reasonable Data Security*. In the *NPRM* we proposed rules that included an overarching data security expectation and specified particular types of practices that carriers would need to implement to comply with that standard, while allowing carriers flexibility in implementing the proposed requirements. Based on the record in this proceeding, we have modified the overarching data security standard to more directly focus on reasonableness of the carriers' data security practices based on the particulars of the carrier's situation. Also based on the record, we decline to mandate specific activities that carriers must undertake in order to meet the reasonable data security requirement. We do, however, offer guidance on the types of data security practices we recommend carriers strongly consider as they seek to comply with our data security requirement—recognizing, of course, that what constitutes ""reasonable" data security is an evolving concept.[210] This guidance should be of particular benefit to smaller providers that may have less established data security programs. Also, our rule directs all providers—including small providers—to adopt contextually appropriate security practices. Contextual factors specified in the rule include the size of the provider and nature and scope of its activities. In including such factors, we take into account small providers' concerns that certain security measures that may be appropriate for larger carriers, such as having a dedicated official to oversee data security implementation, are likely beyond the needs and resources of the smallest carriers.

****151** 71. *Data Breach Notification Requirements*. In formulating our data breach rules, we specifically considered their impact on small carriers and crafted rules designed to balance the burdens on small carriers with the privacy and information security needs of those carriers' customers. First, our adoption of a harm-based trigger substantially reduces compliance burdens on small carriers by not requiring excessive notifications and by granting carriers the flexibility to focus their limited resources on preventing and ameliorating breaches, rather than issuing notifications for inconsequential events. The record shows that because small carriers tend to collect and use customer data far less extensively than larger carriers, they are less likely to have breaches that would trigger the notification requirements of our rules.[211] Second, our customer notification timeline also provides small carriers with greater flexibility; allowing up to 30 days to notify customers of a breach allows small carriers with fewer resources more time to investigate than the 10 days originally proposed. Third, we are creating a centralized portal for reporting data breaches to the Commission and law enforcement. This will streamline the notification process, which particularly reduces burdens on small carriers with fewer staff dedicated to breach mitigation.[212] Finally, for breaches affecting fewer than 5,000 customers, we extend the Commission notification deadline from seven (7) business days to thirty (30) calendar days. This provision will significantly reduce compliance burdens for small carriers, many of whom have fewer than 5,000 customers.[213]

72. *Implementation*. To provide certainty to customers and carriers alike, we establish a ***14112** timeline by which carriers must implement the privacy rules we adopt today. Carriers that have complied with FTC and industry best practices will be well-positioned to achieve prompt compliance with our privacy rules. We recognize, however, that carriers, especially small carriers, will need some time to update their internal business processes as well as their customer-facing privacy policies and choice mechanisms in order to come into compliance with some of our rules.[214]

73. The notice and choice rules we adopt today will become effective the later of (1) eight weeks after announcement PRA approval, or (12) twelve months after the Commission publishes a summary of the Order in the Federal Register. Carriers will need to analyze the new, harmonized privacy rules as well as coordinate with various business segments and vendors, and update programs and policies. Carriers will also need to engage in consumer outreach and education. These implementation steps will take time and we find, as supported in the record, that twelve months after publication of the Order in the Federal Register is an adequate minimum implementation period to implement the new notice and approval rules.[215] In order to minimize disruption to carriers' business practices, we do not require carriers to obtain new consent from all their customers. Rather, we treat as valid or "grandfather" any customer consent that was obtained prior to the effective date of our rules and thus is consistent with our new requirements. We decline to more broadly grandfather preexisting consents obtained by small carriers because we find that the parameters set forth in our rules create the appropriate balance to limit compliance costs while providing customers the privacy protections they need.[216]

****152** 74. The data breach rule we adopt today will become effective the later of (1) eight weeks after announcement PRA approval, or (2) six months after the Commission publishes a summary of the Order in the Federal Register. Although we recognize that carriers may have to modify practices and policies to implement our new rule, we find the harm trigger we adopt and timeline for notifying customers lessen the implementation requirements. Moreover, harmonization of our data breach rule for BIAS and voice services enable providers to streamline their notification processes, which should also lessen carriers' need for implementation time. Given these steps to minimize compliance burdens, we find six months is an adequate minimum timeframe.[217]

75. The data security requirements we adopt today will become effective 90 days after publication of a summary of the Order in the Federal Register. We find this to be an appropriate implementation period for the data security requirements because carriers should already be largely in compliance with these requirements because the reasonableness standard adopted in this Order provides carriers flexibility in how to approach data security and resembles the obligation to which they were previously subject pursuant to Section 5 of the FTC Act. We therefore do not think the numerous steps outlined by commenters that would have been necessary to comply with the data security proposals in the *NPRM* apply to the data security rules we adopt.[218]

76. The prohibition on conditioning offers to provider BIAS on a customer's agreement to waive privacy rights will become effective 30 days after publication of a summary of the Order in the Federal Register. We find that unlike other privacy rules, consumers should benefit from this prohibition promptly. We find no basis for any delay in the effective date of this important protection. All other privacy rules adopted in the Order will be effective 30 days after publication of a summary of the Order in ***14113** the Federal Register.[219] We also adopt a uniform implementation timetable for both BIAS and other telecommunications services.[220]

77. To provide additional flexibility to small carriers, we give small carriers an additional twelve months to implement the notice and customer approval rules we adopt today.[221] We find that an additional one-year phase-in will allow small providers time to make the necessary investments to implement these rules. The record reflects that small providers have comparatively limited resources and rely extensively on vendors over which they have limited leverage to compel adoption of new requirements. We recognize our notice and choice framework may entail upfront costs for small carriers. As such, we find that this limited extension is appropriate.[222]

78. We have considered, but opt against, providing small providers with even longer or broader extension periods, or with exemptions from the rules, as some commenters suggest.[223] In part, this is because the measures we have taken to reduce burdens for small providers have in many cases mitigated commenters' specific concerns. For instance, we find that we have addressed small provider concerns about the adoption of specific security requirements, such as annual risk assessments, by adopting a data security rule that does not prescribe any such requirements.[224] Moreover, as advocated by small providers, we adopt a customer choice framework that distinguishes between sensitive and non-sensitive customer information, as well as decline to mandate a customer-facing dashboard to help manage their implementation and compliance costs. Furthermore, we find that our data breach notification requirements and "take-it-or-leave-it" prohibition do not require implementation extension for small providers as compliance with these protections should not be costly for small carriers that generally collect less customer information and use customer information for narrower purposes.

153 79. **Report to Congress: The Commission will send a copy of the Order, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act.[225] In addition, the Commission will send a copy of the Order, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the Order and FRFA (or summaries thereof) will also be published in the Federal Register.[226]

*14114 STATEMENT OF CHAIRMAN TOM WHEELER

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.
Last week, I visited Consumer Reports' headquarters in Yonkers, New York, where I toured their product testing facility and met with senior leadership. When looking at a smart refrigerator that collects and shares data over the Internet, the discussion turned to privacy. Who would have ever imagined that what you have in your refrigerator would be information available to AT&T, Comcast, or whoever your network provider is?

The more our economy and our lives move online, the more information about us goes over our Internet Service Provider (ISP) — and the more consumers want to know how to protect their personal information in the digital age.

Today, the Commission takes a significant step to safeguard consumer privacy in this time of rapid technological change, as we adopt rules that will allow consumers to choose how their Internet Service Provider (ISP) uses and shares their personal data.

The bottom line is that it's your data. How it's used and shared should be your choice.

Over the past six months, we've engaged with consumer and public interest groups, fixed and mobile ISPs, advertisers, app and software developers, academics, other government actors including the FTC, and individual consumers, to figure out the best approach. Based on the extensive feedback we've received, we crafted today's rules to provide consumers increased choice, transparency and security online.

The time has also come to address the harmful impacts of mandatory arbitration requirements on consumers of communications services. To address this issue comprehensively, we have begun an internal process designed to produce a Notice of Proposed Rulemaking on this important topic by February 2017.

I want to thank the FTC and the Administration for leading the way with the FTC's privacy framework, and the Administration's Consumer Privacy Bill of Rights.

I'd like to acknowledge the companies who believe consumers care about privacy, and came to the table with constructive feedback.

To the consumer and public interest groups who have for years fought for consumer privacy protections in a digital age, thank you.

To our incredibly talented wireline bureau team lead by Matt DelNero and Lisa Hone, your hard work and dedication is inspiring.

And to the Chairman's Office team, led by Ruth Milkman and Stephanie Weiner. Thank you.

***14115 STATEMENT OF COMMISSIONER MIGNON L. CLYBURN APPROVING IN PART AND CONCURRING IN PART**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

****154** Why has this Commission, received more than a quarter of a million filings, of which the vast majority show support for the adoption of strong privacy rules? Because consumers care deeply about their privacy—and so should we.

Ninety-one percent of Americans believe, consumers have lost control of how their personal information is collected, and used by companies. That's ninety-one percent. With news seemingly breaking every week, about a cyberattack, massive data breaches, and companies collecting and selling customer data to government agencies, that number should come as no surprise to anyone.

So when faced with the question, of should I support requiring companies to give consumers more notice, more choice, and more transparency, you hear no double speak from me. Simply put, additional consent here means, that consumers will have more of a say, in how their personal information is used—and I for one, think that is a good thing.

Today, we substantially adopt the FTC's framework on privacy, with some tweaks to account for the current era, and unique position broadband providers occupy in our everyday lives. Where we deviate, we do so with the protection of consumers in mind. This *Order*, I am proud to say, adopts strong privacy protections, and provides robust choice for those who consent to the use, or sharing of their information, as a means of receiving new products, more targeted advertising, or other innovative offerings made possible by big data.

I am grateful to the Chairman and Commissioner Rosenworcel, who agreed to many of my edits. In particular, this item incorporates my suggestions to account for people with disabilities and strengthens protections for protected classes under our national civil rights laws. It also toughens our pay-for-privacy safeguards, and improves the abilities of businesses to contract for their own privacy protections.

But what it does not do, is address the issue of mandatory arbitration, an issue I outlined in my remarks at the #Solutions2020 Forum last week. Mandatory arbitration, put simply, forces consumers with grievances against a company, out of the court system, and into a private dispute resolution system. In other words, their options are limited.

In an op-ed appearing in TIME earlier this week, Senator Franken and I described in detail, why mandatory arbitration is a consumer un-friendly practice.

For those who take exception, I must remind them that in this privacy proceeding, we did provide notice, we developed a record, and had an opportunity to give relief to millions of consumers nationwide, including the 99.9% of mobile wireless customers, who are forced to give up their day in court when they sign up for connectivity. In a rulemaking about transparent notice and choice to consumers for their privacy, I believe it is a natural fit to ensure transparent notice and choice, in the context of dispute resolution.

Public justice systems, discipline private conduct. But private justice systems are “an oxymoron,” according to one appeals court judge, and he is not alone in that thought. The Consumer Financial Protection Bureau, has found that limiting forced arbitration clauses, have a powerful deterrent effect, resulting in companies changing business practices in more consumer-

friendly ways. An inscrutable, unfairly levied below-the-line fee on a bill, may be disputed by a thousand consumers, but a provider can collect that fee from a million customers who may never notice that line item as they pay their monthly bill.

****155** ***14116** Without the watchful eye of the court system, a company can limit its losses to those thousand who do take notice, while keeping the proceeds from the millions who did not. And as one arbitrator put it, "why would an arbitrator cater to a person they will never see again," over a corporation who is repeatedly footing the bill?

Several agencies have stepped up and declared these provisions unlawful in other contexts, and yes, I am disappointed that we did not join this vanguard, in ensuring that consumers are not unwittingly giving up their day in court, when they sign up for communications services. And because of this, I respectfully concur in part. Nevertheless, I am heartened, Mr. Chairman, that we are committed to addressing this issue, in a separate proceeding, with a firm timeline.

To the Wireline Competition Bureau and Office of General Counsel staff, who have wrestled through these difficult issues for years, and somewhat frenetically over the past few days, I thank you. You have further empowered the American consumer through this item, and for that, and more, I am grateful.

***14117 STATEMENT OF COMMISSIONER JESSICA ROSENWORCEL**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.
To understand the future of privacy, I think it is important to begin by focusing on the forces shaping our new digital world. I see three.

First, we live in an era of always-on connectivity. Connection is no longer just convenient. It fuels every aspect of modern civic and commercial life. Sitting outside this connectivity is consigning yourself to the wrong side of the digital divide—and that has a cost because it hampers any shot at 21st century success.

Second, it used to be that the communications relationship was primarily between a customer and his or her carrier. But the number of third parties participating in our digital age connections and transactions has multiplied exponentially. Dial a call, write an e-mail, make a purchase, update a profile, peruse a news site, store photographs in the cloud, and you should assume that service providers, advertising networks, and companies specializing in analytics have access to your personal information. Lots of it. For a long time. Our digital footprints are no longer in sand; they are in wet cement.

Third, the monetization of data is big business. The cost of data storage has declined dramatically. The market incentives to keep our data and slice and dice it to inform commercial activity are enormous—and they are going to grow.

Today these forces collide for all of us in our lives lived online, where what we download, post, say and do says so much about who we are to the world.

But the truth is we are just getting started. Because the future will feature a whole new world of the Internet of Things, where the connectivity we have today will look quaint. Every piece of machinery, pallet of equipment, thermostat, smoke detector, street light, garbage pail, parking meter—you name it—will be a connected device. This creates powerful opportunities that will make us more effective and more efficient, our cities smarter and our communities more connected. But these benefits come with big security challenges. We had an object lesson in these challenges last weekend, with one of the largest Distributed Denial of Service attacks in history, with botnets taking control of insecure connected devices, and compromising them by flooding servers and sites with overwhelming traffic.

****156** So when consumers survey this new digital landscape they wonder what privacy means. They do not want the digital age to decimate their fabled right to be left alone. They want privacy—but more importantly they want control. They want to control the whiplash from these new digital forces—and take some ownership of what is done with their personal information.

Today, the Commission provides consumers with the tools to do just that. We update—for the first time in nearly a decade—our privacy policies under Section 222 of the Communications Act. We establish new rules protecting the privacy of broadband customers. We adopt an opt-in regime for use and sharing of sensitive customer personal information and an opt-out regime for use and sharing of non-sensitive customer personal information. We put in place data security and breach notification policies so every consumer has confidence that efforts are in place to prevent harm from unlawful access to their data.

This is real privacy control for consumers. It helps in the here and now. But with respect to the future of privacy, I think we still have work to do.

Our domestic privacy policies largely rest on a foundation of old sector-specific laws. So continuing work to harmonize our privacy frameworks is hard— but deserves time and attention. To this end, the policies we adopt today are in many ways in sync with the approach taken by our colleagues at the Federal Trade Commission under Section 5 of the Federal Trade Commission Act. To the extent ***14118** they are not, let's face the facts—we are dealing with old laws, new technologies, and hard choices about existing regulatory schemes.

Privacy policy discussion, including ours here today, frequently focuses on three values—transparency, choice, and security. But I think it is time to introduce a fourth—simplicity. The forces at work in the digital world today are only going to make privacy more complex for all of us to control. But consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to understand if their information is protected. So it is incumbent on every policymaker with privacy authority to think about how to make our policies more simple and more consistent. In fact, I think it is time for a 21st century inter-agency privacy council, where this Commission and our colleagues across government can do a better job of aligning privacy policies across the board. That won't be easy. But for the future of privacy, future of consumer control, and future of the digital economy—it will be worth the effort.

***14119 DISSENTING STATEMENT OFCOMMISSIONER AJIT PAI**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.
For the last two decades, the United States has embraced a technology-neutral framework for online privacy. Administered by the Federal Trade Commission, this framework applied across all sectors of the online ecosystem. It reflected the uniform expectation of privacy that consumers have when they go online. It didn't matter whether an edge provider or ISP obtained your data. And it certainly didn't matter whether, as a consumer, you understood what those regulatory classifications meant —let alone the technical and legal intricacies that dictate when a single online company is operating in its capacity as an edge provider as opposed to an ISP. Regardless of all of that, the FTC's unified approach meant that you could rest assured knowing that a single and robust regulatory approach protected your online data.[227]

****157** That's why since the beginning of this proceeding, I have pushed for the Federal Communications Commission to parallel the FTC's framework as closely as possible. I agreed with my colleague that consumers have a "uniform expectation of privacy" and that the FCC thus "will not be regulating the edge providers differently" from ISPs.[228] I agreed that "consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected."[229] I agreed that "harmonizing FCC policies with other federal authorities with responsibilities for privacy is a responsible course of action."[230] And I agreed with the FTC when it said that an approach that imposes unique rules on ISPs that do not apply to all online actors that collect and use consumer data is "not optimal."[231] These are the core principles that I have held throughout this proceeding.

I was disappointed—but not surprised—when FCC leadership circulated an *Order* that departed so dramatically from those principles. Over the past three weeks, my office diligently pursued a compromise framework that would have minimized the

vast differences between the *Order*'s approach and the FTC's regime—one that would have protected consumer privacy while also allowing for more competition in the online advertising market, where edge providers are currently dominant.

For example, I asked my colleagues to acknowledge that persistent online identifiers (like static IP addresses) pose a larger privacy issue than more transitive identifiers. Distinguishing between the two in our de-identification standard would incentivize ISPs to compete with edge providers for online ads and do so through more privacy-protective technologies. Unfortunately, my colleagues were unwilling to compromise on this—or in any other meaningful respect.

***14120** That leaves us with rules that radically depart from the FTC framework. And that leaves us with rules that apply very different regulatory regimes based on the identity of the online actor. As my colleagues' earlier comments make clear, as the FTC has made plain, this makes no sense.

Now, today's *Order* tries to justify this new and complex approach by arguing that ISPs and edge providers see vastly different amounts of your online data. It recounts what it says is a vast sea of data that ISPs obtain. It then says that "By contrast, edge providers only see a slice of any given consumers Internet traffic."[232] A "slice." Really? The era of Big Data is here. The volume and extent of personal data that edge providers collect on a daily basis is staggering. But because the *Order* wants to treat ISPs differently from edge providers, it asserts that the latter only sees a "slice" of consumers' online data. This is not data-driven decision-making, but corporate favoritism.

****158** The reality—something today's *Order* does not acknowledge—is that edge providers do not just see a slice of your online data. Consider what the Electronic Privacy Information Center told us:
The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial threats for consumers are not the ISPs.[233]

Indeed, any review of the headlines rebuts the FCC's assertion that edge providers only see a fraction of your data. Consider these stories, almost all from just the past few weeks: "Google quietly updates privacy policy to drop ban on personally identifiable web tracking."[234] "Privacy Debate Flares With Report About Yahoo Scanning Emails."[235] "Apple keeps track of all the phone numbers you contact using iMessage."[236] "Twitter location data reveals users' homes, workplaces."[237] "Amnesty International rates Microsoft's Skype among worst in privacy."[238]

But due to the FCC's action today, those who have more insight into consumer behavior (edge providers) will be subject to more lenient regulation than those who have less insight (ISPs). This doesn't make sense. And when you get past the headlines, slogans, and self-congratulations, this is the reality that Americans should remember: Nothing in these rules will stop edge providers from harvesting and monetizing your data, whether it's the websites you visit or the YouTube videos you watch or the emails you send or the search terms you enter on any of your devices.

***14121** So if the FCC truly believes that these new rules are necessary to protect consumer privacy, then the government now must move forward to ensure uniform regulation of all companies in the Internet ecosystem at the new baseline the FCC has set.

That means the ball is now squarely in the FTC's court. The FTC could return us to a level playing field by changing its sensitivity-based approach to privacy to mirror the FCC's. No congressional action would be needed in order for the FTC to establish regulatory consistency and prevent consumer confusion.

Were it up to me, the FCC would have chosen a different path—one far less prescriptive and one consistent with two decades of privacy law and practice. The FCC should have restored the level playing field that once prevailed for all online actors using the FTC's framework. After all, as everyone acknowledges, consumers have a uniform expectation of privacy. They shouldn't have to be network engineers to understand who is collecting their data. And they shouldn't need law degrees to determine whether their information is protected.

****159** But the agency has rejected that approach. Instead, it has adopted one-sided rules that will cement edge providers' dominance in the online advertising market and lead to consumer confusion about which online companies can and cannot use their data. I dissent.

***14122 DISSENTING STATEMENT OF COMMISSIONER MICHAEL O'RIELLY**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.
Today, the Commission attempts to solve a problem of its own making and, in the process, creates a host of new ones. Having reclassified broadband Internet access service as a telecommunications service, the FCC usurped part of the FTC's role in overseeing broadband privacy. Not content to inherit a system that, by almost all accounts, was working quite well to protect consumers, the FCC quickly embarked on an expansionist mission, seeking to impose situationally-defective new requirements that are stricter than most consumers would ever want or expect and that exceed the Commission's authority. Finding itself out of its depth, the FCC was forced to rein in some of the most extreme proposals and align itself better with the FTC framework. Landing in a less bad spot, however, should not be confused with setting sound policy. I must dissent for a number of reasons.

Beginning with legal authority, the Commission's attempt to fit broadband into section 222 is fundamentally flawed. The plain language of the statute speaks in terms of telephone service.[239] Accordingly, in its effort to shoehorn broadband into this regime, the Commission is forced to ignore or explain away language that clearly contradicts its position, regulate by analogy, or simply create new obligations out of thin air.[240]

To start, there is no independent authority in section 222(a) to regulate privacy or data security, regardless of the technology. As I have said before, the purpose of section 222(a) was to set forth the general parameters of *who* would be covered by the new rules contained in the other subsections. Before the 1996 Act, the rules only applied to AT&T, the BOCs, and GTE. Section 222(a) changed that by extending the general duty to protect proprietary information to *all* telecommunications carriers, while sections 222(b) and (c) detail *when and how* that duty is to be exercised. Specifically, section 222(b) protects other carriers from anti-competitive practices by requiring the confidentiality of carrier proprietary information, while section 222(c) protects the privacy expectations of consumers with respect to their call records by requiring the confidentiality of "customer proprietary network information", or CPNI. Given this three-part structure, it is not surprising that section 222(a) employs a term — proprietary information — that encompasses both the carrier proprietary information used in 222(b) as well as the CPNI used in section 222(c). It does not give the Commission license to ignore its own history and read section 222(a) and its terminology out of context.

****160** Additionally, the use of "equipment manufacturers" in subsection (a) does not provide or authenticate any independent authority to act under the subsection, as the Commission tries to imagine in this item. Instead, it merely functions to cross reference overall concerns that some believed that equipment procurement by old-school Bell Operating Companies would lead to sharing of improper information from manufacturers. To the extent that concern existed, it was addressed directly in various places in section 273 with specific authority to act provided to the Commission in subsection (g) and, thus, it is inappropriate to read such authority into section 222(a).

***14123** Commenters supplied additional reasons that refute the FCC's interpretation. They point out that the FCC's expansive interpretation of section 222(a) cannot stand because it would nullify other provisions of section 222.[241] And they show that Congress carefully crafted Section 222 to regulate CPNI and deliberately chose not to use the broader category of

"personally identifiable information," or PII, unlike elsewhere in the Act.[242] These arguments further demonstrate that the order's interpretation of section 222(a) is not a permissible or reasonable one. Only a court intent on ignoring its obligations could not understand what the Commission is attempting to do here.

Since there is no independent authority in section 222(a), the categories of information that the FCC made up within section 222(a) — "customer proprietary information" and its subset "personally identifiable information" — are outside the scope of the provision. Yet even if the Commission attempted to ground its rules solely in section 222(c), which I do not concede applies to broadband either, it would still face significant legal problems. Many of the elements that the Commission wants to capture within its rules are not "customer proprietary network information".

First, proprietary information is "information that a person or entity owns to the exclusion of others," and thus it is not proprietary "if other individuals or entities can access the information and use it for their own commercial purposes."[243] That is why, in defining CPNI in section 222(h), Congress specified that it is limited to information that is made available to carriers "solely by virtue of the carrier-customer relationship."[244] Unlike traditional voice calls where the only parties that had access to call records were those already subject to section 222(c) — the local exchange carrier and in some instances the interexchange carrier — multiple parties that are unregulated by section 222 have access to an end user's online activities.[245] Indeed, "an ISP need not rely on its own relationship with its customers to collect information about their online activities because it could obtain the same information independently (at a price) from data brokers or other unregulated third parties."[246] Accordingly, this information would fall outside the scope of section 222(c).[247]

****161** The order responds that proprietary information can't mean information kept secret from everyone else, because other personal information would not be protected by the CPNI rules. And it resorts to platitudes that adhering to the law as it is drafted would "undermine the privacy protective purpose of the statute." But those arguments misunderstand the limited purpose of section 222. It was never intended to cover all information about a person. It defines and protects a specific set of call record information, and until just recently, that has been the Commission's interpretation as well.[248] Far from ***14124** creating a gap, as the order claims, Congress made an intentional allocation of responsibility. Section 222 directs the Commission to protect a discrete category of information and, to the extent Congress is concerned about other types of information, it has enacted other laws covering them, and it can enact additional laws going forward. The FCC is not empowered to supplement its own authority, even if it believes it has policy reasons to do so.[249]

At times, the order runs circles around itself. For instance, the order takes the position that "proprietary information" covers "information that should not be exposed widely to the public." But when confronted with the fact that IP addresses are necessarily disclosed on the open Internet to make the service work, the order responds that "whether information is available to third parties does not affect whether it meets the statutory definition of CPNI."[250]

Second, section 222(c)(1) is limited to "individually identifiable" CPNI. Therefore, the order's inclusion of information that is reasonably linked or linkable to a person *or device* is impermissibly broad.[251] If a device ""cannot be linked to a specific individual[,] ... information that may be linked to the device would fall outside the scope of the statute and should not be subject to these rules."[252]

As a backstop, the order also lists a number of other provisions that provide absolutely no authority for these rules.[253] As I've said before, those provisions were never intended to regulate privacy or data security. In addition, by specifically enacting section 222, Congress made clear that the authority to regulate privacy is found in that provision. Any other reading would render section 222 superfluous.

While the FCC has no authority to adopt broadband privacy rules, I am compelled to comment on the serious deficiencies in the rules themselves in the event that somehow a court erroneously, irresponsibly and lawlessly finds that there is authority for them. In particular, the order fails to adequately justify the rules, including why it takes a different approach from the FTC in several key respects, leaving ISPs with substantially greater burdens than other Internet companies. The order falls back on the tired refrain that broadband providers are "gatekeepers" and that, in that role, they are able to see more information about their customers than edge providers. This ridiculous notion has been thoroughly debunked in the record.[254] The fact that consumers use multiple platforms to access the ***14125** Internet, coupled with the increasing prevalence of encryption, significantly undermines the order's claims that broadband providers have unique or unparalleled access to customers and their information. The Commission's lame attempt at discounting the traffic subject to encryption does a disservice to common sense and ignores the plain fact that consumer traffic from the most popular Internet sites is already encrypted with more to come. Accordingly, to the extent that the rules rely on the faulty gatekeeper proposition, the Commission should be overturned for that reason alone.

****162** The FCC claims that, in moving to a sensitivity-based framework, the rules will be "more properly calibrated to customer and business expectations." But requiring opt-in notice for web browsing history and application usage data is a significant departure from the FTC approach, which is the basis for current expectations.[255] Under the FTC approach, those categories have not been treated as sensitive. While this approach has been in effect, there has been no evidence of any privacy harms, and businesses have been able to ""provide great value to consumers in the form of discounts, convenient features, and other new and innovative services."[256] Requiring opt-in consent for these categories will destroy that value and upend years of settled expectations, burdening rather than benefitting most users.[257]

It will also create confusion. Consumers will receive notices from the broadband providers asking them to opt in. If they do not opt in, but continue to see advertisements based on their web browsing and application usage, some will understandably assume that their broadband providers are violating their privacy policies when, in fact, the ads originate from third parties not subject to FCC rules.[258]

It is also unnecessary. As commenters pointed out, to the extent that web browsing history and application usage data concerns sensitive information, such as health or financial records, it is already covered by the other categories that the FTC, and now the FCC, consider to be sensitive.[259] Commenters also submitted documentation into the record showing how broadband providers and other Internet companies currently differentiate and avoid the use of sensitive web browsing and application usage information under the current FTC framework.[260] Therefore, there is no reason to adopt an added layer of sensitivity that sweeps too broadly.

***14126** The order responds that it is better to be overinclusive because what is non-sensitive to most people could be sensitive to some. But, again, given that there has been no evidence of harm while this approach has been in effect at the FTC, there is no reason to re-draw the line in a way that will burden most consumers. That is not to say that privacy conscious consumers should have no remedy at all. Rather, they should be presented with clear notice of how their providers differentiate sensitive information and have the ability to opt out if they do not think methods are sufficient to protect them.[261]

The Commission must realize that an overly broad opt-in regime has significant consequences for consumers because "[i]t is well understood that an opt-in consent mechanism results in far fewer individuals conveying their consent than is the case under an opt-out consent mechanism" even when substantial benefits are at stake.[262] As one commenter noted: "In the marketing context, a rough rule of thumb is that opt-out consent mechanisms may yield approximately 82% or much higher of individuals preserving their consent, whereas an opt-in consent model may yield only approximately 18% or much lower of individuals consenting."[263] While the Commission anticipates that, in an opt-in regime, many consumers will wish to affirmatively exercise choice options, the "statistics on opt-in consent rates cited above show that this is not the case, and that many individuals will simply not pay attention to the choice or skip past it to get to the service."[264] This isn't consumer choice, it's recognition of consumer apathy.

****163** Perhaps most troubling is that the order explicitly contemplates that it will apply to the Internet of Things. And, it makes this sweeping power grab without explaining how it has authority to do so. When I first cautioned that reclassifying broadband would lead to the FCC regulating edge providers and applications, some scoffed. Then it happened and now it is front and center again. Here, the FCC is refreshingly honest about its ambitions in this item, and I have every reason to expect that the Commission will make good on this vast new stake it has claimed. Those in the edge community should reconsider their belief that the FCC will never venture into their business models: The Commission is intentionally setting itself on a collision course with the FTC's definition with the intention to up the burdens on edge providers and all technology companies, either here or at the FTC.

The ultimate absurdity of these rules is that broadband providers remain free to purchase and use the information they need from those other Internet companies, including edge providers, because these other companies, not covered by the rules, will continue to operate under the FTC's opt-out regime. The rules prohibit a broadband provider from using sensitive "customer proprietary information" without opt-in consent, but "customer proprietary information" is limited to information that the provider "acquires in ***14127** connection with its provision of telecommunications service." Information obtained from an edge provider does not meet that definition.[265]

Therefore, all that the FCC has really done is raise the transaction costs. The FCC, in its typical nanny state fashion, seems to assume that consumers prefer an opt-in regime. But when consumers find out the end result is that they may have to pay more for heightened privacy rules that they never asked for, I doubt they will be grateful that the FCC intervened on their behalf. Indeed, this is a grandiose attempt to enact legacy talking points into rules so that Commission leadership can pat itself on the back while consumers receive no actual, practical protections. Added costs and burdens for providers? Yes. Benefits for consumers? No.

In another departure from the FTC framework and widespread consumer expectations, the order limits inferred consent to first party marketing within a service category, as well as the marketing of customer premises equipment (CPE) and "communications services commonly bundled together with the subscriber's telecommunications service." Here again, there is no rational reason to place undue restrictions on broadband providers.[266] While allowing providers to inform their customers about certain bundled offerings is a welcome change to the original, untenable draft, I would have extended inferred consent to the marketing of all products and services offered by broadband providers and affiliates as long as the affiliated relationship is clear to consumers.[267] Therefore, at a minimum, I would not require opt out consent to market new products and services that are "reasonably understood by customers as within the existing service relationship."[268] As the record demonstrated, consumers expect to receive information from their providers about new products, services, and discounts.[269] In addition, if broadband providers ***14128** "cannot market new products and services on the same terms as online companies — or even other brick and mortar businesses — there will be less incentive to invest and develop new services."[270]

****164** In addition, I was appalled to see a case-by-case approach imported to review mislabeled "pay for privacy" offers. These are consumer incentives offered every day in the real world and now ISPs will need to obtain a blessing from an agency that has no privacy experience.[271] The result is that broadband providers will be reluctant to extend, and may even forgo, valuable offers and discounts that consumers would want for fear that they will fall into another zero-rating style abyss. From that experience, we know that the game is perpetually on hold awaiting heavenly intervention, and some players have just stopped playing. Trying that again here in the privacy context does not make any sense, unless the real intention is to effectively ban pay for privacy offers without actually saying so in an attempt to avoid a legal challenge.

Moreover, I reject the Commission's effort to insert itself into mandatory arbitration clauses by committing to initiate a proceeding on the issue. As commenters explained in the record, mandatory arbitration clauses have benefitted both companies and consumers. In particular, "[m]ultiple studies have found that consumers obtain relief in arbitration at rates higher than they do in court, while being less costly and time-consuming for consumers than litigation."[272] I have heard the argument

that eliminating these clauses will enable consumers to band together in class action lawsuits, but that is unrealistic. The fact-specific nature of many of the disputes that end up in arbitration — such as an incorrect bill — do not lend themselves to class certification.[273]

Any foray into mandatory arbitration clauses is unlikely to withstand legal challenge, so committing to initiate a proceeding is a complete waste of Commission resources. Under the Federal Arbitration Act (FAA), any "written provision in any ... contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction ... shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."[274] Supreme Court precedent has made clear that Congressional intent to override the FAA can only be demonstrated through a "contrary congressional command" that is "discernible from the text, history, or purposes of the statute" and it must be explicit.[275] Accordingly, "given the stringency of this test, the Supreme Court has never held that any federal statute overrides the ***14129** FAA."[276] And nothing in section 222 or the Communications Act generally meets that high hurdle.[277] In short, the Commission would be asking for another muni broadband style reversal.

Shifting to data security and data breach, I recognize that the Commission has significantly moved away from the irrationally strict and unworkable proposals in the NPRM by adopting a reasonableness standard for data security and a harm-based approach for data breach notifications. However, the Commission still lacks authority to adopt all of these rules, and I remain concerned that the Commission is not giving providers sufficient time to come into compliance.[278] Even the larger providers requested at least 12 months,[279] but the Commission does not even afford the smallest providers that much time. The training and auditing alone could take more time than what is given. If it is so important to act on data security and data breach notifications, then the Commission should at least ensure that it is done right rather than right now.

****165** As a whole, this order places substantial, unjustified costs on businesses and consumers. Had the FCC conducted a cost-benefit analysis, which it committed to do but failed to live up to once again, it would have been unable to justify adopting these significant additional restrictions. Given that consumer privacy has been adequately protected under the current FTC framework and that there has been no evidence of any privacy harms, there is no benefit to be gained from increased regulation. On the other hand, there are substantial costs, including the increased transaction costs to purchase the information from unregulated Internet companies that will ultimately be passed on to consumers, the lost opportunity and revenues for broadband providers precluded from competing against Internet companies in the online advertising space, the foreclosure of innovative services that providers won't be able to offer and consumers won't receive, and the costs to consumers themselves who will be forced to participate in the opt-in regime and will pay more as a result.

While there are some statements about changes made to reduce compliance costs (i.e., one type of cost that is reviewed, in part, by the Office of Management and Budget), there is no overall analysis of the costs and benefits of this order. To the extent Commission leadership promised that rulemakings would serve as cost-benefit analyses, which I have explained is not adequate to comply with the relevant Executive Orders in any event, this order never engages in a serious discussion of the costs raised by commenters, failing to deliver even on that meager promise.

Finally, I want to point out that, despite my fundamental objections to this item based on the lack of statutory authority to adopt broadband privacy rules, I was willing to try to find common ground on specific issues, including the treatment of web browsing and app usage information, in order to mitigate the most harmful aspects of the order. My overtures were completely rebuffed by my colleagues. If anyone thinks that the only thing standing in the way of a more bipartisan Commission is an intransigent Commission minority, then this proceeding has proven, once again, that is absolutely incorrect.

STATEMENT OF CHAIRMAN TOM WHEELER

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.
Last week, I visited Consumer Reports' headquarters in Yonkers, New York, where I toured their product testing facility and met with senior leadership. When looking at a smart refrigerator that collects and shares data over the Internet, the discussion turned to privacy. Who would have ever imagined that what you have in your refrigerator would be information available to AT&T, Comcast, or whoever your network provider is?

The more our economy and our lives move online, the more information about us goes over our Internet Service Provider (ISP) — and the more consumers want to know how to protect their personal information in the digital age.

****166** Today, the Commission takes a significant step to safeguard consumer privacy in this time of rapid technological change, as we adopt rules that will allow consumers to choose how their Internet Service Provider (ISP) uses and shares their personal data.

The bottom line is that it's your data. How it's used and shared should be your choice.

Over the past six months, we've engaged with consumer and public interest groups, fixed and mobile ISPs, advertisers, app and software developers, academics, other government actors including the FTC, and individual consumers, to figure out the best approach. Based on the extensive feedback we've received, we crafted today's rules to provide consumers increased choice, transparency and security online.

The time has also come to address the harmful impacts of mandatory arbitration requirements on consumers of communications services. To address this issue comprehensively, we have begun an internal process designed to produce a Notice of Proposed Rulemaking on this important topic by February 2017.

I want to thank the FTC and the Administration for leading the way with the FTC's privacy framework, and the Administration's Consumer Privacy Bill of Rights.

I'd like to acknowledge the companies who believe consumers care about privacy, and came to the table with constructive feedback.

To the consumer and public interest groups who have for years fought for consumer privacy protections in a digital age, thank you.

To our incredibly talented wireline bureau team lead by Matt DelNero and Lisa Hone, your hard work and dedication is inspiring.

And to the Chairman's Office team, led by Ruth Milkman and Stephanie Weiner. Thank you.

STATEMENT OF COMMISSIONER MIGNON L. CLYBURN APPROVING IN PART AND CONCURRING IN PART

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.
Why has this Commission, received more than a quarter of a million filings, of which the vast majority show support for the adoption of strong privacy rules? Because consumers care deeply about their privacy—and so should we.

Ninety-one percent of Americans believe, consumers have lost control of how their personal information is collected, and used by companies. That's ninety-one percent. With news seemingly breaking every week, about a cyberattack, massive data breaches, and companies collecting and selling customer data to government agencies, that number should come as no surprise to anyone.

So when faced with the question, of should I support requiring companies to give consumers more notice, more choice, and more transparency, you hear no double speak from me. Simply put, additional consent here means, that consumers will have more of a say, in how their personal information is used—and I for one, think that is a good thing.

Today, we substantially adopt the FTC's framework on privacy, with some tweaks to account for the current era, and unique position broadband providers occupy in our everyday lives. Where we deviate, we do so with the protection of consumers in mind. This *Order*, I am proud to say, adopts strong privacy protections, and provides robust choice for those who consent to the use, or sharing of their information, as a means of receiving new products, more targeted advertising, or other innovative offerings made possible by big data.

****167** I am grateful to the Chairman and Commissioner Rosenworcel, who agreed to many of my edits. In particular, this item incorporates my suggestions to account for people with disabilities and strengthens protections for protected classes under our national civil rights laws. It also toughens our pay-for-privacy safeguards, and improves the abilities of businesses to contract for their own privacy protections.

But what it does not do, is address the issue of mandatory arbitration, an issue I outlined in my remarks at the #Solutions2020 Forum last week. Mandatory arbitration, put simply, forces consumers with grievances against a company, out of the court system, and into a private dispute resolution system. In other words, their options are limited.

In an op-ed appearing in TIME earlier this week, Senator Franken and I described in detail, why mandatory arbitration is a consumer un-friendly practice.

For those who take exception, I must remind them that in this privacy proceeding, we did provide notice, we developed a record, and had an opportunity to give relief to millions of consumers nationwide, including the 99.9% of mobile wireless customers, who are forced to give up their day in court when they sign up for connectivity. In a rulemaking about transparent notice and choice to consumers for their privacy, I believe it is a natural fit to ensure transparent notice and choice, in the context of dispute resolution.

Public justice systems, discipline private conduct. But private justice systems are “an oxymoron,” according to one appeals court judge, and he is not alone in that thought. The Consumer Financial Protection Bureau, has found that limiting forced arbitration clauses, have a powerful deterrent effect, resulting in companies changing business practices in more consumer-friendly ways. An inscrutable, unfairly levied below-the-line fee on a bill, may be disputed by a thousand consumers, but a provider can collect that fee from a million customers who may never notice that line item as they pay their monthly bill.

Without the watchful eye of the court system, a company can limit its losses to those thousand who do take notice, while keeping the proceeds from the millions who did not. And as one arbitrator put it, “why would an arbitrator cater to a person they will never see again,” over a corporation who is repeatedly footing the bill?

Several agencies have stepped up and declared these provisions unlawful in other contexts, and yes, I am disappointed that we did not join this vanguard, in ensuring that consumers are not unwittingly giving up their day in court, when they sign up for communications services. And because of this, I respectfully concur in part. Nevertheless, I am heartened, Mr. Chairman, that we are committed to addressing this issue, in a separate proceeding, with a firm timeline.

To the Wireline Competition Bureau and Office of General Counsel staff, who have wrestled through these difficult issues for years, and somewhat frenetically over the past few days, I thank you. You have further empowered the American consumer through this item, and for that, and more, I am grateful.

STATEMENT OF COMMISSIONER JESSICA ROSENWORCEL

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

****168** To understand the future of privacy, I think it is important to begin by focusing on the forces shaping our new digital world. I see three.

First, we live in an era of always-on connectivity. Connection is no longer just convenient. It fuels every aspect of modern civic and commercial life. Sitting outside this connectivity is consigning yourself to the wrong side of the digital divide—and that has a cost because it hampers any shot at 21st century success.

Second, it used to be that the communications relationship was primarily between a customer and his or her carrier. But the number of third parties participating in our digital age connections and transactions has multiplied exponentially. Dial a call, write an e-mail, make a purchase, update a profile, peruse a news site, store photographs in the cloud, and you should assume that service providers, advertising networks, and companies specializing in analytics have access to your personal information. Lots of it. For a long time. Our digital footprints are no longer in sand; they are in wet cement.

Third, the monetization of data is big business. The cost of data storage has declined dramatically. The market incentives to keep our data and slice and dice it to inform commercial activity are enormous—and they are going to grow.

Today these forces collide for all of us in our lives lived online, where what we download, post, say and do says so much about who we are to the world.

But the truth is we are just getting started. Because the future will feature a whole new world of the Internet of Things, where the connectivity we have today will look quaint. Every piece of machinery, pallet of equipment, thermostat, smoke detector, street light, garbage pail, parking meter—you name it—will be a connected device. This creates powerful opportunities that will make us more effective and more efficient, our cities smarter and our communities more connected. But these benefits come with big security challenges. We had an object lesson in these challenges last weekend, with one of the largest Distributed Denial of Service attacks in history, with botnets taking control of insecure connected devices, and compromising them by flooding servers and sites with overwhelming traffic.

So when consumers survey this new digital landscape they wonder what privacy means. They do not want the digital age to decimate their fabled right to be left alone. They want privacy—but more importantly they want control. They want to control the whiplash from these new digital forces—and take some ownership of what is done with their personal information.

Today, the Commission provides consumers with the tools to do just that. We update—for the first time in nearly a decade—our privacy policies under Section 222 of the Communications Act. We establish new rules protecting the privacy of broadband customers. We adopt an opt-in regime for use and sharing of sensitive customer personal information and an opt-out regime for use and sharing of non-sensitive customer personal information. We put in place data security and breach notification policies so every consumer has confidence that efforts are in place to prevent harm from unlawful access to their data.

****169** This is real privacy control for consumers. It helps in the here and now. But with respect to the future of privacy, I think we still have work to do.

Our domestic privacy policies largely rest on a foundation of old sector-specific laws. So continuing work to harmonize our privacy frameworks is hard— but deserves time and attention. To this end, the policies we adopt today are in many ways in sync

with the approach taken by our colleagues at the Federal Trade Commission under Section 5 of the Federal Trade Commission Act. To the extent they are not, let's face the facts—we are dealing with old laws, new technologies, and hard choices about existing regulatory schemes.

Privacy policy discussion, including ours here today, frequently focuses on three values—transparency, choice, and security. But I think it is time to introduce a fourth—simplicity. The forces at work in the digital world today are only going to make privacy more complex for all of us to control. But consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to understand if their information is protected. So it is incumbent on every policymaker with privacy authority to think about how to make our policies more simple and more consistent. In fact, I think it is time for a 21st century inter-agency privacy council, where this Commission and our colleagues across government can do a better job of aligning privacy policies across the board. That won't be easy. But for the future of privacy, future of consumer control, and future of the digital economy—it will be worth the effort.

DISSENTING STATEMENT OF COMMISSIONER AJIT PAI

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.
For the last two decades, the United States has embraced a technology-neutral framework for online privacy. Administered by the Federal Trade Commission, this framework applied across all sectors of the online ecosystem. It reflected the uniform expectation of privacy that consumers have when they go online. It didn't matter whether an edge provider or ISP obtained your data. And it certainly didn't matter whether, as a consumer, you understood what those regulatory classifications meant—let alone the technical and legal intricacies that dictate when a single online company is operating in its capacity as an edge provider as opposed to an ISP. Regardless of all of that, the FTC's unified approach meant that you could rest assured knowing that a single and robust regulatory approach protected your online data.[280]

That's why since the beginning of this proceeding, I have pushed for the Federal Communications Commission to parallel the FTC's framework as closely as possible. I agreed with my colleague that consumers have a "uniform expectation of privacy" and that the FCC thus "will not be regulating the edge providers differently" from ISPs.[281] I agreed that "consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected."[282] I agreed that "harmonizing FCC policies with other federal authorities with responsibilities for privacy is a responsible course of action."[283] And I agreed with the FTC when it said that an approach that imposes unique rules on ISPs that do not apply to all online actors that collect and use consumer data is "not optimal."[284] These are the core principles that I have held throughout this proceeding.

****170** I was disappointed—but not surprised—when FCC leadership circulated an *Order* that departed so dramatically from those principles. Over the past three weeks, my office diligently pursued a compromise framework that would have minimized the vast differences between the *Order*'s approach and the FTC's regime—one that would have protected consumer privacy while also allowing for more competition in the online advertising market, where edge providers are currently dominant.

For example, I asked my colleagues to acknowledge that persistent online identifiers (like static IP addresses) pose a larger privacy issue than more transitive identifiers. Distinguishing between the two in our de-identification standard would incentivize ISPs to compete with edge providers for online ads and do so through more privacy-protective technologies. Unfortunately, my colleagues were unwilling to compromise on this—or in any other meaningful respect.

That leaves us with rules that radically depart from the FTC framework. And that leaves us with rules that apply very different regulatory regimes based on the identity of the online actor. As my colleagues' earlier comments make clear, as the FTC has made plain, this makes no sense.

Now, today's *Order* tries to justify this new and complex approach by arguing that ISPs and edge providers see vastly different amounts of your online data. It recounts what it says is a vast sea of data that ISPs obtain. It then says that "By contrast, edge providers only see a slice of any given consumers Internet traffic."[285] A "slice." Really? The era of Big Data is here. The volume and extent of personal data that edge providers collect on a daily basis is staggering. But because the *Order* wants to treat ISPs differently from edge providers, it asserts that the latter only sees a "slice" of consumers' online data. This is not data-driven decision-making, but corporate favoritism.

The reality—something today's *Order* does not acknowledge—is that edge providers do not just see a slice of your online data. Consider what the Electronic Privacy Information Center told us:
The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial threats for consumers are not the ISPs.[286]

Indeed, any review of the headlines rebuts the FCC's assertion that edge providers only see a fraction of your data. Consider these stories, almost all from just the past few weeks: "Google quietly updates privacy policy to drop ban on personally identifiable web tracking."[287] "Privacy Debate Flares With Report About Yahoo Scanning Emails."[288] "Apple keeps track of all the phone numbers you contact using iMessage."[289] "Twitter location data reveals users' homes, workplaces."[290] "Amnesty International rates Microsoft's Skype among worst in privacy."[291]

****171** But due to the FCC's action today, those who have more insight into consumer behavior (edge providers) will be subject to more lenient regulation than those who have less insight (ISPs). This doesn't make sense. And when you get past the headlines, slogans, and self-congratulations, this is the reality that Americans should remember: Nothing in these rules will stop edge providers from harvesting and monetizing your data, whether it's the websites you visit or the YouTube videos you watch or the emails you send or the search terms you enter on any of your devices.

So if the FCC truly believes that these new rules are necessary to protect consumer privacy, then the government now must move forward to ensure uniform regulation of all companies in the Internet ecosystem at the new baseline the FCC has set.

That means the ball is now squarely in the FTC's court. The FTC could return us to a level playing field by changing its sensitivity-based approach to privacy to mirror the FCC's. No congressional action would be needed in order for the FTC to establish regulatory consistency and prevent consumer confusion.

Were it up to me, the FCC would have chosen a different path—one far less prescriptive and one consistent with two decades of privacy law and practice. The FCC should have restored the level playing field that once prevailed for all online actors using the FTC's framework. After all, as everyone acknowledges, consumers have a uniform expectation of privacy. They shouldn't have to be network engineers to understand who is collecting their data. And they shouldn't need law degrees to determine whether their information is protected.

But the agency has rejected that approach. Instead, it has adopted one-sided rules that will cement edge providers' dominance in the online advertising market and lead to consumer confusion about which online companies can and cannot use their data. I dissent.

DISSENTING STATEMENT OF COMMISSIONER MICHAEL O'RIELLY

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.
Today, the Commission attempts to solve a problem of its own making and, in the process, creates a host of new ones. Having reclassified broadband Internet access service as a telecommunications service, the FCC usurped part of the FTC's role in overseeing broadband privacy. Not content to inherit a system that, by almost all accounts, was working quite well to protect consumers, the FCC quickly embarked on an expansionist mission, seeking to impose situationally-defective new requirements that are stricter than most consumers would ever want or expect and that exceed the Commission's authority. Finding itself out of its depth, the FCC was forced to rein in some of the most extreme proposals and align itself better with the FTC framework. Landing in a less bad spot, however, should not be confused with setting sound policy. I must dissent for a number of reasons.

****172** Beginning with legal authority, the Commission's attempt to fit broadband into section 222 is fundamentally flawed. The plain language of the statute speaks in terms of telephone service.[292] Accordingly, in its effort to shoehorn broadband into this regime, the Commission is forced to ignore or explain away language that clearly contradicts its position, regulate by analogy, or simply create new obligations out of thin air.[293]

To start, there is no independent authority in section 222(a) to regulate privacy or data security, regardless of the technology. As I have said before, the purpose of section 222(a) was to set forth the general parameters of *who* would be covered by the new rules contained in the other subsections. Before the 1996 Act, the rules only applied to AT&T, the BOCs, and GTE. Section 222(a) changed that by extending the general duty to protect proprietary information to *all* telecommunications carriers, while sections 222(b) and (c) detail *when and how* that duty is to be exercised. Specifically, section 222(b) protects other carriers from anti-competitive practices by requiring the confidentiality of carrier proprietary information, while section 222(c) protects the privacy expectations of consumers with respect to their call records by requiring the confidentiality of "customer proprietary network information", or CPNI. Given this three-part structure, it is not surprising that section 222(a) employs a term — proprietary information — that encompasses both the carrier proprietary information used in 222(b) as well as the CPNI used in section 222(c). It does not give the Commission license to ignore its own history and read section 222(a) and its terminology out of context.

Additionally, the use of "equipment manufacturers" in subsection (a) does not provide or authenticate any independent authority to act under the subsection, as the Commission tries to imagine in this item. Instead, it merely functions to cross reference overall concerns that some believed that equipment procurement by old-school Bell Operating Companies would lead to sharing of improper information from manufacturers. To the extent that concern existed, it was addressed directly in various places in section 273 with specific authority to act provided to the Commission in subsection (g) and, thus, it is inappropriate to read such authority into section 222(a).

****173** Commenters supplied additional reasons that refute the FCC's interpretation. They point out that the FCC's expansive interpretation of section 222(a) cannot stand because it would nullify other provisions of section 222.[294] And they show that Congress carefully crafted Section 222 to regulate CPNI and deliberately chose not to use the broader category of "personally identifiable information," or PII, unlike elsewhere in the Act.[295] These arguments further demonstrate that the order's interpretation of section 222(a) is not a permissible or reasonable one. Only a court intent on ignoring its obligations could not understand what the Commission is attempting to do here.

Since there is no independent authority in section 222(a), the categories of information that the FCC made up within section 222(a) — "customer proprietary information" and its subset "personally identifiable information" — are outside the scope of the provision. Yet even if the Commission attempted to ground its rules solely in section 222(c), which I do not concede applies to broadband either, it would still face significant legal problems. Many of the elements that the Commission wants to capture within its rules are not "customer proprietary network information".

First, proprietary information is "information that a person or entity owns to the exclusion of others," and thus it is not proprietary "if other individuals or entities can access the information and use it for their own commercial purposes."[296] That is why, in defining CPNI in section 222(h), Congress specified that it is limited to information that is made available to carriers "solely by virtue of the carrier-customer relationship."[297] Unlike traditional voice calls where the only parties that had access to call records were those already subject to section 222(c) — the local exchange carrier and in some instances the interexchange carrier — multiple parties that are unregulated by section 222 have access to an end user's online activities.[298] Indeed, "an ISP need not rely on its own relationship with its customers to collect information about their online activities because it could obtain the same information independently (at a price) from data brokers or other unregulated third parties."[299] Accordingly, this information would fall outside the scope of section 222(c).[300]

**174 The order responds that proprietary information can't mean information kept secret from everyone else, because other personal information would not be protected by the CPNI rules. And it resorts to platitudes that adhering to the law as it is drafted would "undermine the privacy protective purpose of the statute." But those arguments misunderstand the limited purpose of section 222. It was never intended to cover all information about a person. It defines and protects a specific set of call record information, and until just recently, that has been the Commission's interpretation as well.[301] Far from creating a gap, as the order claims, Congress made an intentional allocation of responsibility. Section 222 directs the Commission to protect a discrete category of information and, to the extent Congress is concerned about other types of information, it has enacted other laws covering them, and it can enact additional laws going forward. The FCC is not empowered to supplement its own authority, even if it believes it has policy reasons to do so.[302]

At times, the order runs circles around itself. For instance, the order takes the position that "proprietary information" covers "information that should not be exposed widely to the public." But when confronted with the fact that IP addresses are necessarily disclosed on the open Internet to make the service work, the order responds that "whether information is available to third parties does not affect whether it meets the statutory definition of CPNI."[303]

Second, section 222(c)(1) is limited to "individually identifiable" CPNI. Therefore, the order's inclusion of information that is reasonably linked or linkable to a person *or device* is impermissibly broad.[304] If a device ""cannot be linked to a specific individual[,] ... information that may be linked to the device would fall outside the scope of the statute and should not be subject to these rules."[305]

As a backstop, the order also lists a number of other provisions that provide absolutely no authority for these rules.[306] As I've said before, those provisions were never intended to regulate privacy or data security. In addition, by specifically enacting section 222, Congress made clear that the authority to regulate privacy is found in that provision. Any other reading would render section 222 superfluous.

While the FCC has no authority to adopt broadband privacy rules, I am compelled to comment on the serious deficiencies in the rules themselves in the event that somehow a court erroneously, irresponsibly and lawlessly finds that there is authority for them. In particular, the order fails to adequately justify the rules, including why it takes a different approach from the FTC in several key respects, leaving ISPs with substantially greater burdens than other Internet companies. The order falls back on the tired refrain that broadband providers are "gatekeepers" and that, in that role, they are able to see more information about their customers than edge providers. This ridiculous notion has been thoroughly debunked in the record.[307] The fact that consumers use multiple platforms to access the Internet, coupled with the increasing prevalence of encryption, significantly undermines the order's claims that broadband providers have unique or unparalleled access to customers and their information. The Commission's lame attempt at discounting the traffic subject to encryption does a disservice to common sense and ignores the plain fact that consumer traffic from the most popular Internet sites is already encrypted with more to come. Accordingly, to the extent that the rules rely on the faulty gatekeeper proposition, the Commission should be overturned for that reason alone.

**175 The FCC claims that, in moving to a sensitivity-based framework, the rules will be "more properly calibrated to customer and business expectations." But requiring opt-in notice for web browsing history and application usage data is a significant departure from the FTC approach, which is the basis for current expectations.[308] Under the FTC approach, those categories have not been treated as sensitive. While this approach has been in effect, there has been no evidence of any privacy harms, and businesses have been able to ""provide great value to consumers in the form of discounts, convenient features, and other new and innovative services."[309] Requiring opt-in consent for these categories will destroy that value and upend years of settled expectations, burdening rather than benefitting most users.[310]

It will also create confusion. Consumers will receive notices from the broadband providers asking them to opt in. If they do not opt in, but continue to see advertisements based on their web browsing and application usage, some will understandably assume that their broadband providers are violating their privacy policies when, in fact, the ads originate from third parties not subject to FCC rules.[311]

It is also unnecessary. As commenters pointed out, to the extent that web browsing history and application usage data concerns sensitive information, such as health or financial records, it is already covered by the other categories that the FTC, and now the FCC, consider to be sensitive.[312] Commenters also submitted documentation into the record showing how broadband providers and other Internet companies currently differentiate and avoid the use of sensitive web browsing and application usage information under the current FTC framework.[313] Therefore, there is no reason to adopt an added layer of sensitivity that sweeps too broadly.

The order responds that it is better to be overinclusive because what is non-sensitive to most people could be sensitive to some. But, again, given that there has been no evidence of harm while this approach has been in effect at the FTC, there is no reason to re-draw the line in a way that will burden most consumers. That is not to say that privacy conscious consumers should have no remedy at all. Rather, they should be presented with clear notice of how their providers differentiate sensitive information and have the ability to opt out if they do not think methods are sufficient to protect them.[314]

The Commission must realize that an overly broad opt-in regime has significant consequences for consumers because "[i]t is well understood that an opt-in consent mechanism results in far fewer individuals conveying their consent than is the case under an opt-out consent mechanism" even when substantial benefits are at stake.[315] As one commenter noted: "In the marketing context, a rough rule of thumb is that opt-out consent mechanisms may yield approximately 82% or much higher of individuals preserving their consent, whereas an opt-in consent model may yield only approximately 18% or much lower of individuals consenting."[316] While the Commission anticipates that, in an opt-in regime, many consumers will wish to affirmatively exercise choice options, the "statistics on opt-in consent rates cited above show that this is not the case, and that many individuals will simply not pay attention to the choice or skip past it to get to the service."[317] This isn't consumer choice, it's recognition of consumer apathy.

**176 Perhaps most troubling is that the order explicitly contemplates that it will apply to the Internet of Things. And, it makes this sweeping power grab without explaining how it has authority to do so. When I first cautioned that reclassifying broadband would lead to the FCC regulating edge providers and applications, some scoffed. Then it happened and now it is front and center again. Here, the FCC is refreshingly honest about its ambitions in this item, and I have every reason to expect that the Commission will make good on this vast new stake it has claimed. Those in the edge community should reconsider their belief that the FCC will never venture into their business models: The Commission is intentionally setting itself on a collision course with the FTC's definition with the intention to up the burdens on edge providers and all technology companies, either here or at the FTC.

The ultimate absurdity of these rules is that broadband providers remain free to purchase and use the information they need from those other Internet companies, including edge providers, because these other companies, not covered by the rules, will continue to operate under the FTC's opt-out regime. The rules prohibit a broadband provider from using sensitive "customer proprietary information" without opt-in consent, but "customer proprietary information" is limited to information that the provider "acquires in connection with its provision of telecommunications service." Information obtained from an edge provider does not meet that definition.[318]

Therefore, all that the FCC has really done is raise the transaction costs. The FCC, in its typical nanny state fashion, seems to assume that consumers prefer an opt-in regime. But when consumers find out the end result is that they may have to pay more for heightened privacy rules that they never asked for, I doubt they will be grateful that the FCC intervened on their behalf. Indeed, this is a grandiose attempt to enact legacy talking points into rules so that Commission leadership can pat itself on the back while consumers receive no actual, practical protections. Added costs and burdens for providers? Yes. Benefits for consumers? No.

In another departure from the FTC framework and widespread consumer expectations, the order limits inferred consent to first party marketing within a service category, as well as the marketing of customer premises equipment (CPE) and "communications services commonly bundled together with the subscriber's telecommunications service." Here again, there is no rational reason to place undue restrictions on broadband providers.[319] While allowing providers to inform their customers about certain bundled offerings is a welcome change to the original, untenable draft, I would have extended inferred consent to the marketing of all products and services offered by broadband providers and affiliates as long as the affiliated relationship is clear to consumers.[320] Therefore, at a minimum, I would not require opt out consent to market new products and services that are "reasonably understood by customers as within the existing service relationship."[321] As the record demonstrated, consumers expect to receive information from their providers about new products, services, and discounts.[322] In addition, if broadband providers "cannot market new products and services on the same terms as online companies — or even other brick and mortar businesses — there will be less incentive to invest and develop new services."[323]

**177 In addition, I was appalled to see a case-by-case approach imported to review mislabeled "pay for privacy" offers. These are consumer incentives offered every day in the real world and now ISPs will need to obtain a blessing from an agency that has no privacy experience.[324] The result is that broadband providers will be reluctant to extend, and may even forgo, valuable offers and discounts that consumers would want for fear that they will fall into another zero-rating style abyss. From that experience, we know that the game is perpetually on hold awaiting heavenly intervention, and some players have just stopped playing. Trying that again here in the privacy context does not make any sense, unless the real intention is to effectively ban pay for privacy offers without actually saying so in an attempt to avoid a legal challenge.

Moreover, I reject the Commission's effort to insert itself into mandatory arbitration clauses by committing to initiate a proceeding on the issue. As commenters explained in the record, mandatory arbitration clauses have benefitted both companies and consumers. In particular, "[m]ultiple studies have found that consumers obtain relief in arbitration at rates higher than they do in court, while being less costly and time-consuming for consumers than litigation."[325] I have heard the argument that eliminating these clauses will enable consumers to band together in class action lawsuits, but that is unrealistic. The fact-specific nature of many of the disputes that end up in arbitration — such as an incorrect bill — do not lend themselves to class certification.[326]

Any foray into mandatory arbitration clauses is unlikely to withstand legal challenge, so committing to initiate a proceeding is a complete waste of Commission resources. Under the Federal Arbitration Act (FAA), any "written provision in any ... contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction ... shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."[327] Supreme Court precedent has made clear that Congressional intent to override the FAA can only be demonstrated through a "contrary congressional command" that is "discernible from the text, history, or purposes of the statute"

and it must be explicit.[328] Accordingly, "given the stringency of this test, the Supreme Court has never held that any federal statute overrides the FAA."[329] And nothing in section 222 or the Communications Act generally meets that high hurdle.[330] In short, the Commission would be asking for another muni broadband style reversal.

Shifting to data security and data breach, I recognize that the Commission has significantly moved away from the irrationally strict and unworkable proposals in the NPRM by adopting a reasonableness standard for data security and a harm-based approach for data breach notifications. However, the Commission still lacks authority to adopt all of these rules, and I remain concerned that the Commission is not giving providers sufficient time to come into compliance.[331] Even the larger providers requested at least 12 months,[332] but the Commission does not even afford the smallest providers that much time. The training and auditing alone could take more time than what is given. If it is so important to act on data security and data breach notifications, then the Commission should at least ensure that it is done right rather than right now.

****178** As a whole, this order places substantial, unjustified costs on businesses and consumers. Had the FCC conducted a cost-benefit analysis, which it committed to do but failed to live up to once again, it would have been unable to justify adopting these significant additional restrictions. Given that consumer privacy has been adequately protected under the current FTC framework and that there has been no evidence of any privacy harms, there is no benefit to be gained from increased regulation. On the other hand, there are substantial costs, including the increased transaction costs to purchase the information from unregulated Internet companies that will ultimately be passed on to consumers, the lost opportunity and revenues for broadband providers precluded from competing against Internet companies in the online advertising space, the foreclosure of innovative services that providers won't be able to offer and consumers won't receive, and the costs to consumers themselves who will be forced to participate in the opt-in regime and will pay more as a result.

While there are some statements about changes made to reduce compliance costs (i.e., one type of cost that is reviewed, in part, by the Office of Management and Budget), there is no overall analysis of the costs and benefits of this order. To the extent Commission leadership promised that rulemakings would serve as cost-benefit analyses, which I have explained is not adequate to comply with the relevant Executive Orders in any event, this order never engages in a serious discussion of the costs raised by commenters, failing to deliver even on that meager promise.

Finally, I want to point out that, despite my fundamental objections to this item based on the lack of statutory authority to adopt broadband privacy rules, I was willing to try to find common ground on specific issues, including the treatment of web browsing and app usage information, in order to mitigate the most harmful aspects of the order. My overtures were completely rebuffed by my colleagues. If anyone thinks that the only thing standing in the way of a more bipartisan Commission is an intransigent Commission minority, then this proceeding has proven, once again, that is absolutely incorrect.

Footnotes

1 *See*47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to ... customers.").

2 Consistent with the statutory definition of CPNI, we define CPNI with respect to BIAS providers as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." *See infra* Part III.B.3.a(i).

3 *See* Executive Office of the President, Administration Discussion Draft: Consumer Privacy Bill of Rights Act (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf ("2015 Administration CPBR Discussion Draft" or "CPBR").

4 Section 222 addresses the conditions under which carriers may "use, disclose, or permit access to" customer information. 47 U.S.C. § 222(c)(1), (c)(3), (d), (f). For simplicity throughout this document we sometimes use the terms "disclose" or "share" in place of "disclose or permit access to."

5 *See generally* Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (2012 FTC Privacy Report).

6 47 U.S.C. § 605.

7 *See, e.g.*, Bernard Strassburg, Address to the Ass'n for Comp. Machinery, *The Marriage of Computers and Communications: Some Regulatory Implications* (Oct. 20, 1966), *in* 9 Jurimetrics J. 12-18 (1966), *available at* http://heinonline.org/HOL/Page?handle=hein.journals/juraba9&div=9&g_sent=1&collection=journals.

8 *See Amendment of Section 64.702 of the Commission's Rules and Regulations*, Final Order, 77 FCC 2d 384 (1980) (*Computer II*), *recon.*, 84 FCC 2d 50 (1980), *further recon.*, 88 FCC 2d 512 (1981), *aff'd sub nom. Computer and Commc'n Indus. Ass'n v. FCC*, 693 F.2d 198 (D.C. Cir. 1982), *cert. denied*, 461 U.S. 938 (1983); *Amendment of Section 64.702 of the Commission's Rules and Regulations*, Phase I, 104 FCC 2d 958 (1986); *Application of Open Network Architecture and Nondiscrimination Safeguards to GTE Corp.*, Report and Order, 9 FCC Rcd 4922, 4944-45, para. 45 (1994); *Application of Open Network Architecture and Nondiscrimination Safeguards to GTE Corp.*, Memorandum Opinion and Order, 11 FCC Rcd 1388, 1419-25, paras. 73-86 (1995); *Furnishing of Customer Premises Equipment by Bell Operating Telephone Companies and the Independent Telephone Companies*, Report and Order, 2 FCC Rcd 143 (1987), *recon. on other grounds*, 3 FCC Rcd 22 (1987); *aff'd*, *Ill. Bell Tel. Co. v. FCC*, 883 F.2d 104 (D.C. Cir. 1989).

9 *See*47 U.S.C. § 153(50).

10 *See* Joint Explanatory Statement of the Committee of Conference, 104th Cong., 2d Sess. 204; *see also* H.R. Rep. No. 204, 104th Cong., 1st Sess. 91 (1995).

11 47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers ....").

12 47 U.S.C. § 222(c)(1). Section 222(d) enumerates exceptions to this prohibition. 47 U.S.C. § 222(d).

13 *See, e.g.*, Electronic Transaction Association (ETA) Comments at 2; AT&T Comments at 1; Multicultural Media, Telecom and Internet Council et al. (MMTC et al.) Comments at 2; Interactive Advertising Bureau (IAB) Comments at 5 ("IAB believes that industry self-regulation is the preferred approach to address online privacy.").

14 *See generally Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*).

15 15 U.S.C. § 45(a)(1).

16 *See* FTC Staff Comments at 4-6.

17 *See*15 U.S.C. §§ 45(a)(2) (exempting "common carriers subject to the Acts to regulate commerce"), 44 (defining "Acts to regulate commerce" as including "the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto"); 47 U.S.C. § 153(51) (providing that "[a] telecommunications carrier shall be treated as a common carrier under [the Communications Act] only to the extent that it is engaged in providing telecommunications services").*See also* FTC Staff Comments at 2, n.5.

18 *See* 2015 Administration CPBR Discussion Draft, § 4(a)(1).

19 *Id.*

20 *See Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5736-42, paras. 314-27 (2015), *aff'd United States Telecom Ass'n v. F.C.C.*, 825 F.3d 674 (D.C. Cir. 2016) (*2015 Open Internet Order*) (discussing the historical classification of broadband Internet access service).

21 *See*15 U.S.C. § 45(a)(1) (prohibiting unfair or deceptive acts or practices in or affecting commerce).

22 *2015 Open Internet Order*, 30 FCC Rcd at 5733, para. 306; *see also United States Telecom Ass'n v. F.C.C.*, 825 F.3d at 712.

23 *2015 Open Internet Order*, 30 FCC Rcd at 5821-22, paras. 463-64 (concluding that "forbearance from the application of section 222 with respect to broadband Internet access service is not in the public interest ... and that section 222 remains necessary for the protection of consumers ...."); *see also Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy*, Enforcement Advisory No. 2015-03, 30 FCC Rcd 4849 (Enf, Bur. 2015) (*Enf. Bur. Privacy Advisory*) (providing guidance "to broadband providers about how the Enforcement Bureau intends to enforce Section 222 in connection with BIAS during the time between the effective date of the *Open Internet Order* and any subsequent Commission action providing further guidance and/or adoption of regulations applying Section 222 more specifically to BIAS").

24 *2015 Open Internet Order*, 30 FCC Rcd at 5823, para. 467.

25 *See generally Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) (*Broadband Privacy NPRM*).

26 *Id.* at 2510, para. 24.

27 *See, e.g.*, NTCA—The Rural Broadband Association (NTCA) Comments at 11; *see also* CTIA—The Wireless Association (CTIA) Comments at 106; Letter from Mike Montgomery, Executive Director, CALinnovates, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-016, at 1-2 (filed Oct. 19, 2016).

28 *See* Letter from Paul Ohm, Professor, Georgetown University Law Center, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106 Attach., Testimony Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives at 3 (filed June 19, 2016) (Paul Ohm Testimony).

29 *See 2015 Open Internet Order*, 30 FCC Rcd at 5629, para. 80 (noting that "once a consumer chooses a broadband provider, that provider has a monopoly on access to the subscriber").

30 Letter from Kathleen McGee, Bureau Chief, Bureau of Internet and Technology, New York State Attorney General, to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106 at 2 (filed June 30, 2016) (NY Attorney General June 30, 2016 *Ex Parte*) (also claiming that BIAS providers can collect "not only a consumer's name, address and financial information but also every website he or she visited, the links clicked on those websites, geo-location information, and the content of electronic communications"); *see also, e.g.*, Ghostery Apr. 29, 2016 *Ex Parte* Attach. at 3-5; Consumer Action Comments at 1; Consumer Watchdog Comments at 4 ("The ISP is in a unique position to amass deeply revealing personal profiles, share the data with third parties or use it for its own purposes."); Public Knowledge et al. Comments, Attach. Public Knowledge White Paper, Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World at 51-52, 55-56 (Public Knowledge White Paper); American Association for Justice (AAJ) Comments at 8 (explaining that "BIAS providers are now privy to an extensive amount of personal information about their customers"); Electronic Frontier Foundation (EFF) Comments at 1.

31 *See, e.g.*, Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech, et al., Working Paper, Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others at 24-25 (filed May 27, 2016) (Peter Swire Working Paper); *see also* AT&T Comments at 4; CTIA Comments at 7-8.

32 National Consumers League (NCL) Reply at 11.

33 *See, e.g.*, Upturn Comments at 6.

34 *See, e.g.*, Peter Swire Working Paper at 4 (stating that "non-ISPs are increasingly gathering commercially valuable information about online user activity from multiple context"); National Black Caucus of State Legislators (NBCSL) Comments at 1 ("Webmail, Internet videos, social media, and other firms, and even devices like open-source smartphones, all track and use enormous volumes of sensitive

data"); Advanced Communications Law & Policy (ACLP) Comments at 13; Howard Beales Comments at 5 ("Each provider has particular insights into the consumer's online activities, but there is no entity in a 'unique' position to assemble a 'comprehensive' picture of online behavior."); Consumer Workers of America (CWA) Comments at 2-3; International Center for Law & Economics (ICLE) Comments at 9; AT&T Comments at 3 (arguing that "ISPs have *less*, not more, comprehensive visibility than many edge providers into their users' online activities"); Verizon Comments at 18 (asserting that "repeated and prolonged interactions provide social networking sites with access to vast amounts of commercially valuable information about their users, including user-generated content and metadata, which they use to facilitate targeted advertising"); CenturyLink Comments at 6 (arguing that to ""the extent that user information (for example, web browsing activity and location information) is visible to the user's broadband provider, it also is visible to, and collected by, various third-party entities").

35 *See, e.g.*, Paul Ohm Testimony at 3; EFF Comments at 1 ("No edge provider enjoys the ability to see everything a consumer does online. The technology now available for telecommunications providers allows for the possibility that every communications, activity, and movement can be tracked in real or near-real time.").

36 *See* Dillon Reisman and Arvind Narayanan, Princeton Center for Information Technology Policy, WC Docket No. 16-106, *Ex Parte* Presentation at 32 (filed June 17, 2016) (Reisman and Narayanan June 17, 2016 *Ex Parte*) (showing that Google and Twitter are present on approximately 20 percent of websites and Facebook is present on approximately 25 percent of websites). By "third party tracking capability," we mean any method by which one party injects a tracking mechanism into a customer's traffic in order to monitor the customer's activity when the customer interacts with other parties. Cookies are a common third party tracker, but there are many other methods. *See id.* at 31 (explaining that "[t]hird parties on the web are any resources (images, tracking pixels, advertisements, code, etc.) loaded on a webpage that come from domains that are not the main domain you visited").

37 *See* Reisman and Narayanan June 17, 2016 *Ex Parte* at 32.

38 *Id.* at 35.

39 *See* Feamster Edge Provider Comments at 2; *see also* Upturn Comments at 6 ("DNS queries are almost never encrypted.").

40 Return Path Comments at 3.

41 Mozilla Comments at 4-5.

42 *See* National Cable & Telecommunications Association (NCTA) Reply at 21-24; AT&T Comments at 3-4; Howard Beales Comments at 4; CenturyLink Comments at 7; CTIA Comments at 14; Comcast Comments at 28 (explaining that if traffic is "encrypted using [Hypertext Transfer Protocol] HTTPS, the ISP only sees the top-level domain used to deliver packets, but otherwise is prevented from seeing either the contents of packets received or transmitted by the customer, or the full website address ... of the websites that the customer visits"); Employment and Training Association (ETA) Comments at 6-7; Information Technology and Innovation Foundation (ITIF) Comments at 3-5; T-Mobile Comments at 5.

43 Public Knowledge et al. Comments at 6 ("At an even more basic level, the timing of packet traffic can reveal data about a subscriber."); *see also id.* ("Traffic timing can reveal the hours when a subscriber is awake, asleep, or at work. It can reveal a person's religious beliefs (as with observance of the Sabbath), or unexpected changes in lifestyle, such as holidays, new relationships, or lost jobs."); Paul Ohm Testimony at 4 ("When you visit a website protected by the most widespread form of encryption in use, https or http over TLS, even though your BIAS provider cannot tell which individual page you are visiting on the website, it still can tell the domain name of the website you are communicating with, how often you return, roughly how much data you send and receive, and for how long each visit lasts."); Greenlining Institute and Media Alliance (Greenlining Institute) Comments at 5-6; Mozilla Comments at 4 ("All of a user's network traffic goes through their ISP, which means they have unfettered access to usage patterns and metadata. Usage patterns and metadata can be as revealing, or in some ways even more revealing, than content. Furthermore, users typically don't think about the potential for disclosure of private information that can come from metadata."); Software & Information Industry Association (SIIA) Comments at 3 ("Broadband service providers are unique in their ability to see the domains that their subscribers visit, even in cases where a website uses encryption.").

44 *See* Narayanan and Reisman Reply at 6; *see also* Upturn Comments at 8 ("A growing body of computer science research demonstrates that a network operator can learn a surprising amount about the contents of encrypted traffic without breaking or weakening encryption. By examining the features of the traffic — like the size, timing and destination of the encrypted packets — it is possible

to uniquely identify certain web page visits or otherwise reveal information about what those packets likely contain."); Feamster ISP Data Use Comments at 4.

45 *See* Upturn Comments at 3-6 (explaining that the fraction of total Internet traffic that is encrypted is a poor proxy for the privacy interests of a typical user, as 85 percent of the top 50 sites in each of health, news, and shopping categories still fail to encrypt browsing by default); *see also* Letter from Arvind Narayanan, Assistant Professor of Computer Science, Princeton University, to Chairman Tom Wheeler, FCC, WC 16-106 at 2 (filed May 27, 2016) (Narayanan Comments) (explaining that in their research, "we find that only 14.2% of the top 55,000 websites default to HTTPS on their home pages as of January 2016. This number falls to 8.6% on the top 1 million websites. Only a further 2.9% of the top 55,000 sites even offer HTTPS as an option").

46 *See* Sandvine Comments at 10 (forecasting that "by the end of 2016, global Internet traffic will be more than 70% encrypted, with some networks surpassing the 80% threshold"); *see also* Peter Swire Working Paper at 7; AT&T Reply at 19; Comcast Comments at 5; USTelecom Reply at 5.

47 *See* Free Press Reply at 11; Reisman and Narayanan June 17, 2016 *Ex Parte*, Attach., Part 2: ISPs and Privacy at 1 ("The percentage of traffic that is encrypted is not the right choice of metric since it is skewed by video statistics, especially Netflix."); *see also* NCL Reply at 9 (stating that "video streaming websites such as Netflix, which itself accounts for roughly 35 percent of North American internet traffic, are moving towards encryption").

48 Reisman and Narayanan June 17, 2016 *Ex Parte* at 13.

49 Upturn Comments at 3. Upturn also explains that devices such as "smart thermostats, home voice integration systems, and other appliances, fail to encrypt at least some of the traffic that they send and receive." *Id.* at 5.

50 Reisman and Narayanan June 17, 2016 *Ex Parte* at 18.

51 *See* NCL Reply at 9.

52 *See* Narayanan Comments at 2 (explaining challenges to encryption that many "third parties do not support encryption, and that this impedes the adoption of HTTPS by websites"); *see also* Upturn Comments at 4 ("In order for a site to migrate to HTTPS without triggering warnings in its users' browsers, each one of the third-party partners that site uses on its pages must support HTTPS.").

53 *See, e.g.*, OTI Comments at 7 ("The context in which broadband customers share private information with BIAS providers is specific and accompanied by cabined expectations: the customers share the information with BIAS providers to facilitate provision of a service for which they have contracted. The information is therefore most appropriately thought of as a loan to, rather than transferred to, broadband providers."); *see also* Consumer Federation of California (CFC) Comments at 5 ("When engaging in a transaction, a consumer may be required to provide personal information .... The consumer expectation is that the information is provided to complete the transaction, and not for other purposes.").

54 *See, e.g.*, Feamster Edge Provider Comments at 3 ("For example, in many cases, a user may register with an edge provider using a pseudonym. The user may simply elect not to provide certain personal information or data to a social network, or even to not use the social network at all.").

55 *2015 Open Internet Order*, 30 FCC Rcd at 5633, para. 84.

56 *See* New York State Attorney General Reply at 1-2 ("Consumers cannot avoid a BIAS provider the way consumers can avoid (without penalty), or otherwise freely and easily choose between, search engines or other websites, or smartphone applications."); CFC Comments at 6-7 (explaining that if a consumer wants to switch BIAS providers, the consumer must undertake the time-consuming, and often difficult, process of finding and establishing broadband service with a new provider, which requires a new contract and possibly new equipment. The consumer must also terminate service with the existing provider, which may cause the consumer to incur financial penalties.); *2015 Open Internet Order*, 30 FCC Rcd at 5631, para. 81 ("Among the costs that consumers may experience are: high upfront device installation fees; long-term contracts and early termination fees; the activation fee when changing service providers; and compatibility costs of owned equipment not working with the new service. Bundled pricing can also play a role, as 'single-product subscribers are four times more likely to churn than triple-play subscribers.' These costs may limit consumers' willingness and ability to switch carriers if such a choice is indeed available."). *But see* CTIA Comments at 15-16 (asserting that in the market for wireless broadband, providers are adopting practices that drive down switching costs, e.g., "they are

moving away from term-contracts with cancellation penalties, and offering to pay switching costs for new customers"); Free State Foundation Comments at 5-6; Howard Beales Comments at 3 (claiming BIAS providers "are not protected by uniquely high costs of switching that might justify different treatment").

57 CFC Comments at 6 ("Even if a consumer could easily substitute a BIAS provider, consumers are usually limited to the local dominant telephone provider and the local dominant cable television provider. Consumers do not have a wide variety of choices in BIAS providers. They can only use the services of BIAS providers who have invested in the infrastructure to deliver high-speed Internet in their local area."); Paul Ohm Testimony at 3 ("It is also appropriate for Congress to protect the privacy of information sent through a BIAS provider because of the relative lack of choice consumers enjoy for BIAS services").

58 *See Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, As Amended by the Broadband Data Improvement Act*, 31 FCC Rcd 699, 736, para. 86 (2016) (*2016 Broadband Progress Report*) (explaining further that in rural areas, only 13 percent of Americans have more than one option for service compared to 44 percent in urban areas).

59 *See, e.g.*, NCTA Comments at 54 ("The NPRM fails to cite any empirical evidence to support the notion that consumers believe there should be different privacy and data protection regimes depending upon whether their data is used by an ISP rather than by a search engine, Web site, app provider, or any of the advertising, analytics or other third party entities working with such edge providers."); Howard Beales Comments at 3 (claiming BIAS providers "do not pose a unique or more comprehensive privacy risk than other participants in the Internet ecosystem");CTIA Comments at 7 (arguing "ISPs' access to online consumers' personal information in this ecosystem is neither comprehensive nor unique").

60 *See, e.g.*, American Advertising Federation (AAF) et al. Comments at 2; Association of National Advertisers (ANA) Comments at 9 (arguing the Commission, offers insufficient evidence that privacy concerns are legitimate or that they will result in tangible harm to consumers); T-Mobile Comments at 11 ("The NPRM also fails to identify a problem with BIAS provider practices that needs to be remedied, or to demonstrate that the existing privacy framework or the marketplace is not protecting consumers."); SIIA Comments at 4.

61 NCL Reply at 13 ("Despite claims that the Commission's reclassification of BIAS as a common carrier under Title II will discourage investment and impose costs, the telecommunications industry had a strong financial year in 2015); *see also id.* (explaining that "AT&T's net income was over $13 billion, which marked a 60 percent increase from 2014").

62 *See* Public Knowledge et al. Reply at 7; OTI Comments at 10-11 (reporting that in January 2016, the City of Portland, Oregon's Office for Community Technology reported that in focus groups conducted by the city to improve the city's understanding of adoption challenges, privacy concerns were raised in every group); *see also 2016 Broadband Progress Report*, 31 FCC Rcd at 751-52, para. 126 (finding that consumers fearful of the loss of privacy may be less likely to use broadband connectivity, thus decreasing the demand for broadband investment and deployment); FTC Staff Comments at 2 (stating that "while consumers continue to increase their online presence, privacy and security are important not just for consumers but is also a crucial component for building trust in the online marketplace").

63 Mozilla Comments at 1.

64 *Broadband Privacy NPRM*, 31 FCC Rcd at 2557, para. 167.

65 *See 2007 CPNI Order*, 22 FCC Rcd at 6929, para. 3.

66 *See generally Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9611-12, paras. 9-11 (2013) (*2013 CPNI Declaratory Ruling*).

67 *2015 Open Internet Order*, 30 FCC Rcd at 5822-23, para. 466.

68 *See*47 CFR § 64.2003(o), (p) (defining "telecommunications carrier or carrier" and "telecommunications service"). In accordance with these definitions, we continue to consider entities providing interconnected VoIP service to be telecommunications carriers for the purposes of these rules. *See infra* Part IV.E. The Commission has not classified interconnected VoIP service as telecommunications

service or information service as those terms are defined in the Act, and we need not and do not make such a determination today. *See*47 U.S.C. § 153(24), (53) (defining "information service" and ""telecommunications service"); *2007 CPNI Order*, 22 FCC Rcd at 6929, para. 3 (extending application of the CPNI rules to providers of interconnected VoIP service).

69 Specifically, a broadband Internet access service is "a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this part." 47 CFR § 8.2(a); *2015 Open Internet Order*, 30 FCC Rcd at 5682, para. 187; *see also* INCOMPAS Comments at 3 (distinction in BIAS definition between mass market and business services should apply in Section 222 context); Information Technology Industry Council (ITIC) Comments at 6 (the definition of BIAS should exclude Internet intermediary services and "over the top" services).

70 As used in the foregoing sentence and in the definition of "customer" below, a "person" includes any individual, group of individuals, corporation, partnership, association, unit of government, or legal entity, however organized. *Cf. Preserving the Open Internet*, Report and Order, 25 FCC Rcd 17905, 17937, para. 54 n.172 (2010) (*2010 Open Internet Order*); 47 CFR § 54.8(a)(6).

71 *2015 Open Internet Order*, 30 FCC Rcd at 5685, para. 191.

72 *See, e.g.*, *2015 Open Internet Order*, 30 FCC Rcd at 5773, para. 377 (explaining that email and cloud-based storage are "separable information services" from the broadband Internet access service).

73 *See* Letter from Loretta Polk, Vice President & Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1-2 (filed Oct. 20, 2016) (NCTA Oct. 20, 2016 *Ex Parte*).

74 *See*47 U.S.C. § 222(a), (c).

75 *See* American Cable Association (ACA) Comments at 57 (supporting "a single privacy and data security framework" and harmonization of Section 222 rules and definitions); Rural Wireless Association (RWA) Reply at 7 ("Harmonization provides several benefits, including increased provider efficiency, better customer understanding, and higher compliance rates."). Nex-Tech explains that "because it is already subject to the CPNI rules as a provider of voice service, Nex-Tech has aligned its [BIAS] policies and procedures with respect to customer information with its compliance of the Commission's voice CPNI rules. Nex-Tech and WTA ... generally believe this is common across the board for RLECs." Letter from Patricia Cave, Director, Government Affairs, WTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed April 25, 2016) (WTA & Nex-Tech Apr. 25, 2016 *Ex Parte*).

76 *See, e.g.*, *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13332-35 (2014) (*TerraCom NAL*) (voice services).

77 47 CFR § 64.2003(f).

78 *See, e.g.*, OTI Comments at 14 ("Including only current customers would be too narrow because of the strong incentives for BIAS providers to collect and retain data from all customers without limitation.").

79 *See, e.g.*, FTC, Big Data: A Tool for Inclusion or Exclusion?, at 1 (2016), https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report (2016 FTC Big Data Report) ("A common framework for characterizing big data relies on the 'three Vs,' the volume, velocity, and variety of data, each of which is growing at a rapid rate as technological advances permit the analysis and use of this data in ways that were not possible previously."); Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values at 1 (2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (2014 Administration Big Data Report) ("The collection, storage, and analysis of data is on an upward and seemingly unbounded trajectory, fueled by increases in processing power, the cratering costs of computation and storage, and the growing number of sensor technologies embedded in devices of all kinds.").

80 *See, e.g.*, OTI Comments at 14 ("Including only current customers would be too narrow because of the strong incentives for BIAS providers to collect and retain data from all customers without limitation."). *But see* WISPA Reply at 26-28 (stating that the rules should not protect applicants and former customers).

81 *See* Rafi Goldberg, NTIA, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online *Activities* (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (discussing, *inter alia*, how privacy concerns can deter many Americans from engaging in important economic and civic online activities).

82 47 U.S.C. § 1302(a); *see generally 2016 Broadband Progress Report*, 31 FCC Rcd 699.

83 *TerraCom NAL*, 29 FCC Rcd at 13333, para. 23. In *TerraCom* we observed, *inter alia*, that "consumers applying for telecommunications services have a reasonable expectation that the carrier will protect the confidentiality of the [proprietary information] they provide as part of that transaction" and that the carriers themselves treated applicants as "customers" in their forms and policies. *Id.* at 13332-35, paras. 21-28.

84 *See* WISPA Comments at 23-24 (asserting that applicants should be excluded because they can review a provider's privacy policy before sharing personal information); CTIA Comments at 95 (asserting that inclusion would hinder providers' ability to solicit prospective customers); Sprint Comments at 4; T-Mobile Comments at 56; INCOMPAS Comments at 9-10 (including former customers could hinder providers' ability to try to win them back); NTCA Comments at 13-17 (asserting that other industries are not required to protect applicant and former customers beyond FTC standard; the inclusion will burden small providers).

85 *See, e.g.*, Paul Vixie Comments at 3-4; Center for Digital Democracy (CDD) Comments at 14 (asserting that the rules should protect each user in a household).

86 *See* Common Sense Kids Action Comments at 9 (supporting a "'customer dashboard' in which a main subscriber can set different privacy preferences for different devices or log-ins."). *See infra* Part III.H.2.

87 *See* Access Now Comments at 4. *But see* Sprint Comments at 4-5 (including "all conceivable users of the network would lead to unworkable obligations for providers"); Security and Software Engineering Research Center (S^2ERC) Comments at 5-6 (only the account holder should qualify as a customer); NTCA Comments at 17-18 (same).

88 *See* OTI Comments at 17-18 ("Separate accounts for other members of the household provide a straightforward mechanism for providing notice of privacy practices and acquiring opt-in or opt-out consent for those practices."); CDD Comments at 14 ("[T]hose with a login (or are identified as a distinct customer by the subscriber) should be provided with the same fair treatment for their privacy."); Access Now Comments at 4 (supporting protections for users other than the primary account holder); Paul Vixie Comments at 3-4 (same); Consumer Federation of California Comments at 14 (same).

89 47 U.S.C. § 222(h)(1).

90 *See*47 U.S.C. § 222(h)(1)(B); Comcast Comments at 78-79 (BIAS "does not fit the definition of either" telephone exchange service or telephone toll service); NTCA Comments at 19 (agreeing that (h)(1)(B) is inapplicable to BIAS); *accord* USTelecom Comments at 6.

91 *See* CDT Reply at 19; OTI Reply at 5-6.

92 *See* CTIA Comments at 44 (arguing that unlike voice context, many types of BIAS CPNI are available to third parties); USTelecom Comments at 6-7 ("the same data, and even more, is available to other members of the Internet ecosystem"); Cincinnati Bell Tel. Co. (Cincinnati Bell) Comments at 6 (information "sent onto the open Internet in order to make the service work" should not qualify as CPNI); CenturyLink Comments at 15-16 (information "easily obtained by multiple parties ... cannot be deemed CPNI"); NTCA Comments at 21-22 (arguing that source IP addresses should not be protected because customers share them with third parties).

93 *See, e.g.*, OTI Reply at 5-6 ("Whether other online entities have access to this information is irrelevant to the statutory determination .... The mere fact that third parties have access to similar or even identical information does not factor into the statute because that information was not provided *to the carrier by the customer*."). We note, for clarity, that both inbound and outbound traffic are made available to the carrier by the customer solely by virtue of the carrier-customer relationship. The directionality of the traffic is irrelevant as to whether it satisfies the statutory definition of CPNI.

94 CDT Reply at 19.

95 *See, e.g.*, OTI Reply at 5-6.

96 *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1236 (10th Cir. 1999) ("[T] he specific and dominant purpose of § 222 is the protection of customer privacy."); CDT Reply at 19 ("[I]t does not follow that BIAS providers should be able to freely share sensitive information simply because some other actors are already privy to it. That the data exists in the hands of certain other entities does not mean that further dissemination by the BIAS provider no longer implicates consumer privacy.").

97 *See* CTIA Comments at 49 ("Data acquired from third parties falls wholly outside of this definition."); *accord* Comcast Comments at 75-76.

98 *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27. CPE is "equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications." 47 U.S.C. § 153(16); *see also*47 CFR § 64.2003(h). A mobile station is "a radio-communication station capable of being moved and which ordinarily does move." 47 U.S.C. § 153(34). *See infra* para. 80.

99 *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27.

100 *See infra* para. 76; *See Cellco P'ship, d/b/a Verizon Wireless*, Order, 31 FCC Rcd 1843 (Enf. Bur. 2016) (*Verizon UIDH Consent Decree*).

101 *See* Public Knowledge Comments at 27-28; Public Knowledge White Paper at 60-61. *See also infra* Part III.B.3.c.

102 *See infra* Part III.B.3.b.

103 *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

104 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2514, para. 40; *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

105 Access Now Comments at 4. *Accord* Electronic Frontier Foundation (EFF) Comments at 3 (supporting illustrative examples instead of a comprehensive list).

106 *2007 CPNI Order*, 22 FCC Rcd at 6931; *see also*47 CFR § 64.2003(d); 47 CFR § 64.5103(c).

107 *See* EFF Comments at 3 ("Illustrative examples ... will provide useful guidance for providers and reduce compliance costs without risking obsolescence."); Jon Peha Reply at 6 (broad definition of CPNI necessary given BIAS providers' gatekeeping role).

108 *See* James F. Kurose & Keith W. Ross, Computer Networking: A Top-Down Approach 47-50 (6th ed. 2013) (Kurose & Ross).

109 *See, e.g.*, David D. Clark et al., *Tussle in Cyberspace: Defining Tomorrow's Internet*, 13 IEEE/ACM Transactions on Networking 462-475 (2005); Kurose & Ross at 49-53.

110 Across all devices, equivalent layers perform the equivalent functions. This compatibility and interoperability is typically represented as horizontal relationships. Kurose & Ross at 53-55.

111 *See* Internet Engineering Task Force, Requirements for Internet Hosts — Communications Layers, RFC 1122 (Oct. 1989), https://tools.ietf.org/html/rfc1122.

112 *See* Kurose & Ross at 53-55.

113 *See id.* at 756-60.

114 *See id.* at 47-55; Internet Engineering Task Force, Requirements for Internet Hosts — Communications Layers, RFC 1122 (Oct. 1989), https://tools.ietf.org/html/rfc1122.

115 *See, e.g.*, Kurose & Ross at 55.

116 *See id.*, Chapter 2.

117 *See id.*, Chapter 3. Two transport protocols are widely deployed on the Internet: the Transmission Control Protocol (TCP), which ensures that data arrives intact, and the User Datagram Protocol (UDP), which provides fewer guarantees about data integrity. *Id.*

118 *See id.*, Chapter 4.

119 *See id.*

120 *See id.*, Chapter 5.

121 *See id.*

122 In this section, we provide guidance on what data elements constitute CPNI; this is distinct from the question of whether a data element constitutes *individually identifiable* CPNI and is thus "customer proprietary information." *See infra* Appx. A, § 64.2002(f).

123 *See*47 U.S.C. § 222(h)(1)(A).

124 NTCA Comments at 20.

125 *See 2007 CPNI Order*, 22 FCC Rcd at 6931, para. 5; *see also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended; 2000 Biennial Regulatory Review—Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14864, para. 7 (2002) (*2002 CPNI Order*). In 2011, the Sixth Circuit agreed with AT&T's argument that information in a service plan "clearly constitutes CPNI" in the voice context. *CMC Telecomm, Inc. v. Mich. Bell Tel. Co.*, 637 F.3d 626, 630 (6th Cir. 2011).

126 *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para. 22 ("The location of a customer's use of a telecommunications service also clearly qualifies as CPNI."); 47 U.S.C. § 222(h)(1)(A).

127 Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1285, 1289 (1999) (codified at 47 U.S.C. § 222(f) (""Authority to use location information")).

128 *See, e.g.*, CTIA Comments at 135 (urging rules to "cover only precise GPS location information"); Future of Privacy Forum Reply at 6-7; NCTA Comments at 61.

129 *See, e.g.*, Future of Privacy Forum Comments at 20-25; S^2ERC Comments at 6; Farsight Security Comments at 5.

130 *See*47 U.S.C. § 222(h)(1)(A). *See also* CDT Reply at 18-19; Letter from Laura Moy, Institute for Public Representation, Counsel, New America's Open Technology Institute, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 4-6 (filed Oct. 13, 2016) (OTI Oct. 13, 2016 *Ex Parte*).

131 *See supra* Part III.B.3.a(i)(a).

132 *See, e.g.*, Kurose & Ross at 463-65. *Cf.* NTCA Comments at 21 ("a MAC address is associated to a device"). *See also* CDT Reply at 19 ("It is believed that some future forms of BIAS network architectures may remove the need for a network modem, making available a MAC address farther up into the BIAS provider's network outside of the home network."); EFF Comments at 3-4 (device identifiers implicate customers' privacy interests and should be protected). The Commission has previously recognized that unique device identifiers such as an "electronic serial number" are "call data information" in the TRS CPNI context. 47 CFR § 64.5103(c).

133 *See* Kurose & Ross at 463-65; Front Porch Comments at 2 ("ISPs use this address for internal network management purposes, including access permissions, data consumption, and service tier monitoring."); CDT Comments at 13-14 ("MAC addresses and other device identifiers relate to the destination of a telecommunications service because they are used to route packets to individual devices connected to a network."); NCTA Comments at 62-63 ("device identifiers or other data elements ... may be used by broadband providers to facilitate email traffic routing"). We disagree with Sandvine, which argues that link layer information such as MAC addresses do not relate to the technical configuration of network traffic or the destination of packets. *See* Sandvine Comments at 22-23.

134 For a brief overview of Internet architecture and layering, see *supra* Part III.B.3.a(i)(a).

135 *See*47 U.S.C. § 222(h)(1)(A).

136 *See* Internet Engineering Task Force, The Internet Numbers Registry System, RFC 7020 (2013), https://tools.ietf.org/html/rfc7020 (discussing non-reserved globally unique unicast IP addresses assigned through the Internet Numbers Registry System).

137 *See, e.g.*, Kurose & Ross at 130, 331-63.

138 The Commission has previously held telephone numbers dialed to be CPNI. *See 2007 CPNI Order*, 22 FCC Rcd at 6931, para. 5. Further, our CPNI rules for TRS providers recognize IP addresses as call data information. 47 CFR § 64.5103(c). By this analogy, we mean only that both are "roughly similar numerical identifiers" used to route telecommunications. *See* Internet Society June 6, 2016 *Ex Parte* at 2. We do not intend to imply that IP addresses are or should be administered in the same manner as telephone numbers. *See id.* at 1-2 (discussing the differences in each identifier's governance). This definitional change to our regulations in no way asserts Commission jurisdiction over the assignment or management of IP addressing.

139 *See* Comcast Comments at 78 ("IP addresses identify the 'logical' location of a device for purposes of routing Internet traffic" (footnote omitted)); CDT Comments at 14 (citations omitted); Sandvine Comments at 22-23 (IP addresses relate to destination); NCTA Comments at 62 ("IP addresses ... may be used by broadband providers to facilitate email traffic routing" (citation omitted)); CDT Comments at 14 ("IP addresses are the destinations to which BIAS providers deliver packets and also may be associated with physical locations."); S^2ERC Comments at 6-7.

140 *See, e.g.*, CDD Comments at 15; CDT Comments at 14. A BIAS provider is uniquely capable of geo-locating an IP address. Most notably, in the case of mobile broadband Internet access service, the provider knows the geo-location of the cell towers to which the customer's device connects and can use this to determine the customer's device location.

141 Harold Feld, et al., Public Knowledge, Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World 47 (2016) (Public Knowledge White Paper) (citing Dan Jerker B. Svantenson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet"*, 23 J. Marshall J. Computer & Info. L. 101, 109-11 (2004)).

142 *See supra* Part III.B.3.a(i)(a); Sandvine Comments at 22-23 (arguing that IP addresses relate to technical configuration).

143 *See, e.g.*, Comcast Comments at 77; NCTA Comments at 21.

144 47 U.S.C. § 222(h)(1)(A).

145 *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27; *Verizon UIDH Consent Decree*, 31 FCC Rcd at 1843-44, paras. 2-5.

146 Cincinnati Bell Comments at 6; *accord* Comcast Comments at 81; William Rinehart Comments at 3 (Rinehart); *see also* S^2ERC Comments at 6-7 (arguing that IP addresses are widely accessible, but also can be "sensitive information"); Peter Swire & Justin Hemmings (Swire & Hemmings) Reply at 7-8 (arguing that IP addresses are available to intermediaries between the customer and the content provider).

147 *See supra* para. 49.

148 A dynamic IP address is one that the BIAS provider can change. *See generally* Network Working Group, Internet Eng'g Task Force, *RFC 2131: Dynamic Host Configuration Protocol* (1997), https://tools.ietf.org/html/rfc2131; Network Working Group, Internet Eng'g Task Force, *RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* (2003), https://tools.ietf.org/html/rfc3315.

149 Return Path Comments at 3. *See also, e.g.*, Comcast, Comcast Legal Response Ctr., *Law Enforcement Handbook (Rev. May 1, 2015)* at 10 (2015), https://www.comcast.com/~/Media/403EEED5AE6F46118DDBC5F8BC436030.ashx (noting that Comcast retains dynamic IP address log files for 180 days).

150 We note that these potential privacy benefits of dynamic IP addresses depend upon the specific network configuration and practices of the BIAS provider. For example, a provider may assign a dynamic IP address to a customer for a long period of time, such that

it is effectively equivalent to a static IP address. In certain configurations (e.g., IPv6 without privacy extensions), a dynamic IP address can be *more* revealing than a static IP address, because it includes other network identifiers (such as a MAC address). *See, e.g.*, Network Working Group, Internet Eng'g Task Force, *RFC 3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6* at 3 (2001), https://tools.ietf.org/html/rfc3041; Comcast, Comcast Legal Response Ctr., *Law Enforcement Handbook (Rev. May 1, 2015)* at 10, https://www.comcast.com/~/Media/403EEED5AE6F46118DDBC5F8BC436030.ashx (noting that Comcast retains dynamic IP address log files for 180 days).

151 *See* Feamster ISP Data Use Comments at 5. Whether or not the customer uses the BIAS provider's in-house DNS lookup service is irrelevant to whether domain names satisfy the statutory definition of CPNI. *See* Farsight Security Comments at 7.

152 *See supra* Part III.B.3.a(i)(a).

153 CDT Comments at 14 (citing Internet Eng'g Task Force, *RFC 791: Internet Protocol - DARPA Internet Program Protocol Specification* 12 (1981), https://tools.ietf.org/html/rfc791).

154 *See* CDT Comments at 13-14; EFF Comments at 3-4.

155 *See*47 U.S.C. § 222(h)(1)(A); *see also* EFF Comments at 4.

156 There are many common forms of traffic statistics, such as IPFIX, and we believe it is important to focus on how BIAS providers use these data, rather than single out particular technologies. *See* Feamster ISP Data Use Comments at 2-7.

157 *2007 CPNI Order*, 22 FCC Rcd at 6930-31, para. 5; *see also*47 CFR § 64.5103(c); *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 25; *2007 CPNI Order*, 22 FCC Rcd at 6936, para. 13 n.45.

158 *See*47 U.S.C. § 222(h)(1)(A); OTI Comments at 20-21; CDT Comments at 14-15 ("Essentially, ports are a more granular form of destination information than IP and MAC addresses, indicating [to] which applications particular packets may be destined."); Public Knowledge White Paper at 47-48.

159 *See* CDT Comments at 14 ("Network ports are subaddresses within the internet protocol and are used by operating systems to sort and deliver packets to individual applications.").

160 *See* Network Working Group, Internet Eng'g Task Force, *RFC 1180: A TCP/IP Tutorial* 23, 24 (1991), https://tools.ietf.org/html/rfc1180 ("Well-defined port numbers are dedicated to specific applications." *Id.* at 24). Port destinations are analogous to telephone extensions in the voice context.

161 *See* NTCA Comments at 22 (port information "can be used to discern whether a person was using email or browsing the Internet"); CDT Comments at 14-15 ("For instance, ports 109 and 110 indicate the use of the Post Office Protocol (POP), marking the packet as an email transmission, while port 1214 indicates the use of the Kazaa peer-to-peer file sharing protocol."); OTI Comments at 20-21 ("For instance, port 80 is used for HTTP traffic and port 443 is used for HTTPS traffic. Some ports are very specific, and information about traveling to those ports may reveal even more detailed information about a BIAS customer's use of the service. For example, port 194 is used for Internet Relay Chat and port 666 for the 1993 video game Doom."). Though sometimes port numbers may not reveal anything of significance, *see, e.g.*, Farsight Security Comments at 8 ("One result of the widespread use of perimeter firewalls is that 'everything' seems to tunnel its traffic over port 80. Port numbers have largely gone from reliable clues to the type of application generating traffic seen on the wire to either: [e]verything over port 80, or [e]verything over a random dynamic port."), they often do, and therefore we conclude that they relate to the destination, type, or technical configuration of the service. *See, e.g.*, Internet Assigned Numbers Authority, *Service Name and Transport Protocol Number Registry* (Oct. 17, 2016), http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml; *see generally* Internet Eng'g Task Force, *RFC 6335: Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry* (2011), https://tools.ietf.org/html/rfc6335.

162 *See* CDT Comments at 14-15 ("At the transport layer, the two most common protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) include header fields specifying source and destination ports as well as packet size.").

163 *Id.*

164 *See* 47 U.S.C. § 222(h)(1)(A); CDT Comments at 15 (discussing the uses of application headers).

165 *See supra* Part III.B.3.a(i)(a).

166 *See* Ctr. for Democracy & Tech., *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (2016), https://cdt.org/files/2016/01/2016-01-20-Packets_Layers_fnl.pdf (CDT White Paper). Application headers are analogous in the voice telephony context to a customer's choices within telephone menus used to route calls within an organization (e.g., "Push 1 for sales. Push 2 for billing."). *See Broadband Privacy NPRM*, 31 FCC Rcd at 2517, para. 50.

167 *See* Kurose & Ross at 51; CDT Comments at 15; CDT White Paper.

168 *See* CDT Comments at 15. Application headers may also include information relating to persistent identifiers, use of encryption, and virtual private networks (VPNs). Email headers may also include the subject line.

169 For example, HTTP has a field called "Content-Length." *See* Network Working Group, Internet Eng'g Task Force, *RFC 2616: Hypertext Transfer Protocol — HTTP/1.1* at 119 (1999), https://www.ietf.org/rfc/rfc2616.txt.

170 *See* CDT Comments at 15 ("These identifiers also encompass each element of CPNI, relating [to] the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service to an individual subscriber.").

171 *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27; *Verizon UIDH Consent Decree*, 31 FCC Rcd at 1843-44, paras. 1-5.

172 *See* CDT Comments at 15 ("In the practice known as 'HTTP header injection,' BIAS providers add a new HTTP header line after the message leaves the customer's browser. This header serves as a unique marker identifying all HTTP messages sent from a single subscriber account.").

173 *See* 47 U.S.C. § 222(h)(1)(A).

174 *See* T-Mobile, *T-Mobile Privacy Policy* (Nov. 25, 2015), http://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy ("We may also collect information about applications on your device, the fact that an application has been added, when an application is launched or fails to launch, and length of time an application has been running."); AT&T, *AT&T Privacy Policy* (July 24, 2015), https://www.att.com/gen/privacy-policy?pid=2506#print (AT&T collects "how often you open an application, how long you spend using the app and other similar information."); Sprint, *Sprint Corporation Privacy Policy* (July 22, 2016), https://www.sprint.com/legal/privacy.html (Sprint collects information about "applications purchased, applications downloaded or used, and other similar information."); Verizon, *Verizon Full Privacy Policy*, http://www.verizon.com/about/privacy/full-privacy-policy (last visited Oct. 5, 2016) (Verizon collects "application and feature usage").

175 *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9615-16, para. 21-23.

176 *See* NTCA Comments at 22-23; *see supra* para. 48.

177 *See supra* Part III.B.3.a(i)(a); *see also* Public Knowledge White Paper at 48; CDT Comments at 17.

178 *See* Sandvine Comments at 2-3; CDT Reply at 14 (BIAS providers scan payloads to "searc[h] for protocol non-compliance ... viruses and spam, interference, and for collecting network statistics."). BIAS providers also use various network management techniques to minimize network congestion while transmitting application payloads.

179 *See infra* Part III.B.3.d.

180 *See* 47 U.S.C. § 222(h)(1)(A).

181 47 U.S.C. § 153(16); 47 CFR § 64.2003(h).

182 *See generally Bundling of Cellular Customer Premises Equipment and Cellular Service*, Report and Order, 7 FCC Rcd 4028 (1992).

183 47 U.S.C. § 153(34).

184 *See* NTCA Comments at 25.

185 *See id.* at 23-25.

186 *See supra* para. 49

187 *See* NTCA Comments at 25; *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Order, 13 FCC Rcd 12390, 12392-93, paras. 2-4 (CC Bur. 1998) (*1998 CPNI Clarification Order*).

188 *1998 CPNI Clarification Order*, 13 FCC Rcd at 12393, para. 4.

189 47 U.S.C. § 222(a).

190 *See TerraCom NAL*, 29 FCC Rcd at 13330-32, paras. 14-20 (defining the scope of the term "proprietary information").

191 *See infra* Parts III.B.3.c, III.B.3.d.

192 *See TerraCom NAL*, 29 FCC Rcd at 13330-31, para. 15 ("In the context of public broadcasting, for example, the Corporation for Public Broadcasting (CPB) must maintain for public inspection certain financial information about programming grants. But Congress also recognized that 'proprietary, confidential, or privileged information' should not be made public, and Congress thus expressly excluded such information from public disclosure. Similarly, ... [r]ecognizing that [entities that review interoperability of telephone equipment] necessarily gain access to extremely valuable trade secrets, Congress explicitly prohibited those review entities from 'releasing or otherwise using any proprietary information' belonging to the manufacturer without written authorization."); *see also* CDT Comments at 12.

193 *See Furnishing of Customer Premises Equipment and Enhanced Services by American Telephone & Telegraph Co.*, Order, 102 F.C.C.2d 655, 692-93, para. 64 (1985) (discussing 47 C.F.R. § 64.702 (1984) and noting that "customer proprietary information ... belongs to the customers, and many may not want it to be made public").

194 *See infra* Part III.B.3.c. *See, e.g.*, 18 U.S.C. § 2710 (Video Privacy Protection Act); 18 U.S.C. §§ 2721-2725 (Driver's Privacy Protection Act); 45 CFR pt. 164 (HIPAA rules); 16 CFR pt. 313 (Gramm-Leach-Bliley Act rules); 16 CFR pt. 682 (Fair Credit Reporting Act rules); 12 CFR pt. 1022 (Fair and Accurate Credit Transaction Act disposal rule); 45 CFR pt. 5b (Privacy Act rules); 34 CFR pt. 99 (FERPA rules); 16 CFR pt. 312 (COPPA rules); 2015 Administration CPBR Discussion Draft § 4(a)(1). *See also* CDT Comments at 8-9; Electronic Privacy Information Center (EPIC) Comments at 14-15.

195 *TerraCom NAL*, 29 FCC Rcd at 13330-31, paras. 14, 17.

196 *Id.*, para. 14.

197 *Id.*

198 *See* CTIA Comment at 33-34 (arguing that information cannot be proprietary if it is available to others); NTCA Comments at 28-29 (many types of PII are publicly available). *But see* Free Press Reply at 8-10 ("That edge providers may have access to certain kinds of 'Proprietary Information' is immaterial to whether the FCC can protect the use of that information by broadband ISPs.").

199 *See* Daniel J. Solove, Nothing to Hide 178 (2011) ("The problem with the secrecy paradigm is that we *do* expect some degree of privacy in public. We don't expect total secrecy, but we also don't expect somebody to be recording everything we do.") (emphasis in original). A panopticon limited to the public sphere can still infringe the dignity of the private individual. *See United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

200 *See Corley v. United States*, 556 U.S. 303, 314 (2009) ("a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant") (internal quotation marks, alterations, and citation omitted).

201 *See* Competitive Carriers Association (CCA) Comments at 4 (proposal is a ""significant expansion" of coverage); CenturyLink Comments at 35-36 ("broad scope" of coverage could increase compliance costs); INCOMPAS Comments at 8 ("sweeping alterations

to the current framework"); Internet Commerce Coalition (ICC) Comments at 13 (broader coverage than previous rules); USTelecom Comments at 7 ("massive expansion" of coverage under Section 222); WISPA Comments at 12-13 ("vast expansion of the universe of information that would be subject to protection").

202 *See* 2012 FTC Privacy Report at v, vii-ix, 15-22; *see also* ACLU Comments at 2-3 ("The nation's mail, telephone, and telegraph infrastructures have long been subject to rules protecting [Americans'] privacy.").

203 FTC Staff Comments at 4. *See, e.g.*, *FTC v. E.M.A. Nationwide, Inc.*, 767 F.3d 611 (6th Cir. 2014); *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009); *FTC v. INC21.com Corp.*, 688 F.Supp.2d 927 (N.D. Cal. 2010), *aff'd*, 475 Fed. Appx. 106 (9th Cir. 2012); *Snapchat, Inc.*, Decision & Order, FTC Docket No. C-4501 (Dec. 23, 2014), https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter; *Accretive Health, Inc.*, Decision & Order, FTC Docket No. C-4432 (Feb. 5, 2014), https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter; *Compete, Inc.*, Decision & Order, FTC Docket No. C-4384 (Feb. 20, 2013), https://www.ftc.gov/enforcement/cases-proceedings/102-3116/compete-inc.

204 *See, e.g.*, *TerraCom NAL*, 29 FCC Rcd at 13325, para. 2; *Cox Commc'n Inc.*, Order, 30 FCC Rcd 12302, 12303, para. 4. (Enf. Bur. 2015) (*Cox Consent Decree*); *Verizon UIDH Consent Decree*, 31 FCC Rcd at 1843, para. 2.

205 *See TerraCom NAL*, 29 FCC Rcd at 13325, para. 2.

206 *See*47 U.S.C. § 605; 18 U.S.C. § 2511 (ECPA); *see also infra* Part III.B.3.d.

207 *See* Lee Rainie, The State of Privacy in post-Snowden America, Pew Research Center (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (91 percent of Americans agree that consumers have lost control of how personal information is collected and used by companies and 68 percent support more protective privacy and data retention laws); Rafi Goldberg, NTIA, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities (May 13, 2016), https://www.ntia.doc.gov/print/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (consumers change their online behavior if they believe their privacy is compromised); Morrison & Foerster, Consumer Outlooks on Privacy, 7 (2016), www.mofo.com/~/ media/Files/Resources/2016/MoFoInsightsConsumerOutlooksPrivacy.pdf (describing consumer privacy expectations).

208 Lee Rainie, The State of Privacy in post-Snowden America, Pew Research Center (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

209 CDT Comments at 8-9 (citing regulations issued under Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), Fair and Accurate Credit Transactions Act (FACTA), Privacy Act, Family Educational Rights and Privacy Act (FERPA), the Communications Act, Telephone Consumer Protection Act (TCPA), Children's Online Privacy Protection Act (COPPA), and CAN-SPAM Act of 2003).

210 The Act also protects the PII of cable and satellite subscribers. *See*47 U.S.C. § 338(i); 47 U.S.C. § 551 (collectively, "Satellite and Cable Privacy Acts").

211 *See, e.g.*, Satellite and Cable Privacy Acts; 18 U.S.C. § 2710 (Video Privacy Protection Act (VPPA)); 18 U.S.C. §§ 2721-2725 (Driver's Privacy Protection Act (DPPA)); 45 CFR pt. 164 (HIPAA rules); 16 CFR pt. 313 (GLBA rules); 16 CFR pt. 682 (FCRA rules); 12 CFR pt. 1022 (FACTA disposal rule); 45 CFR pt. 5b (Privacy Act rules); 34 CFR pt. 99 (FERPA rules); 16 CFR pt. 312 (COPPA rules); 2015 Administration CPBR Discussion Draft § 4(a)(1). *See also* CDT Comments at 8-9; EPIC Comments at 14-15.

212 *Compare Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) ("[O]ur contemplation cannot be only of what has been, but of what may be. The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."), *with Riley v. California*, 134 S.Ct. 2473, 2490 (2014) ("Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

213 In the *TerraCom NAL*, we found NIST guidelines to be "informative" for determining the scope of PII; similarly we use those guidelines to inform our rule here. *See TerraCom NAL*, 29 FCC Rcd at 13331, para. 17; NIST, Guide to Protecting the Confidentiality

of Personally Identifiable Information (PII) at § 2.1 (2010), http://www.nist.gov/manuscript-publication-search.cfm?pub_id=904990 (NIST PII Guide); 2012 FTC Privacy Report at 18-22; 2015 Administration CPBR Discussion Draft at § 4(a)(1). *See also Cox Consent Decree*, 30 FCC Rcd at 12306-07, paras. 2(s), 4.

214 *See infra* Appx. A, at § 64.2002.

215 *See* NIST PII Guide § 2.1 (defining linked and linkable); CDT Comments at 9 ("'Identifiable' information is increasingly contextual; while one or two data points alone may not identify an individual, these data could be linked to that person if combined with other data.").

216 *See, e.g.*, Access Now Comments at 5; CDT Comments at 9-10; EFF Comments at 5; EPIC Comments at 18-19; Front Porch Comments at 2; FTC Staff Comments at 9; Public Knowledge Comments at 28.

217 *See* NIST PII Guide §§ 2.1-2.2; 2012 FTC Privacy Report at 18-22; 2015 Administration CPBR Discussion Draft at § 4(a)(1); 34 CFR §§ 99.3, 303.29; 17 CFR § 227.305(b); 32 CFR §§ 310.4, 311.3(g), 329.3; 6 CFR § 37.3; 45 CFR § 75.2; 2 CFR § 200.79. *See also* Clay Johnson III, Deputy Director for Management, Office of Management and Budget, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, at 1 n.1 (2007), https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

218 FTC Staff Comments at 9 (emphasis in original).

219 CDT Comments at 10.

220 NIST PII Guide § 2.1.

221 Software & Information Industry Association (SIIA) Comments at 11-12.

222 FTC Staff Comments at 9.

223 *See* AT&T Reply at 39-40 (supporting reasonableness qualifier); T-Mobile Comments at 20 (linkability standard overbroad without a reasonableness qualifier like the FTC); CompTIA Comments at 2-3 (same); CTIA Comments at 38 (same); NCTA Reply at 40 (same); SIIA Reply at 3 (same); WISPA Reply at 16-17; Cincinnati Bell Comments at 5 ("[T]he Commission's PII regime should mirror the existing FTC definitions.").

224 FTC Staff Comments at 10. As discussed above, devices in the BIAS context include a customer's smartphone, tablet, computer, modem, router, videophone, IP caption phone, and other consumer devices capable of connecting to broadband services. *See supra* para. 80.

225 FTC Staff Comments at 10. *Accord* EPIC Comments at 18 (discussing how persistent identifiers like device information can be used to map out an individual's interactions); SIIA Comments at 12 (supporting the FTC's test for linkability to a "consumer, computer, or device").

226 Digital Advertising Alliance, Application of Self-Regulatory Principles to the Mobile Environment, 6 (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf (DAA Mobile Guidance) (defining "De-Identification Process").

227 *See* Audience Partners Comments at 9-17; Future of Privacy Forum Comments at 5.

228 *See supra* paras. 67-71.

229 *See* CenturyLink Comments at 16; Cincinnati Bell Comments at 7.

230 "I find little comfort in the Court's notion that no invasion of privacy occurs until a listener obtains some significant information by use of the device .... A bathtub is a less private area when the plumber is present even if his back is turned." *Kyllo v. United States*, 533 U.S. 27, 39 (2001) (quoting *U.S. v. Karo*, 468 U.S. 705, 735 (1984) (Stevens, J., concurring in part and dissenting in part)). *See also* EPIC Comments at 18.

231 *See infra* Part III.D.1.

232 *See, e.g.*, Access Now Comments at 5; CDT Comments at 8-10; Consumer Watchdog Comments at 5; EFF Comments at 5; EPIC Comments at 18-19; OTI Comments at 22; Return Path Comments at 5.

233 *See, e.g.*, *TerraCom NAL*, 29 FCC Rcd at 13331-32, paras. 17-18; *see also AT&T Services, Inc.*, Order and Consent Decree, 30 FCC Rcd 2808, 2811, para. 2(s) (Enf. Bur. 2015) (*AT&T Consent Decree*).

234 *See* NIST PII Guide §§ 2.1-2.2.

235 *See, e.g.*, *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009); *Snapchat, Inc.*, Decision and Order, F.T.C. Docket No. C-4501 (Dec. 23, 2014), https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter; *Accretive Health, Inc.*, Decision and Order, F.T.C. Docket No. C-4432 (Feb. 5, 2014), https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter; *Compete, Inc.*, Decision and Order, F.T.C. Docket No. C-4384 (Feb. 20, 2013), https://www.ftc.gov/enforcement/cases-proceedings/102-3116/compete-inc; *Craig Brittain*, Decision and Order, F.T.C. Docket No. C-4564 (Dec. 28, 2015), https://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter.

236 2015 Administration CPBR Discussion Draft § 4(a)(1).

237 *See, e.g.*, DPPA, 18 U.S.C. § 2725(3)-(4); COPPA, 15 U.S.C. § 6501(8); COPPA Rule, 16 CFR § 312.2; GLBA, 15 U.S.C. § 6809(4); 12 CFR § 1022.3(g) (FCRA regulations); California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22577(a); California Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code § 22947.1(k); Cal. Civ. Code § 1798.82(h); Conn. Gen. Stat. Ann. § 36a-701b(a); N.Y. Gen. Bus. Law §§ 899-aa(1)(a), (b); La. Stat. Ann. § 51:3073(4); Fla. Stat. § 501.171(1)(g).

238 OTI asks us to clarify the meaning of "other online contact information." OTI Comments at 22. The term is meant to be technology neutral and encompass other methods of BIAS-enabled direct messaging. *See also*16 CFR § 312.2 (defining "online contact information" for the COPPA Rule).

239 *See* Audience Partners Comment at 11-13 ("IP addresses are incapable of identifying an individual without being linked to additional information"); Direct Marketing Association (DMA) Comments at 17 (information "that does not, on its own, identify a specific individual" should not qualify as PII); IAB Comments at 10 (an "anonymous identifier" should not qualify as PII); NCTA Comments at 22 (MAC addresses and IP addresses cannot identify an individual on their own); Front Porch Comments at 2-3 (IP addresses should not qualify as PII because while they "might be issued to a subscriber for a period of time, a personal IP address can also change at any time, and therefore, is not reliable.").

240 *See supra* paras. 67-71.

241 In many cases, a unique numerical identifier will be *more* specific than the person's actual name. *See, e.g.*, Mona Chalabi and Andrew Flowers, *Dear Mona, What's the Most Common Name in America?*, FiveThirtyEight (Nov. 20, 2014), http://fivethirtyeight.com/features/whats-the-most-common-name-in-america/ (discussing the large number of people with common names such as James Smith or Maria Garcia).

242 *See* CDT Comments at 13-14, 16 (discussing how MAC addresses and IP addresses in protocol headers, as well as other traffic statistics, can be shared with BIAS providers, allowing the provider to link them to the subscriber); Feamster Edge Provider Comments at 2 (BIAS providers can "link information about IP addresses seen in network traffic traces to CPNI from its subscribers"). In situations where the BIAS provider sold or leased a device to a customer—such as a smartphone, modem, or router—the provider could associate device identifiers with the customer from its records. *See* Sandvine Comments at 22 ("In some domains a device is fairly synonymous with a person (e.g., mobile phone).").

243 *CIA v. Sims*, 471 U.S. 159, 178 (1985) (internal quotation marks, alterations, and citation omitted); *see also U.S. v. Maynard*, 615 F.3d 544, 561-63 (D.C. Cir. 2010), *aff'd on other grounds sub nom.*, *United States v. Jones*, 132 S.Ct. 945 (2012) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what person does repeatedly, what he does not do, and what he does ensemble."); 2016 FTC Big Data Report at 3-5 (discussing the "Life Cycle of Big Data"). *See also* Access Now Comments at 5 ("[S]eemingly anonymous information can often—and easily—be re-associated with identified individuals.").

244 FTC Staff Comments at 11.

245 47 U.S.C. § 222(h)(3).

246 S. Conf. Rep. No. 104-230 at 205 (1996) ("The subscriber list information provision guarantees independent publishers access to subscriber list information at reasonable and nondiscriminatory rates, terms and conditions from any provider of local telephone service."). In an earlier report, the Senate stated, "This provision is intended to assure that persons who utilize subscriber information, including publishers of telephone directories unaffiliated with local exchange carriers, are able to purchase published or to-be-published subscriber listings and updates from carriers on reasonable terms and conditions."S. Rep. No. 103-367 at 97 (1994). *See also*47 U.S.C. § 222(e) (requiring carriers providing telephone exchange service to make subscriber list information available to directory publishers on nondiscriminatory and reasonable terms).

247 H.R. Rep. No. 104-204 at 91 (1995).

248 S. Rep. No. 103-367 at 97 (1994).

249 *See* T-Mobile Comments at 21-22 ("[B]roadband providers do not publish directories of customer information today."). Section 222(e) likewise recognizes that subscriber list information is the publication of directories in the context of telephone exchange service. *See*47 U.S.C. § 222(e) ("Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.").

250 *See, e.g.*, T-Mobile Comments at 22 (stating that providers "may" publish directories in the future, but not identifying any concrete plans to do so).

251 *Cf.* S. Rep. No. 103-367 at 97 (1994) (when subscribers "declin[e] the opportunity to limit [subscriber list information's] disclosure" they "have little expectation of privacy" in it). *See also* Greenlining Institute Comments at 50 ("the 'subscriber list' exception to CPNI applies narrowly, relates only to listing information exchanged between those actually in the business of publishing directories and actually used for that purpose").

252 *See, e.g.*, Greenlining Institute Comments at 45-46 (supporting this conclusion); S^2ERC Comments at 8 (same).

253 *See* T-Mobile Comments at 21-22; ICC Comments at 13-14 (arguing that IP addresses are analogous to subscriber list information and that names and addresses are "widely available"); DMA Comments at 13-14 (seeking "exemptions based on comparisons of" subscriber list information and certain types of information in the BIAS context); NTCA Comments at 29-30 (arguing that customer names, addresses, and telephone numbers should not be protected by these rules).

254 *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14487, para. 146-47 (1999) (*1999 CPNI Reconsideration Order*) (adopting the conclusions of the Common Carrier Bureau in the *1998 CPNI Clarification Order*); *1998 CPNI Clarification Order*, 13 FCC Rcd at 12395-96, paras. 8-9 (finding that names, addresses, and telephone numbers are not CPNI).

255 As PII, this information is subject to our customer choice rules, discussed in detail below. *See infra* Part III.D. Our customer choice rules will continue to allow this information to be used to publish publicly available telephone directories, consistent with the current practice of allowing customers to keep their information unlisted.

256 *See* ACA Comments at 57-58; WTA & Nex-Tech Apr. 25 *Ex Parte* at 1 (urging Commission to "harmonize definitions, procedures and requirements in order to reduce the complexity of regulation of privacy and minimize the burdens on small providers").

257 *TerraCom NAL*, 29 FCC Rcd at 13330-31, paras. 14, 16.

258 *See* 2012 FTC Privacy Report at 55-56 (expressing concern regarding the potential for ISPs to use content for purposes other than providing service); FTC Staff Comments at 20-21 (supporting privacy protection for content); *accord* ACLU Comments at 7-8; AAJ

Comments at 9; EFF Comments at 5; EPIC Comments at 26; OTI Comments at 23; Public Knowledge White Paper at 59. *See also infra* Part III.D.1.a.(i).

259 *See* Public Knowledge White Paper at 48 (arguing that BIAS providers can view unencrypted payloads); CDT Comments at 17 ("BIAS subscribers sending and receiving unencrypted transmissions are no less deserving of privacy protections than subscribers who only visit sites supporting HTTPS or who employ proxy or VPN services."). BIAS providers' inability to access encrypted content is irrelevant; what matters is the information the BIAS providers *can* access. Moreover, even when traffic is encrypted, some content may remain visible or inferable to the provider. *See infra* para. 180.

260 FTC Staff Comments at 20.

261 *See, e.g.*, An Act to Regulate Radio Communications, ch. 287, § 4, Reg. 19, 37 Stat. 302, 307 (1912); Radio Act of 1927, ch. 169, § 27, 44 Stat. 1162, 1172; Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1103-04; 47 U.S.C. § 605; 18 U.S.C. §§ 2510-2522; 18 U.S.C. §§ 2701-2712; 18 U.S.C. §§ 3121-3127.

262 ACLU Comments at 7; *see also* OTI Comments at 23 ("Recognizing packet contents as communications contents, and establishing an opt-in standard for content, would honor BIAS customers' reasonable expectation that their provider is not inspecting their traffic for purposes other than to provide service.").

263 *See*18 U.S.C. § 2510(8) ("—[C]ontents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."); 47 U.S.C. § 605(a) (restricting the disclosure of "the existence, contents, substance, purport, effect, or meaning" of a communication by wire or radio). *See also* OTI Comments at 23 (quoting Section 705 and supporting content protections).

264 *See* Mozilla Comments at 4 ("Usage patterns and metadata can be as revealing, or in some ways even more revealing, than content."); CDT Comments at 16 ("Such detailed information about a customer's communications may reveal more than just patterns of broadband usage; but also clues as to the content of those communications and the behaviors and interests of that customer."). *See also, e.g.*, *Riley v. California*, 134 S.Ct. 2473, 2490 (2014) (Cell phones carry "a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate."); *United States v. Maynard*, 615 F.3d 544, 561-63 (D.C. Cir. 2010), *aff'd on other grounds sub nom.*, *United States v. Jones*, 132 S.Ct. 945 (2012) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble.").

265 *See supra* Part III.B.3.b. Because we conclude that Section 222(a) protects content as its own category of customer PI, we need not determine which types of content are also CPNI or PII.

266 *See supra* Part III.B.3.a(i)(a).

267 *See* EPIC Comments at 26 (quoting Tim Berners-Lee) ("The access by an ISP of information within an internet packet, other than that information used for routing, is equivalent to wiretapping a phone or opening sealed postal mail."); OTI Comments at 23 ("Recognizing packet contents as communications contents, and establishing an opt-in standard for content, would honor BIAS customers' reasonable expectation that their provider is not inspecting their traffic for purposes other than to provide service.").

268 *See supra* Part III.B.3.a(i)(a).

269 *See* Public Knowledge White Paper at 48 ("As revealing as the packet headers may be, the payloads potentially reveal far more information.").

270 BIAS providers' use of application payloads for network management is also one reason why BIAS content is not wholly equivalent to telephone conversations. Voice carriers do not scan a phone conversation to secure the network or reduce congestion. Application payloads in the broadband Internet context are far more sophisticated and complex than mere audio transmissions over a telephone line. *See* Public Knowledge White Paper at 59.

271 *See* Free Press Reply at 12 (arguing that BIAS providers can infer a significant amount about content by examining other elements of the packet).

272 *See supra* para. 76; *see also* EPIC Comments at 26 (quoting Tim Berners-Lee) ("The URLs which people use reveal a huge amount about their lives, loves, hates, and fears. This is extremely sensitive material."); Andrew G. West & Adam J. Aviv, On the Privacy Concerns of URL Query Strings, 2014 Proc. of the 8th Workshop on Web 2.0 Sec. and Privacy, available at http://w2spconf.com/2014/papers/privacy_query_strings.pdf; (Reisman and Narayanan June 17, 2016 *Ex Parte* at 22-24 (observing that customer names and other PII are included in some URLs).

273 *See supra* para. 78; *Riley v. California*, 134 S.Ct. at 2490 (The applications a person uses "can form a revealing montage of the user's life.").

274 FTC Staff Comments at 20. *See also Riley v. California*, 134 S.Ct. at 2490 ("An Internet search and browsing history ... could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

275 47 U.S.C. § 605(a).

276 18 U.S.C. §§ 2510-2522.

277 47 U.S.C. §§ 1001-1010.

278 *See, e.g.*, Electronic Transactions Association Comments at 11; USTelecom Comments at 34; NCTA Comments at 96.

279 *See* ACLU Comments at 7-8 ("All of the reasons why Congress charged the Commission with protecting customer information 'that relates to the quantity ... type, destination, location, and amount of use of a telecommunications service' without doubt apply to content as well. The Commission should make this clear despite existing laws that have some bearing on the legality of content monitoring by BIAS providers."); *see also* EFF Comments at 2-3.

280 Similarly, for example, both the Children's Online Privacy Protection Act and the Video Privacy Protection Act may protect videos that young children watch online. *See*18 U.S.C. § 2710; 15 U.S.C. § 6502.

281 CTIA Comments at 64 ("Additionally, the *data types* protected by Section 705—the 'existence, contents, substance, purport, effect, or meaning' of a communication—bear scant resemblance to many of the elements of 'customer proprietary information' that the Proposed Rules seek to cover—*e.g.*, device identifiers, IP addresses, and so forth. These incongruities demonstrate that Section 705 does not provide authority for the Proposed Rules.") (emphasis in original).

282 Letter from 38 Public Interest Organizations to the Honorable Tom Wheeler, Chairman, FCC at 2 (Sept. 7, 2016) (https://www.fcc.gov/ecfs/filing/10907040663545). *See also* CDD Comments at 17; EPIC Comments at 21-23; OTI Comments at 21-22; Privacy Rights Clearinghouse Comments at 5.

283 The FTC approach has broad support in the record. *See, e.g.*, AT&T Reply at 36; Access Now Comments at 11; Audience Partners Comments at 17; CTIA Comments at 38; Email Sender & Provider Coalition Comments at 7-8; ICC Comments at 12; ITIF Comments at 19; Sprint Reply at 3-4; T-Mobile Comments at 35.

284 2015 Administration CPBR Discussion Draft at § 4(a)(2)(A).

285 As discussed in greater detail below, this third part of the test applies to entities with which the provider contracts to share de-identified customer information. It does not apply to the general disclosure or publication of highly aggregated summary statistics that cannot be disaggregated—for example, the use of statistics in advertisements (e.g., "We offer great coverage in rural areas, because that is where 70% of our customers live."); *see also* AT&T Comments at 70-71. *See infra* Part III.B.4.a(iii).

286 The record does not demonstrate a need to treat de-identified information differently in the voice context versus the BIAS context. We agree with the Greenlining Institute and other commenters that a uniform regime, "is easier for the carriers, easier [for] enforcement, and easier for customers to understand[.]" Greenlining Institute Comments at 16. *See also* ACA Comments at 57-58 (supporting harmonization of Section 222 rules).

287 *See* Privacy Rights Clearinghouse Comments at 5; OTI Comments at 6, 21-22 (stating that a recent study found that supposedly de-identified datasets from medical records, search queries, social network data, genetic information, geo-location data, and taxi-cab

history could all be used to specifically identify individuals); *accord* CDD Comments at 17; EFF Comments 14; EPIC Comments at 22; OTI Reply at 12-13; Public Knowledge White Paper at 49-50. *See also, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); U.S. Public Policy Council of the Association for Computing Machinery, *Response to Request for Information, Big Data Review*, 79 FR 12251 at 2, https://usacm.acm.org/images/documents/BigDataOSTPfinal.pdf. In 2000, Latanya Sweeney, now the Director of the Data Privacy Lab in the Institute for Quantitative Social Science at Harvard University, demonstrated that 87 percent of the population in the United States had reported characteristics that likely made them unique based only on 5-digit ZIP, gender, and date of birth. Latanya Sweeney, Abstract, *Uniqueness of Simple Demographics in the U.S. Population* (Carnegie Mellon Univ., Lab. For Int'l Data Privacy 2000), https://dataprivacylab.org/projects/identifiability/index.html. In 2008, researchers at the University of Texas at Austin succeeded in using publicly available information to identify Netflix subscribers in a dataset of movie ratings from which personal identifiers had been removed, explaining that "[r]emoving identifying information is not sufficient for anonymity." Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets, in Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 111, 118 (2008), https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

288 2014 Administration Big Data Report at 8.

289 EPIC Comments at 22.

290 2012 FTC Privacy Report at 20.

291 *See id.*; CDD Comments at 20; EPIC Comments at 22-23.

292 *See* Privacy Rights Clearinghouse Comments at 5.

293 *See, e.g.*, IMS Health Comments at 15.

294 47 U.S.C. § 222(h)(2) ("The term 'aggregate customer information' means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.").

295 *See, e.g.*, AT&T Reply at 36-39; CTIA Comments at 36-37; CenturyLink Comments at 17; Comcast Reply at 47-48; Sprint Reply at 3-4; T-Mobile Comments at 34-35; Verizon Comments at 44.

296 *See* 2012 FTC Privacy Report at 21; *see also* 2015 Administration CPBR Discussion Draft at Sec. 4(a)(2)(A); Access Now Comments at 11; CDT Comments at 9-10; EFF Comments at 14; EPIC Comments at 21-23; FTC Staff Comments at 9; Public Knowledge Comments at 28.

297 *See supra* Part III.B.3.c.

298 *See* 2012 FTC Privacy Report at 21-22; NTCA Comments at 57; *see also supra* note 283. *See also* 2015 Administration CPBR Discussion Draft at Sec. (4)(a)(2)(A) (defining "de-identified data" and requiring that it be "alter[ed] such that there is a reasonable basis for expecting that the data could not be linked as a practical matter to a specific individual or device"). *See also supra* para. 89.

299 *See supra* Part III.B.3.c.

300 *See supra* note 287.

301 *See, e.g.*, AT&T Reply at 38 n.102; EFF Comments at 14 ("the field of reidentification is constantly advancing, and any [pre-set list of identifiers] would quickly become obsolete"); NTCA Comments at 57; S^2ERC Comments at 14 (agreeing that "the categories of what can potentially be reasonably linkable information will continue to evolve").

302 AT&T Reply at 38.

303 *Cf. id.* at 36 (claiming that the FTC framework adopted a commercial reasonableness standard); CTIA Comments at 43 (CPNI is de-identified if the provider uses "commercially reasonable techniques").

304 *See supra* para. 1.

305 *See* EPIC Comments at 21-22 ("Because not all de-identification techniques adequately anonymize data, it is important that the process employed is robust, scalable, transparent, and shown to provably prevent the identification of consumer information."); *see also supra* note 287.

306 2012 FTC Privacy Report at 21.

307 *See* 2012 FTC Privacy Report at 22 n.113. *See, e.g.*, WTA & Nex-Tech Apr. 25, 2016 *Ex Parte* at 1-2 (data retention mandates are burdensome for small providers).

308 *See* Verizon Reply at 23-24 ("[P]roviders should be allowed to use and disclose de-identified data as long as the provider—and anyone it shares the data with—honors a consumer's choices prior to using that data in a way that would target the customer.").

309 Verizon Comments at 44; *see also id.* at 44-45.

310 *See* AT&T Comments at 69; Audience Partners Comments at 10-11, 14-17; NCTA Comments at 67; NTCA Comments at 56.

311 FTC Staff Comments at 10. *Accord* EFF Comments at 5; EPIC Comments at 18-19 (discussing how persistent identifiers like device information can be used to map out an individual's interactions); Software & Info. Indus. Ass'n Comments at 12 (supporting the FTC's test for linkability to a "consumer, computer, or device").

312 Digital Advertising Alliance, Application of Self-Regulatory Principles to the Mobile Environment at 6 (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf (defining "De-Identification Process").

313 *See supra* paras. 67-71.

314 *See* NCTA Oct. 20, 2016 *Ex Parte* at 12.

315 NCTA expresses concern that finding that IP addresses can constitute PII will undermine judicial precedent under the Video Privacy Protection Act. NCTA Oct. 20, 2016 *Ex Parte* at 11. As noted, we are not making categorical findings, but rather are looking to the "reasonably linkable" standard in finding whether information constitutes PII. We also observe that we are confronted with interpreting Section 222 of the Communications Act and its requirements concerning the protection of "proprietary information of, and relating to, ... customers." This is distinct from the language of the VPPA, which more specifically defines PII as "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."18 U.S.C. § 2710(a)(3). Accordingly, a Commission finding that certain information is or is not PII for purposes of Section 222 of the Communications Act does not answer the question of whether or not a court should consider that information to be PII under the VPPA or any other statutory provision.

316 2012 FTC Privacy Report at 22.

317 *See supra* para. 8; *infra* Part III.C.

318 *See* NTCA Comments at 57; IMS Health Comments at 16; S^2ERC Comments at 13-14; Paul Vixie Comments at 21 ("Public commitments are mere theater. Commission investigations with sanctions against violators would speak far more loudly and far more credibly than the most earnest of BIAS provider 'pinkie promises' to be good.").

319 *See* 2012 FTC Privacy Report at 21-22.

320 *See supra* note 283.

321 *See* 2015 Administration CPBR Discussion Draft at Sec. 4(a)(2)(A)(ii). *See also* 2014 Administration Big Data Report at 8 ("In practice, data collected and de-identified is protected in this form by companies' commitments to not re-identify the data[.]").

322 Executive Office of the President, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy at 22 (2012) (2012 White House Privacy Blueprint), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

323 *See* Audience Partners Comments at 17-18 (arguing that providers should be able to satisfy this part of the test with a statement in their privacy policies); WTA Comments at 24-25 (supporting a privacy policy statement and observing that such a requirement would align with the FTC's unfair and deceptive practices guidance).

324 Digital Advertising Alliance, Application of Self-Regulatory Principles to the Mobile Environment at 6 (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf ("An entity should take reasonable steps to protect the non-identifiable nature of data if it is distributed to non-Affiliates and obtain satisfactory written assurance that such entities will not attempt to reconstruct the data in a way such that an individual may be re-identified and will use or disclose the de-identified data only for uses as specified by the entity."). The DAA guidance also requires that these commitments from recipients of the data be passed along to any further downstream recipients as well, which we support. *Id.*

325 AT&T, Privacy FAQ, http://about.att.com/sites/privacy_policy/terms#aggregate (last visited Oct. 5, 2016) (under the heading "Do you provide companies with individual anonymous data as part of your External Marketing & Analytics Program?").

326 *See supra* note 287; *see also* FTC Staff Comments at 9.

327 Verizon Reply at 23-24. *See also* Audience Partners Comments at 18-19; IMS Health Comments at 16; NTCA Comments at 57.

328 Verizon Comments at 44 ("Providers should exercise reasonable monitoring to ensure these contracts are not violated."); *see also* Sprint Reply at 4 (carriers should take "appropriate safeguards [to] mitigate privacy risks" associated with de-identified data); AT&T Reply at 38 ("ISPs should of course take reasonable safeguards to keep de-identified data from re-identification.").

329 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2556, para. 162. *See also* NTCA Comments at 57 (fourth prong is unnecessary); *accord* Audience Partners Comments at 18-19; IMS Health Comments at 17; Cincinnati Bell Comments at 14-15.

330 *See* 2012 FTC Privacy Report at 21 (arguing that companies sharing customer information should "exercise reasonable oversight to monitor compliance with these contractual provisions and take appropriate steps to address contractual violations"); Lehr et al. Comments at 6; CDT Reply at 13-14. *See also*47 U.S.C. § 217 ("In construing and enforcing the provisions of this chapter, the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that person.").

331 AT&T Comments at 70-71.

332 *Id.* at 70; *see also* IMS Health Comments at 16-17.

333 Reisman and Narayanan June 17, 2016 *Ex Parte* at 48, https://www.fcc.gov/ecfs/filing/60002158273/document/60002354966

334 *See* EFF Comments at 15-16; Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) Comments at 5; Feamster July 13, 2016 *Ex Parte*.

335 Since telecommunications carriers must be able to provide secure networks to their customers, we include security research within the scope of research allowed under this limitation. Security research also falls under the exception covered in Part III.D.2.b, *infra*, regarding uses of customer PI to protect the rights and property of a carrier, or to protect users from fraud, abuse, or unlawful use of the networks.

336 *See infra* Part III.D.2.a.

337 We accordingly need not resolve the longstanding debate in the broader privacy literature concerning the circumstances under which data may be said to be reasonably de-identified, including the specific debate in the record concerning the appropriate role of aggregation. *See generally, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); Future of Privacy Forum Comments.

338 Letter from 38 Public Interest Organizations to the Honorable Tom Wheeler, Chairman, FCC at 1 (Sept. 7, 2016) (https://www.fcc.gov/ecfs/filing/10907040663545).

339 Letter from Paul Ohm, Professor of Law, Georgetown University Law Center, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed July 28, 2016) (Paul Ohm July 28, 2016 *Ex Parte*).

340 Latanya Sweeney, *Only You, Your Doctor, and Many Others May Know*, JOTS — Technology Science (Sept. 29, 2015), http://techscience.org/a/2015092903/ ("Policy should adopt best practices, which improve over time as privacy technology and the science of data privacy advances. Society can learn from cycles of published re-identifications, because the knowledge of vulnerabilities will rapidly lead to improved techno-policy protections. It is an evolutionary cycle. First, a re-identification vulnerability becomes known, which leads to improved practices and technical solutions, which in turn leads to other re-identifications, and so on, until eventually we achieve robust technical, policy, or administrative solutions.").

341 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2527, para. 82; *see also* 2012 FTC Privacy Report at 61-64; Letter from Matthew M. Polka, President & CEO, American Cable Association, et al., to the Honorable Tom Wheeler, Chairman, FCC (March 1, 2016) (on file with WCB) (Industry Framework); New America's Open Technology Institute, The FCC's Role in Protecting Online Privacy 7 (2016) (OTI White Paper); Letter from Marc Rotenberg, Executive Director, EPIC, et al., to Tom Wheeler, Chairman, FCC, at 3 (Jan. 20, 2016); Letter from Jason Kint, Digital Content Next, to Tom Wheeler, Chairman, FCC, at 3-4 (Feb. 26, 2016).

342 *See*47 U.S.C. §§ 551(a), 338(i)(1) (directing cable providers and satellite carriers, respectively, to "clearly and conspicuously" notify their subscribers of data collection and disclosure practices).

343 *See 2015 Open Internet Order*, 30 FCC Rcd at 5669, para. 154 (citing Howard Beales, Richard Craswell & Steven C. Salop, *The Efficient Regulation of Consumer Information*, 24 J. L. & Econ. 491 at 513 (1981); Howard Beales, Richard Craswell & Steven C. Salop, *Information Remedies for Consumer Protection*, 71 Am. Econ. Rev. 410 at 411 (Papers & Proceedings, May 1981); Alissa Cooper, *How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and United Kingdom*, at Section 2.4.3 (Sept. 2013)).

344 *See infra* note 354.

345 47 CFR §§ 64.2001-64.2011.

346 *See 2010 Open Internet Order*, 25 FCC Rcd at 17939, para. 56; *2015 Open Internet Order*, 30 FCC Rcd at 5673, para. 164.

347 We observe in particular that notice is fundamental to the FTC's privacy regime, acting as a basis for its implementation of FIPPs and forming required components of their enforcement proceedings. *See* 2012 FTC Privacy Report; Facebook, Inc., Decision and Order, F.T.C. File No. 092-3184 (2012), https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc (Facebook Consent Order); Google, Inc., Decision and Order, F.T.C. File No. 102-3136 (2011), https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter (Google Consent Order).

348 *See, e.g.*, Comcast Comments at 16-17, 22 ("[C]ompanies must provide consumers with understandable privacy notices ... [and] should make an effort to educate consumers about their data privacy practices."); CTIA Comments at 103; Hughes Network Systems (Hughes) Comments at 3; Industry Framework at 5 (arguing that carriers should provide notices "describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share that CPNI with third parties"); INCOMPAS Comments at 9 (supporting FIPPs of transparency, choice, and security); Consumer Action Comments at 2 ("Consumers deserve to know what information is being collected about them, how it's being used and why it will be shared with other entities."); EPIC Reply at 3 (asserting that FCC should ensure fair information practices); CDT Comments at 6-7; Mozilla Comments at 6 ("Our users and our community have told us — through surveys, comments and emails — that transparency and control matter to them. They want to know what is happening with their data; they want to control what data is shared, understand how their data is used and what they get for that exchange."); Aleecia M. McDonald (McDonald) Reply at 1 ("Even the most minimal set of FIPPs include notice, choice, access, integrity, and enforcement.").

349 Moreover, the record reflects that many BIAS providers and other telecommunications carriers already provide thorough notice of their privacy practices. *See infra* note 360.

350 *See* EPIC Comments at 6; CDD Comments at 17; Behavioral Economics Consulting Group Comments at 3 ("In many cases, disclosure has no effect on behavior ... Research has shown that transparency is only effective in preventing deception when the information shared is *meaningful* and *comprehensible to the recipient*.").

351 2014 Administration Big Data Report at 55 ("For the vast majority of today's ordinary interactions between consumers and first parties, the notice and consent framework adequately safeguards privacy protections."); *id.* at 61 ("While notice and consent remains fundamental in many contexts, it is now necessary to examine whether a greater focus on how data is used and reused would be a more productive basis for managing privacy rights in a big data environment.").

352 2014 Administration Big Data Report at 54 ("[F]ocusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."); *see also* Technology Policy Institute (TPI) Comments, Attach., Thomas Lenard and Scott Wallsten White Paper, An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking at 24 (Lenard and Wallsten White Paper) (citing 2014 Administration Big Data report in criticizing notice and consent); SIIA Comments at 8-9 (same).

353 We will consider information to be misleading if it includes material misrepresentations or omissions.

354 *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8117-18, para. 73 (1998) (*1998 CPNI Order*); *see also, e.g.*, ViaSat Comments at 3 (stating that "transparency is critical for 'consumers to make informed choices' regarding the collection and use of customer information"); California Attorney Gen. (California AG) Reply at 4 ("Consumers can only exercise privacy choices when they are aware of them and understand their implications."); U.S. Dep't of Health, Educ. And Welfare, Sec'y's Advisory Comm. on Automated Data Systems., Records, Computers, and the Rights of Citizens 41 (1973) (HEW Report) ("There must be a way for an individual, to find out what information about him is in a record and how it is used."); FTC, Privacy Online: A Report to Congress (1998) ("[D]ata collectors must disclose their information practices before collecting personal information from consumers").

355 *See, e.g.*, Privacy Rights Clearinghouse Comments at 3 ("BIAS providers' data practices are largely invisible to customers and data is becoming increasingly valuable and easy to collect, store, and share. This highlights the need for clear, conspicuous, and easy-to-understand privacy notices.").

356 FTC Staff Comments at 12.

357 *Id.* (explaining that privacy advocates, regulators, the press, consumers, and others will have access to information about how companies collect, use, and share data).

358 *See 1998 CPNI Order*, 13 FCC Rcd at 8161, para. 135.

359 Comcast Comments at 22 ("Each ISP should provide notice to its customers that describes the CPNI that it collects."); EPIC Comments at 9-10 (asserting that notices "must include ... the type of data collected about consumers").

360 *See* CTIA Comments at 98 ("ISPs already publish privacy policies, providing their customers with significant information about their data practices, including a description of the type of information they collect, how they use it, with whom (and under what circumstances) they share it, and so forth."); T-Mobile Comments at 39; Hughes Comments at 3; AT&T Comments at 48-49 ("ISP privacy policies clearly set forth what information ISPs collect and how it is used."); Verizon Comments at 6 ("Verizon informs customers about what information it collects and gives consumers choices about how their data may be used.").

361 In particular, we eliminate a number of specific requirements for voice providers' notices regarding customers' CPNI. *See infra* Part III.C.5.

362 *See* CDD Comments at 20; OTI Comments at 33; T-Mobile Comments at 39; CTIA Comments at 98; AT&T Comments at 48-49; Verizon Comments at 6.

363 *See* CTIA Comments at 105-06.

364 *See* EFF Comments at 12-13; EPIC Comments at 9-10; OTI Comments at 33; CTIA Comments at 98.

365 47 CFR § 64.2008(c)(2) (requiring telecommunications carriers to describe the "specific entities" to which CPNI will be disclosed).

366 16 CFR § 313.6(c)(3).

367 *Id.* (listing "illustrative examples" of financial service providers as "mortgage bankers, securities broker-dealers, and insurance agents" and ""non-financial companies" as "retailers, magazine publishers, airlines, and direct marketer.").

368 *See, e.g.*, FTC Staff Comments at 11-12 (supporting disclosure of categories of entities); CTIA Comments at 103 ("ISPs should be able to report general categories of data-sharing partners, rather than listing each and every affiliate, vendor, or contractor with whom the ISP works."). Because we harmonize these rules across BIAS and other telecommunications services, we eliminate the requirement that telecommunications services specify the "specific entities" that receive customer information in their notices of privacy policies accompanying solicitations for customer approval. 47 CFR § 64.2008(c)(2) ("the notification must specify the ... specific entities that will receive the CPNI ...").

369 *See, e.g.*, OTI Comments at 33; EFF Comments at 12-13; EPIC Comments at 9-10.

370 *See* CTIA Comments at 105 ("ISPs may enter into agreements with third-party agents, independent contractors, and other entities for a variety of different purposes, ranging from one-off transactions to repeat interactions."); NTCA Comments at 39-40 ("[T]his would create an administrative nightmare and hamstring a provider's ability to create arrangements in 'real market time' with third parties ... Moreover, this requirement could be triggered if a third party undergoes an internal corporate restructuring, and then foists upon the provider a liability whose cause of action rests solely within the domain of the restructured third-party.").

371 *See* EFF Comments at 12-13 (disclosure of specific entities can encourage customers to opt in to sharing when they trust particular third parties); *see also* CDD Comments at 17 (stating that providers "should be able to be both candid and succinct" and should be able to "test layout and design factors to ensure their privacy policies are actually in view (as the industry is able to do with 'viewability' of digital ads").

372 *See* CDD Comments at 19; T-Mobile Comments at 39 (describing existing layered approach to privacy notices); WISPA Comments at 16 (asserting that "a layered privacy policy notice ... should be considered" as a voluntary safe harbor).

373 This mechanism is described below in Part III.D.4.

374 *See, e.g.*, OTI Comments at 33-34, 36; Online Trust Alliance Comments at 2.

375 *See* Lauren Willis (Willis) Reply at 7 (citing Idris Adjerid, et al., *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency*, Symposium on Usable Privacy & Security (2013)).

376 *See infra* Part III.D.4.

377 *See, e.g.*, NTCA Comments at 36-38; CTIA Comments at 104-05.

378 *See, e.g.*, Lee Rainie and Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center, December 2015, http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf; Joseph Turow, et al., *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, Univ. of Penn. Annenberg School of Comm'n (June 2015), available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf; Joseph Turow, et al., *Americans Reject Tailored Advertising and Three Activities that Enable it* (September 29, 2009); available at SSRN: http://ssrn.com/abstract=1478214; *see also* CDD Comments at 5 (citing consumer belief that they lack control over their data); Free Press Reply at 25-26; CDD Reply at 2.

379 *See infra* Part III.G.1. As noted below, this provision does not mean that carriers categorically cannot engage in financial incentive practices. *See infra* Part III.G.2.

380 47 CFR § 64.2008(c)(3).

381 *See, e.g.*, California AG Reply at 3 (asserting "the choices offered to individuals [are often] illusory, frequently amounting to 'take it or leave it' or 'all or nothing'").

382 *See infra* Part III.C.3.

383 NTCA Comments at 37-38 (footnote omitted).

384 OTI Comments at 40.

385 As the FTC has done in its groundbreaking work in this area, the FCC will be vocal in support of customer privacy interests that a carrier's bankruptcy may raise. *See, e.g.*, Letter from Jessica L. Rich, Director, FTC's Bureau of Consumer Protection to Elise Frejka, Esq. (May 16, 2015), *available at* https://www.ftc.gov/public-statements/2015/05/letter-jessica-rich-director-bureau-consumer-protection-bankruptcy-court (letter to bankruptcy court-appointed Consumer Privacy Ombudsperson expressing concern about possible sale of certain PII and suggesting conditions to protect customer privacy); *FTC v. Toysmart*, No. 00-11341-RGS (D. Mass. 2000), *available at* https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc (consent order relating to sale in bankruptcy of children's information, including shopping preferences).

386 *See* Comcast Comments at 44 (noting potential fatigue with repeated notices); CTIA Comments at 101-102 (recommending against periodic notices); NCTA Reply at 53 (arguing the most relevant time for notice is at point of sale).

387 *See, e.g.*, FTC Staff Comments at 24-25 (stating that customers should receive choice solicitations at "most relevant time," which is when they "sign up for service"); CDD Comments at 20 ("[P]rivacy decisions should be at or near the point of sale."); Sprint Comments at 12 (stating that notices may be most effective at the outset of the provider-customer relationship); Comcast Reply at 12 (citing FTC Staff Comments at 24); *cf., e.g.*, Privacy Rights Clearinghouse Comments at 4 (citing Consumer Fin. Prot. Bureau, *CFPB Finalizes Rule to Promote More Effective Privacy Disclosures*, October 20, 2014, http://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-rule-to-promote-more-effective-privacy-disclosures/) (stating that frequency of notice presentation irrelevant as long as other standards are met); USTelecom Comments at 12 (citations omitted) (approving of a single initial notice).

388 FTC Staff Comments at 24-25.

389 CDD Comments at 20; Sprint Comments at 12.

390 *See 2010 Open Internet Order*, 25 FCC Rcd at 17939-40, paras. 56-57; *see also FCC Enforcement Bureau and Office of General Counsel Advisory Guidance for Compliance with Open Internet Transparency Rule*, Public Notice, 26 FCC Rcd 9411, 9413-14 (2011) (*2011 Open Internet Transparency Guidance*).

391 CTIA Comments at 143; *see also* NTCA Comments at 52-53.

392 *See* Cincinnati Bell Comments at 12-13; Lenard and Wallsten White Paper at 18; FTC Staff Comments at 13 (citing 2012 FTC Privacy Report at 61); *see also* INCOMPAS Comments at 6; NTCA Comments at 7 (citation omitted).

393 ITTA Comments at 21 (noting potential difficulty in providing notice if point of sale is over the telephone); ViaSat Comments at 3-4 (asserting that "the Commission should permit BIAS providers at the point of sale to direct consumers to such online disclosures orally or in writing—rather than, for example, requiring BIAS providers to have employees read privacy notices aloud to potential customers when signing them up for service over the phone").

394 *See, e.g.*, Hughes Comments at 3 ("Hughes provides all consumers with 24 hour access to our plain language privacy policy on our website ... Accordingly, Hughes, an early adopter of consumer privacy protections, fully supports the FCC requiring all broadband providers to provide clear, transparent privacy disclosures on their website to prospective customers and current subscribers."); OTI Comments at 40 (supporting proposal); NTCA Comments at 36-38 (supports homepages links as persistent access to notice); ViaSat Comments at 3 ("[P]rivacy disclosures should be readily available to customers through the provider's website.").

395 *2010 Open Internet Order*, 25 FCC Rcd at 17939-40, para. 57.

396 OTI Comments at 40 ("[C]onsumers generally cannot adequately account for privacy harms that result from information disclosure far in the future ... circumstances may have changed, particularly if customers can access the information BIAS providers have collected about them .... Customers may make hasty decisions in the moment simply to obtain Internet access [and] therefore appreciate the reminder that they have the opportunity to change their mind."); Hughes Comments at 5 (stating that persistent notice and choice mechanisms allow customers to re-evaluate their choices); Mozilla Comments at 7 (stating that customers should be able to easily change their minds).

397 NTCA Comments at 35-38; ViaSat Comments at 3-4 ("[T]he Commission should permit BIAS providers at the point of sale to direct consumers to such online disclosures orally or in writing—rather than, for example, requiring BIAS providers to have employees read privacy notices aloud to potential customers when signing them up for service over the phone.").

398 *See* NTCA Comments at 36 (noting the existence of mobile apps that track data usage and consumption, or enable bill payment).

399 *See* NTCA Comments at 35-36; Privacy Rights Clearinghouse Comments at 4. The notice may be provided either within the application itself or through a link in the application to a different location hosting the notice.

400 *See, e.g.*, NTCA Comments at 35-36; S^2ERC Comments at 11.

401 *See* S^2ERC Comments at 11.

402 *See* NTCA Comments at 35-36 (approving of links to privacy policies on apps that serve as mobile web interfaces).

403 *See* CDD Comments at 19 (suggesting marketing techniques can prevent customers from being overwhelmed by regular notices); OTI Comments at 34-35 (recommending annual reminders of choice options).

404 *See infra* Part III.C.4.

405 *See* Privacy Rights Clearinghouse Comments at 4; WTA Comments at 15; XO Comments at 15; Rural Wireless Association Comments at 7.

406 *See supra* note 403.

407 *See* NTCA Comments at 41; WTA Reply at 7; *see also infra* Part III.C.5.

408 *See, e.g.*, CTIA Comments at 102-03; Mobile Future Comments at 4 (citing 2012 FTC Privacy Report at 27); NCTA Comments at 85; WTA Comments at 14; ACA Reply at 14-15.

409 *See, e.g.*, Rural Wireless Association Comments at 6-7 (expressing concern "about the financial burdens that the proposed privacy notice framework will impose on small providers"); NTCA Comments at 41-42; WTA Comments at 10.

410 *See* FTC Staff Comments at 14 (citing 16 CFR § 437.3(a) ("business opportunity rule"); 16 CFR § 14.9 ("requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials")).

411 *See*47 CFR §§ 64.2001-2011; *2010 Open Internet Order*, 25 FCC Rcd at 17939, para. 56; *2015 Open Internet Order*, 30 FCC Rcd at 5673, para. 164; FTC Staff Comments at 11-15; 2012 FTC Privacy Report at 60-64.

412 *See, e.g.*, T-Mobile Comments at 41-42; Future of Privacy Forum Reply at 6.

413 T-Mobile Comments at 39 (noting T-Mobile's existing layered privacy notices); WISPA Comments at 16 (suggesting voluntary layered notices). We note that as standard business practices for conveying complex information improve, we expect notices of providers' privacy policies to keep pace.

414 *See infra* note 427.

415 Consumer Action Comments at 2 ("The provider's privacy practices should be easily available, written in a clear way and linked to a user-friendly opt-out and preference page."); Comcast Comments at 42-43 ("Two of the key tenets of the FTC's regime and Administration's Consumer Privacy Bill of Rights are transparency and choice, including making privacy practices as simple and clear as possible so that consumers can make informed decisions."); FTC Staff Comments at 11 ("FTC staff supports the proposed requirement to clearly and conspicuously disclose privacy policies."); Privacy Rights Clearinghouse Comments at 3 ("BIAS providers' data practices are largely invisible to customers .... This highlights the need for clear, conspicuous, and easy-to-understand privacy notices."); EPIC Comments at 9-10 ("Internet-based services must provide individuals in concise and easily understandable language, accurate, clear, timely, and conspicuous information about the covered entity's privacy and security practices."); CCA Reply at 34 (asserting that policies should be easily findable by customers).

416 Free Press Comments at 15 (criticizing notices presented among distractions); Greenlining Comments at 34-40 (noting examples of confusing or obscure language); Willis Reply at 7-8 (noting that firms can "sabotage" disclosures through, *inter alia*, distractions, delays between notice and ability to act, and placing disclosures at the end of lengthy processes to exhaust consumers); Willis Reply at 11-12 (detailing techniques that discourage customer action on privacy notices); OTI Comments at 34 (criticizing "endless scrolling" pages obscuring privacy notices).

417 *See* Greenlining Institute Comments at 33 ("It is unlikely that a customer reads and digests any of this information."); CDD Comments at 4 n.6 (arguing that "oblique and disingenuous" policies provider little consumer notice but shield providers from liability); OTI Comments at 34 (calling for enforcement against inadequately readable notices).

418 *Broadband Privacy NPRM*, 31 FCC Rcd at 2527-29, paras. 82, 83.

419 *See* Willis Reply at 5.

420 FTC Staff Comments at 12.

421 FTC Staff Comments at 12-13; New York Attorney General Reply at 2.

422 T-Mobile Comments at 39.

423 ADTRAN Comments at 10-11.

424 *See, e.g.*, T-Mobile Comments at 39; WISPA Comments at 16; Ghostery Apr. 29, 2016 *Ex Parte* at 18.

425 Behavioral Economics Consulting Group Comments at 3; *see also* McDonald Reply at 3 (noting misleading characterizations of targeted advertising).

426 California Attorney General Reply at 4-5; *see also* 2014 Administration Big Data Report at 56 (advocating a "no surprises" rule based upon respecting the context of a consumer's expectations of contextual use); INCOMPAS Comments at 12 (noting heightened privacy implications for provisions that would surprise customers); T-Mobile Comments at 29 (same); Mozilla Comments at 6 (advocating "no surprises" as a data principle).

427 *See, e.g.*, Snapchat Consent Decree at 3 (prohibiting Snapchat from misrepresenting the extent which Snapchat or its products or services maintain and protect the privacy, security, or confidentiality of any covered information, including but not limited to: "(1) the extent to which a message is deleted after being viewed by the recipient; (2) the extent to which respondent or its products or services are capable of detecting or notifying the sender when a recipient has captured a screenshot of, or otherwise saved, a message; (3) the categories of covered information collected; or (4) the steps taken to protect against misuse or unauthorized disclosure of covered information").

428 FTC Staff Comments at 14; Asian American and Pacific Islander Technology & Telecommunications Table (AAPI) Comments at 1.

429 *Cf.* Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials, 16 CFR § 14.9; Business Opportunity Rules, 16 CFR § 437.3(a).

430 FTC Staff Comments at 14. We note that for the purposes of this rule, ""language" also includes American Sign Language, meaning that if the customer transacts business with the carrier in American Sign Language, the notice would need to be made available in that language.

431 AAPI Comments at 1.

432 *See* CTIA Comments at 103-04; EFF Comments at 14; Lehr et al. Comments at 4.

433 FTC Staff Comments at 13-14; Hughes Comments at 3-4 (noting the CAC has a precedent for developing standard notices); WISPA Comments at 16 (approving of CAC process as a model for standardized notices); WISPA Reply at 31 (specifically recommending the CAC develop standardized privacy notices). The Committee's purpose is to make recommendations to the Commission regarding

consumer issues within the Commission's jurisdiction and to facilitate the participation of consumers in proceedings before the Commission.

434 ACA Reply at 14-15; NTCA Comments at 41-42 (supporting standardized safe harbor notice, but no mandated standard); Privacy Rights Clearinghouse Comments at 3 (recommending standardized notice); Rural Wireless Association Comments at 7; ViaSat Comments at 4; WISPA Comments at 16 (recommending standardized safe harbor if notice is required); WISPA Reply at 31; Letter from Jodi Goldberg, Associate Corporate Counsel, Hughes Network Systems, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, Attach. at 1 (filed Oct. 14, 2016) (Hughes Oct. 14, 2016 *Ex Parte*) (supporting standardized notices as a safe harbor). We note that the record is largely lacking on specific models for or details about how to format such notices.

435 FTC Staff Comments at 13; Greenlining Institute Comments at 41-42; EFF Comments at 13-14; ViaSat Comments at 2 ("[P]rivacy practices often can be a point of competitive differentiation between service providers.").

436 *See, e.g.*, ACA Comments at 49-51; CTIA Comments at 104; EFF Comments at 13-14.

437 The Committee previously developed the Open Internet broadband consumer labels, as well as developed guidelines on consumer disclosures via its Consumer Information Disclosure Task Force. *Consumer and Governmental Affairs, Wireline Competition, and Wireless Telecommunication Bureaus Approve Open Internet Broadband Consumer Labels*, GN Docket No. 14-28, Public Notice, 31 FCC Rcd 3358; FCC Consumer Advisory Committee, Recommendations Regarding Pre-Sale Consumer Disclosures (Aug. 4, 2010), at https://apps.fcc.gov/edocs_public/attachmatch/DOC-300826A1.pdf.

438 47 CFR §§ 0.291, 0.331, 0.361.

439 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2533-34, para. 96. As with our requirements for the notice of privacy policy, if a carrier does not have a website, it may provide notices of material change notices to customers in paper form or some other format agreed upon by the customer.

440 *See id.*

441 *See 2015 Open Internet Order*, 30 FCC Rcd at 5671-73, paras. 161-164; Facebook Consent Order; Google Consent Order.

442 *See, e.g.*, FTC Staff Comments at 14-15; EFF Comments at 13; Comcast Comments at 49; CTIA Comments at 122-23; T-Mobile Comments at 41; WISPA Comments at 14.

443 *See* FTC Staff Comments at 14-15; EFF Comments at 13; Comcast Comments at 49; CTIA Comments at 122-23; T-Mobile Comments at 41; WISPA Comments at 14.

444 *See, e.g.*, Online Trust Alliance Comments at 3; McDonald Reply at 3 ("Many ISPs provided limited information to users, at best informing users that terms and conditions had changed without explaining the scale and scope of privacy change. Some ISPs reportedly did not notify users at all.").

445 *2015 Open Internet Order*, 30 FCC Rcd at 5671-72, para. 161.

446 *Id.* at 5672-73, para. 164.

447 *See* CTA Comments at 11 (arguing that material change notices will result in notice fatigue).

448 The definition differs from that in the *2015 Open Internet Order* in two respects: the customer's interest is defined by the customer's decisions on privacy, and not choice of provider, service, or application; and the reference to edge providers, which are not relevant to the material changes at issue, has been removed. *See* WISPA Comments at 14.

449 *Cf.* NTCA Reply at 42-43 (submitting that push notices and billing statements, supplemented by a notice on the website, are sufficient); *contra* CenturyLink Comments at 21-22 (arguing that initial notice of privacy policies and disclosure on a website is sufficient).

450 *See* NCTA Comments at 85 (suggesting text messages as one form of notice and solicitation).

451 *But cf.* CenturyLink Comments at 21-22 (arguing that actively contacting customer required further data collection).

452 *See, e.g.*, Letter from Rebecca Murphy Thompson, EVP & General Counsel, Competitive Carriers Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed Oct. 13, 2016) (CCA Oct. 13, 2016 *Ex Parte*).

453 *2015 Open Internet Order*, 30 FCC Rcd at 5677, para. 171.

454 *Id.*

455 *See, e.g.*, CenturyLink Comments at 21-22.

456 *See generally* NTCA Comments at 40-41 (noting that many customers do not receive printed billing statements).

457 *Cf.* McDonald Reply at 3-4 (noting 11 percent of consumers in one survey who believed an opt-out notice was a scam).

458 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2533-35, paras. 96, 100; 31 FCC Rcd at 2605, Appendix A (proposed § 64.7001(c)(1)).

459 *See* FTC Staff Comments at 14-15; *see also* 2012 FTC Privacy Report at 57-58.; EFF Comments at 13; Comcast Comments at 49; CTIA Comments at 122-23; T-Mobile Comments at 41; WISPA Comments at 14. The Administration CPBR similarly notes that "previously collected personal data" calls for increased privacy controls over ongoing collection. 2015 Administration CPBR Discussion Draft, § 102(e)(2). As discussed in Part III.D.1.a(ii) below, if the material change affects previously collected information, then, consistent with FTC precedent and recommendations, the carrier must obtain opt-in consent for that new use of previously collected information.

460 *See* Charter Reply at 13-14; NTCA Comments at 47; INCOMPAS Comments at 4-5; WTA Comments at 12.

461 *See, e.g.*, NTCA Comments at 38-39; RWA Comments at 6-7; WTA Comments at 9; Letter from Catherine M. Hilke, Assistant General Counsel, Verizon, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Aug. 17, 2016).

462 *See* Letter from Catherine M. Hilke, Assistant General Counsel, Verizon, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 1 (filed Oct. 13, 2016) (Verizon Oct. 13, 2016 *Ex Parte*).

463 *See supra* note 360.

464 *See* Privacy Rights Clearinghouse Comments at 4; WTA Comments at 15; XO Comments at 15.

465 *See*47 CFR § 64.2008(c)(1).

466 *See* Letter from William H. Johnson, Senior Vice President, Federal Regulatory & Legal Affairs, Verizon, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed June 23, 2016).

467 Section 222 addresses the conditions under which carriers may "use, disclose, or provide access to" customer information. 47 U.S.C. § 222(c)(1), (c)(3), (d), (f). For simplicity throughout this document we sometimes use the terms "disclose" or "share" in place of "disclose or provide access to."

468 *See, e.g.*, 47 U.S.C. §§ 551(c), 338(i)(4) (imposing on cable operators and satellite carriers, respectively, requirements to obtain subscriber consent prior to disclosing personally identifiable information).

469 *See supra* note 341.

470 As discussed below, we do not consider a carrier's sharing of customer PI with the carrier's own agents to constitute sharing with third parties that requires either opt-in or opt-out consent. *See infra* note 623.

471 *See, e.g.*, Verizon Comments at 9 ("[H]aving to deal with different and even inconsistent privacy frameworks will inevitably lead to consumer confusion and frustration."); CTIA Comments at 96 ("The Commission likewise should use data sensitivity and flexibility as its touchstones so that its rules ... will meet consumer expectations, avoid consumer confusion, and minimize other harms associated with disparate privacy regulation across the ecosystem."); CTIA Comments at 117 (agreeing "in principle that there may be significant

advantages to harmonizing regulations to create the *right* regulatory framework for voice, broadband, and cable services—including both the delivery of an improved and simplified customer experience, and the realization of saved administrative costs."); LGBT Technology Partnership Comments at 4 ("In this regard, we encourage the Commission to adopt the FTC guidelines that protect date for all consumers and treats all companies equally thus avoiding consumer confusion and conflicting regulations."); Greenlining Institute Comments at 18 ("Commenters believe that a uniform regime is not only easier for the carriers, easier of enforcement, and easier for customers to understand, it is also consistent with the Open Internet Order in terms of law and policy."); WISPA Comments at 16 ("A combined privacy policy would provide more clarity and less confusion to customers.").

472 WTA & Nex-Tech Apr. 25, 2016 *Ex Parte* at 1 (urging the Commission to "harmonize definitions, procedures and requirements in order to reduce the complexity of regulation of privacy and minimize the burdens on small providers"); Rural Wireless Association Comments at 7 ("RWA recommends that the Commission harmonize its proposals with existing regulations regarding CPNI."); WISPA Comments at 16-17 ("A combined privacy policy ... would reduce the administrative burdens and costs of developing and maintaining separate policies, especially for small carriers that do not have sufficient resources."); WTA Comments at 3 ("[T]he Commission should make certain that its new broadband CPNI customer approval, security and notification rules correspond as much as practicable to its existing rules for voice and cable television service."); WTA Comments at 10 ("The Commission should also harmonize customer solicitation and approval requirements for voice and broadband services.").

473 We also require carriers to obtain customer opt-in consent for material retroactive uses of customer PI, as discussed below. *See infra* para. 195.

474 *Broadband Privacy NPRM*, 31 FCC Rcd at 2543-46, paras. 122-30 (proposing to require opt-out consent for uses of customer PI that were for the purpose of marketing communications-related services to customers, or for sharing information with affiliates offering communications-related services for the purpose of marketing those communications-related services to customers; and to require opt-in consent for all other purposes that require consent).

475 *Broadband Privacy NPRM*, 31 FCC Rcd at 2548-49, para. 136 (seeking comment on a sensitivity-based framework); *see infra* note 477.

476 *See* FTC Staff Comments at 21-22 (citing 2012 FTC Privacy Report at 40, n.189). The Administration's CPBR similarly proposes that individuals' control over the processing of their data be "in proportion to the privacy risk to the individual and consistent with context." 2015 Administration CPBR Discussion Draft § 102(a).

477 *See* FTC Staff Comments at 21-22; Future of Privacy Forum Comments at 26 (citing the NAI and DAA frameworks as drawing the sensitive/non-sensitive distinction); Future of Privacy Forum Reply at 8; Richard Bennett Comments at 5; ICLE Comments at 18; CompTIA Comments at 7; Internet Commerce Coalition Comments at 3; ACA Comments at 51-52; State Privacy & Security Coalition Comments at 5; CenturyLink Comments at 16, 28; Comcast Comments at 13; NCTA Comments at 3; WISPA Comments at 23; INCOMPAS Comments at 12; T-Mobile Comments at 8, 29; AT&T Comments at 1, 96-97; ANA Comments at 18; FTC Commissioner Maureen Ohlhausen (Ohlhausen) Comments at 1-2.

478 *See* National Consumers League Comments at 7 ("NCL views all information held by BIAS providers to be sensitive and thus require the same, strict data security protections."); Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed May 9, 2016) (Public Knowledge May 9, 2016 *Ex Parte*) ("[O]nly by treating all information as the most sensitive can the Commission ensure that highly sensitive information will not be compromised.").

479 *See, e.g.*, OTI Oct. 13, 2016 *Ex Parte* at 3; Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Oct. 18, 2016).

480 *See, e.g.*, Public Knowledge Comments at 24-26; Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed July 26, 2016) (Public Knowledge July 26, 2016 *Ex Parte*); Paul Ohm Reply at 10-12; National Consumers League Comments at 2.

481 *See, e.g.*, Future of Privacy Forum Reply at 8; *see also* Letter from Austin C. Schlick, Director, Communications Law, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Oct. 3, 2016) (Google Oct. 3, 2016 *Ex Parte*).

482 *See, e.g.*, *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (upholding the Commission's CPNI framework which required opt-in approval for certain uses and opt-out for others); 45 CFR §§ 164.508, 164.510 (HIPAA rule) (requiring opt-in approval for certain uses, and

allowing opt-out approval (i.e., "opportunity for the individual to agree or to object") for others); COPPA, 15 U.S.C. § 6502 (requiring opt-in consent for most uses of children's information, but permitting certain uses with disclosures).

483 *See 1998 CPNI Order*, 13 FCC Rcd at 8152, para. 118 (observing that "Section 222(c)(1) is silent on the issue of whether a customer may grant a carrier partial use or access to CPNI outside the scope of Section 222(c)(1)" and concluding that "[a] customer could grant approval for partial use, for example, by limiting the uses made of CPNI, the time period within which approval remains valid, and *the types of information that may be used*") (emphasis added).

484 *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (HIPAA); *see also* FTC Staff Comments at 21.

485 *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (GLBA); *see also* FTC Staff Comments at 21. *See also infra* note 791.

486 *See, e.g.*, FTC Staff Comments at 21.

487 *See, e.g.*, Children's Online Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998) (COPPA); Common Sense Kids Action Comments at 2-3; Letter from Ariel Fox Johnson, Senior Policy Counsel, Privacy and Consumer Affairs, Common Sense Kids Action, to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106, at 2 (filed Oct. 5, 2016) (Common Sense Kids Action Oct. 5, 2016 *Ex Parte*) ("Children's information, all of it, is sensitive. This is why the FTC's COPPA Rule protects a wide swathe of children's information—not just their social security numbers."); FTC Staff Comments at 21.

488 FTC Staff Comments at 19-20.

489 *See, e.g.*, Letter from Michelle R. Rosenthal, Senior Corporate Counsel, T-Mobile, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1-2 (filed Oct. 14, 2016) (T-Mobile Oct. 14, 2016 *Ex Parte*) (asking the Commission to "consider narrowing the scope of sensitive CPNI to the five FTC categories"); Letter from James J.R. Talbot, Executive Director — Senior Legal Counsel, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed Oct. 17, 2016) (AT&T Oct. 17, 2016 *Ex Parte*) (claiming that the FTC considers information sensitive only if it is content or "falls within the traditional categories of sensitive data"); Advertisers Oct 10, 2016 *Ex Parte* at 3-4 (suggesting that FTC has "long held that 'sensitive data' encompasses a limited set of data types"); Letter from Sydney M. White, Counsel to Internet Commerce Coalition, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 18, 2016) (ICC Oct. 18, 2016 *Ex Parte*).

490 FTC 2012 Privacy Report at 58-60 (observing general consensus that five categories were sensitive).

491 *See* FTC, Self-Regulatory Principles for Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting, & Technology (2009) 12 (setting out the principle that "companies should obtain affirmative express consent before they use sensitive data—*for example*, data about children, health, or finances—for behavioral advertising" (emphasis added)); FTC Staff Comments at 19-20 (supporting opt-in "for sensitive information that could be collected by BIAS providers, *including*: (1) content of communications and (2) Social Security numbers or health, financial, children's or precise geolocation data" (emphasis added)).

492 *See 2007 CPNI Order*, 22 FCC Rcd at 6936, para. 13 (finding that "the release of call detail over the telephone presents an immediate risk to privacy" and imposing restrictions on its release); *id.* at 6936, n.45 (explaining that "'call detail' or 'call records' includes any information that pertain to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for in inbound calls, the number from which the call was placed, and the time, location, or duration of any call"; and finding that "a narrower definition that included only inbound or outbound telephone numbers would make it too easy for unauthorized persons with partial information to confirm and expand on that information").

493 *See* Consumer Watchdog Comments at 2-3; Lee Rainie, The State of Privacy in post-Snowden America, Pew Research Center (Sept. 21, 2016) at http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/ft_16-01-20_ssnumbers-1/.

494 *See* CTIA Comments at 96-97; Comcast Comments at 18; ANA Comments at 12; Electronic Transactions Association Comments at 13; Future of Privacy Forum Comments at 27; NCTA Comments at 44.

495 *See* Letter from Maria L. Kirby, AVP Regulatory Affairs & Assoc. General Counsel, CTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 18, 2016); Letter from Michelle R. Rosenthal, Senior Corporate Counsel, Government Affairs,

Federal Regulatory, T-Mobile, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1, n.1 (filed Oct. 19, 2016); *see also, e.g.*, 2012 FTC Report at 58-60; FTC Staff Comments at 19-20; CTIA Comments at 96-97; DMA Comments at 10-11; ANA Comments at 12; CCA Reply at 19-22; Verizon Reply at 21-22; Letter from Melissa Newman, Vice President-Federal Regulatory Affairs, CenturyLink, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 5 (filed Sept. 13, 2016); Letter from Francis M. Buono, Sr. Vice President, Legal Regulatory Affairs & Sr. Dep. General Counsel, Comcast Corp., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Aug. 2, 2016); Future of Privacy Forum Comments at 22-23.

496 *See* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (1999).

497 *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring). *Accord* CDT Comments at 14; EFF Comments at 3-4.

498 *See Riley v. California*, 134 S.Ct. 2473, 2490 (2014) ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."); CDD Comments at 14.

499 *Goldenshores Technologies, LLC*, Decision and Order, F.T.C. Docket No. C-4446, at 3 (March 31, 2014). *Accord Snapchat, Inc.*, Decision and Order, F.T.C. Docket No. C-4501, at 2 (Dec. 31, 2014); *Designware, LLC*, Decision and Order, F.T.C. Docket No. C-4390, at 3 (April 11, 2013). As noted above in paragraph 66, we do not draw distinctions between technologies used to determine precise geo-location. We make clear, however, that we do not consider a customer's postal or billing address to be sensitive precise geo-location information, but rather to be non-sensitive customer PI when used in context as customer contact information.

500 AAJ Comments at 8; ACLU Comments at 7-8; EFF Comments at 5; FTC Staff Comments at 21; OTI Comments at 23; Public Knowledge White Paper at 59; CCA Reply at 19.

501 *See, e.g.*, 47 U.S.C. § 605; 18 U.S.C. § 2510 et seq.; 18 U.S.C. § 2701 et seq.; 18 U.S.C. § 3121 et seq.

502 FTC Staff Comments at 20-21; *see also supra* note 500.

503 FTC Staff Comments at 20.

504 *See supra* note 500.

505 Access Now Comments at 6.

506 Designating content as sensitive customer PI will not, despite NCTA's concerns, require a carrier to obtain additional customer approval to accept or respond to communications with its customers. *See infra* para. 215; *see also* Letter from Loretta Polk, Vice President and Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 18, 2016).

507 *See, e.g.*, Paul Ohm Testimony at 4-5 (explaining that a list of websites visited reveals a customer's reading history); Upturn Comments at 3-4 (explaining that web addresses can reveal web page content); OTI White Paper at 3-5. Some commenters raise the issue of cases drawing distinctions between ""content" and "metadata" in the context of ECPA as standing for the proposition that all non-content data is non-sensitive. *See, e.g.*, Letter from Sydney M. White, Counsel to the Internet Commerce Coalition, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 13, 2016) (ICC Oct. 13, 2016 *Ex Parte*). We disagree. While the text of ECPA requires a court to make determinations of what is and is not "content" of communications to determine that statute's applicability, neither the statute nor the case law interpreting it suggests that information other than content cannot be considered sensitive under the Communications Act.

508 *See, e.g.*, Letter from Dallas Harris, Policy Fellow, Public Knowledge to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1-2 (filed Oct. 21, 2016) (Public Knowledge Oct. 21, 2016 *Ex Parte*) (noting that the confidentiality of communications is not limited to their content in Sections 222 and 705).

509 *See, e.g.*, Letter from Gaurav Laroia, Policy Counsel, Free Press, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed Oct. 7, 2016).

510 *See, e.g.*, AT&T Oct. 17, 2016 *Ex Parte* at 3; Google Oct. 3, 2016 *Ex Parte* at 1.

511 *See, e.g.*, OTI White Paper at 3-5 (explaining that "[b]ecause of their special role handling all of a user's Internet traffic, ISPs have a uniquely detailed and comprehensive perspective on the activities of their subscribers."); Upturn White Paper at 6 (explaining that, even with encryption, "ISPs can still almost always see the domain names that their subscribers visit."); CDT Reply at 21 ("[A] BIAS provider's access to a consumer's data is unique because the BIAS provider serves as the gatekeeper between the consumer and the internet and the shepherd of the consumer's data across the internet ... [A] BIAS provider [in the case of location information] will always have some form of location data for the consumer with the phone ... simply because the BIAS provider cannot serve a phone that it cannot find."); Public Knowledge White Paper at 45 (arguing that "[b]roadband providers uniquely enjoy a confluence of both a total view into subscribers' Internet access habits on the one hand, and knowledge of physical information about the subscribers such as home address and financial information on the other."); Online Trust Alliance Comments at 1.

512 EFF Comments at 4. *See also* 18MillionRising.Org Petition and Comments at 1 ("The tracking and cataloguing of consumers' online habits are especially harmful to marginalized communities, for whom information regarding immigration status, mental health, race, and religion can be particularly sensitive."); Julie Brill, Comm'r, Fed. Trade Comm'n, Net Neutrality and Privacy: Challenges and Opportunities, Keynote Address at Georgetown Institute for Public Representation and Center for Privacy and Technology Symposium on Privacy and Net Neutrality at 6 (Nov. 19, 2015), available at https://www.ftc.gov/publicstatements/2015/11/net-neutrality-privacy-challenges-opportunities ("Even if an ISP just looks at the IP addresses to which you connect and the time at which connections occur, it can get an intimate portrait of your interests, daily rhythms, habits—as well as those of all members of your household.").

513 *See* Paul Ohm Testimony at 4-5; *see also* Paul Ohm July 28, 2016 *Ex Parte* at 4-5; Future of Privacy Forum Reply at 6-7 (explaining that "sensitive data would include the content of detailed browsing histories"); Consumer Watchdog Comments at 2-3; *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. Sup. Ct. 2002) (en banc) (protecting privacy in book purchases).

514 The cable and satellite privacy provisions of the Act were created in significant part to protect the privacy of video viewing habits. *See* H.R. Rep. No. 934, 98th Cong., 2d Sess. 29 (1984) ("Subscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions"); 47 U.S.C. § 551; 47 U.S.C. § 338(i). Video rental records have also been recognized by Congress as worthy of particular privacy protection. VPPA, 18 U.S.C. § 2710 et seq. As such, we disagree with Google's assertions that web browsing has not traditionally been considered sensitive information. Google Oct. 3, 2016 *Ex Parte* at 1 (drawing a distinction between medical records and shopping habits).

515 *See, e.g.*, Andrew G. West & Adam J. Aviv, On the Privacy Concerns of URL Query Strings, 2014 Proc. of the 8th Workshop on Wed 2.0 Sec. and Privacy, available at http://w2spconf.com/2014/papers/privacy_query_strings.pdf; Reisman and Narayanan June 17, 2016 *Ex Parte* at 22-24 (customer names and other PII included in some URLs); *see also* Peter Swire Working Paper at 9 (noting that encryption can block access to detailed URLs, which "can reveal granular details of a user's search or other online activities").

516 *See, e.g.*, OTI White Paper at 5.

517 *See* OTI Oct. 13, 2016 *Ex Parte* at 7-9; Letter from Brandi Collins, Director of Campaigns: Economic, Environmental, & Media Justice Departments, Color of Change, to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106 (filed Oct. 20, 2016) (Color of Change Oct. 20, 2016 *Ex Parte*); Letter from Laura M. Moy & Eric. G. Null, New America's Open Technology Institute, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Sept. 12, 2016); Letter from Brandi Collins, Director of Campaigns: Economic, Environmental & Media Justice Departments, Color of Change, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 2-3 (filed Oct. 3, 2016) (Color of Change Oct. 3, 2016 *Ex Parte*).

518 *See, e.g.*, Public Knowledge White Paper at 47 ("The IP address of the service being accessed can indicate much information about the subscriber based on the nature of the service: a household with children, for example, is likely to visit Disney's website; a domestic violence victim far more likely to be accessing helpline information.").

519 *See, e.g.*, Feamster ISP Data Use Comments at 5 ("A user's DNS lookups can reveal activity patterns, the website that a user is visiting, and (due to website fingerprinting attacks) possibly even the web *pages* that a user visits .... This concern is likely to grow as consumers increasingly deploy [[Internet of Things devices] in their homes, as the DNS and IPFIX traffic from these devices may reveal an increasing amount of information about user behavior and activity.") (emphasis in original).

520 *See, e.g.*, OTI Oct. 13. 2016 *Ex Parte* at 8-9.

521 We do not take a position on how sensitive this information would be in other contexts, or what levels of customer approval would be appropriate in those circumstances.

522 *See, e.g.*, 2012 FTC Privacy Report at 56; CDT Reply at 10; OTI Comments at 3-9; McDonald Reply at 6-7.

523 *See supra* note 511.

524 *See, e.g.*, Reisman and Narayanan June 17, 2016 *Ex Parte* at 34-35.

525 *See, e.g.*, Comcast Comments at 26-27.

526 *See, e.g.*, James Cooper Comments at 3 (noting that "it is clear that certain data (e.g. social security and credit card numbers, bank account information, drivers' license numbers, insurance information) may raise the risk of new- or existing-identity theft, and geolocation data may increase safety risks from stalking. Less clear, however, is the theory by which data, such as browsing histories, shopping records, MAC address, and application usage statistics, threaten privacy.").

527 *See supra* para 34.

528 *See, e.g.*, Reisman and Narayanan June 17, 2016 *Ex Parte* at 17-19; Upturn White Paper at 3-6; McDonald Reply at 4-5.

529 *See, e.g.*, Upturn White Paper at 3-5. Comcast notes that few dispute on the record that a growing volume of traffic is encrypted. Comcast Reply at 38. However, the volume of encrypted data is not indicative of how much customer privacy is protected. For instance, a very small amount of browsing information can reveal that a customer is visiting a site devoted to a particular disease, while many times that data, unencrypted, would only reveal that the user had streamed a particular video. *See* Reisman and Narayanan June 17, 2016 *Ex Parte* at 10-16.

530 Upturn White Paper at 6-9; Reisman and Narayanan June 17, 2016 *Ex Parte* at 26; SIIA Comments 3 ("Broadband service providers are unique in their ability to see the domains that their subscribers visit, even in cases where a web site uses encryption. Recent technical analysis has noted that '[b]ecause the user's computer is assigned by default to use the ISP's DNS server, the ISP is generally capable of retaining and analyzing records of the queries, which the users themselves send to the ISP in the normal course of their browsing.'"); Consumer Action Comments at 1; Consumer Watchdog Comments at 4; Internet Association Reply at 7.

531 Comcast Reply at 38.

532 *See, e.g.*, Narayanan and Reisman Reply at 3-4 (explaining that it is ""technically infeasible" for ISPs to determine the sensitivity of Internet traffic); Upturn White Paper at 6-9 (describing how DNS information and encrypted network traffic can be highly revealing); EFF Comments at 5-6 (arguing that BIAS providers should not be able to "identify or inspect" network information "in order to determine whether it falls into a 'sensitive' category"); *see also* Common Sense Kids Action Oct. 5, 2016 *Ex Parte* at 1 (observing that privacy protections for children under COPPA extend to "how a child moves across different sites and services over time").

533 *See, e.g.*, Public Knowledge Comments at 24-26; Public Knowledge July 26, 2016 *Ex Parte* at 3; Paul Ohm Reply at 10-12; National Consumers League Comments at 2.

534 *See, e.g.*, Future of Privacy Forum Reply at 8 (suggesting that providers could "scan" or "categorize" network information into sensitive and non-sensitive categories).

535 *See, e.g.*, ICC Oct. 18. 2016 *Ex* Parte at 3; Letter from Christopher L. Shipley, Attorney & Policy Advisor, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 18, 2016); Advertisers Oct. 19, 2016 *Ex Parte* at 2.

536 *See* Ohm Reply at 11-12 (noting that "[a]dvertisers can definitely target ads to people suffering from a particular disability on DAA platforms, definitely not on Facebook, and probably not on Google or NAI. Genomic information is only prohibited within the NAI definition [of sensitive information], arguably within Googles, and likely not Facebook's or DAA's. Ads targeted to symptoms might be barred by Google and maybe NAI, but probably not by Facebook or DAA.")

537 Common Sense Kids Action Oct. 5, 2016 *Ex Parte* at 2.

538 *See, e.g.*, OTI Oct. 13, 2016 *Ex Parte* at 2; Letter from Laura M. Moy & Eric. G. Null, New America's Open Technology Institute, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Sept. 12, 2016); Letter from 38 Public Interest Organizations to Chairman Tom Wheeler, Sept. 7, 2016, at 3-4; Letter from Brandi Collins, Director of Campaigns: Economic, Environmental & Media Justice Departments, Color of Change, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 2-3 (filed Oct. 3, 2016) (Color of Change Oct. 3, 2016 *Ex Parte*).

539 AT&T, *U-verse With AT&T Gigapower*, https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1011211 (last visited Sept. 13, 2016).

540 *Id.*

541 Torod Neptune, Verizon Wireless, How Verizon Selects from Verizon Wireless Works, Dec. 3, 2012, http://www.verizonwireless.com/news/article/2012/12/verizon-selects.html ("Verizon Selects will use location, web browsing and mobile application usage data, as well as other information including customer demographic and interest data, to create specific insights."); Verizon Wireless, Verizon Selects FAQs, http://www.verizonwireless.com/support/verizon-selects-faqs/ (last visited Oct. 5, 2016) ("Verizon Selects uses ...[i]nformation about your wireless device including websites you visit, apps and features you use, and device and advertising identifiers ..."). We provide these examples only to demonstrate that BIAS providers already treat web browsing and application usage history as sensitive and as subject to opt-in consent, and we do not mean to suggest that these existing or past programs are reasonable or consistent with the rules and standards we discuss in this Order.

542 Advertisers Oct. 10, 2016 *Ex Parte* at 4.

543 For instance, in both cases, the courts found that plaintiffs had failed to allege that they had suffered "loss" as that term is narrowly defined under the Computer Fraud and Abuse Act. *Mount v. PulsePoint, Inc.*, No. 13 Civ. 6592 (S.D.N.Y. Aug. 17, 2016), 2016 WL 5080131 at *7-8; *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256 (C.D. Cal. April 28, 2011), 2011 WL 1661532 at *6. We do not adopt the CFAA's definitions of "damage" or "loss" for the purposes of this Order.

544 WISPA Comments at 21; Electronic Transactions Association at 13.

545 Paul Vixie Comments at 29; CDT Comments at 8.

546 CDT Comments at 8.

547 *See, e.g.*, EU General Data Protection Regulation, Article 9, Processing of Special Categories of Personal Data; Google, Sensitive Categories, http://www.google.com/policies/privacy/key-terms/#toc-terms-sensitive-categories; Google, Sensitive Personal Information, http://www.google.com/policies/privacy/key-terms/#toc-terms-sensitive-info; Facebook, Restricted information for Lead Ads, https://www.facebook.com/policies/ads/#lead_ads.

548 For instance, some commenters have suggested that information considered non-sensitive at one point might reveal through later analysis information about protected classes. *See, e.g.*, Color of Change Oct. 3, 2016 *Ex Parte* at 2-3 ("[I]nformation drawn from the non-sensitive data can easily become proxy for protected class and sensitive information").

549 FTC Staff Comments at 21.

550 *See*47 CFR § 64.2003(k); NAI, NAI Code of Conduct at 6, http://www.networkadvertising.org/code-enforcement/code (last visited Oct. 13, 2016); NAI, NAI Mobile Application Code at 3, https://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf (last visited Oct. 13, 2016).

551 *See* Access Now Comments at 6.

552 *See supra* note 477.

553 *See, e.g.*, CenturyLink Comments at 16; James Cooper Comments at 3; ANA Comments at 25-26; CTIA Comments at 96-97; NTCA Comments at 28 ("[T]he proposition that Social Security numbers, date and place of birth, mother's maiden name, and unique government identification numbers ... are guarded by customer is likely consistent with current consumer expectations."); CCA Reply at 19.

554 FTC Staff Comments at 19-20 ("[T]he FTC has advocated that companies provide meaningful choices to consumers, with the level of choice being tied to consumer expectations. Under this approach, the FTC supports the use of opt-in for sensitive information that could be collected by BIAS providers.").

555 *See* Verizon Reply at 7-9; CIPL Comments at 5; CompTIA Comments at 7; Lehr et al. Comments at 2-3.

556 Willis Reply at 12-18 (noting defaults made "slippery" through marketing encouraged opting in to certain programs).

557 *See* CenturyLink Comments at 27 (expressing concern that opt-in requirements may force providers to balance informing customers of information-sharing programs against the possibility of annoying or confusing those customers).

558 *See* Willis Reply at 8-10; Behavioral Economics Consulting Group at 2 ("Research in Behavioral Economics has shown that most of the time, peoples' decisions do not conform to a model in which people are information seeking rational actors, guided by self-interest. In particular, where the decision is complex, the stakes are high — and/or the arena is unfamiliar, people are more likely to procrastinate or avoid a decision. In effect, the individual "chooses' avoidance — and ends up being assigned whatever the system's designers have designated as the proxy for 'no answer.' Whoever defined that proxy becomes the *de facto* decision maker.").

559 *Cf.* Greenlining Institute Comments at 29 (noting "dense, slippery and confusing language" in privacy notices); Access Now Comments at 10 ("Opt-out mechanisms typically suffer from cumbersome processes, offer little notice or explanation on the nature of the use, and often even deliberately obfuscate the methods and purposes of corporate programs that track users. Moreover, opt-out is useless in situations where customers have no context to understand the program or service at issue, how it impacts their privacy, or that it even exists in the first place."); Consumer Action Comments at 2; Consumer Watchdog Comments at 6; Privacy Rights Clearinghouse Comments at 4 ("It is tenuous at best to assume that a customer has approved use or sharing merely because she has not opted out of a practice. This is especially true if an opt-out choice is buried deep in a privacy notice, and is in no way in line with customers' expectations."); CDD Comments at 17.

560 *See, e.g.*, Willis Reply at 11-12, n.31 (citing reports that only 0.5 percent of consumers opted out of a financial privacy default, when a far larger number of consumers expressed preferences against tracking); McDonald Reply at 3 (noting that in response to NebuAd tracking, "The total percentage of users to opt out was about 1 ..... [T]his is dramatically lower than the percentage of users who prefer not to have data collected and used for targeted advertising. A majority of users who wanted to opt out did not, and their privacy preferences were violated by their ISPs."); Paul Ohm Reply at 7-10.

561 FTC Staff Comments at 14-15 (recommending "affirmative express consent before making changes that apply to previously collected consumer information"); 2012 FTC Privacy Report at 57-58 (rejecting arguments from AT&T and Phorm that opt-out approval was sufficient, or that approval should be scaled to sensitivity or identifiability of data); EFF Comments at 13; WISPA Comments at 14; CTIA Comments at 122-23.

562 *See, e.g.*, FTC Staff Comments at 14-15 (recommending "affirmative express consent before making changes that apply to previously collected consumer information"); 2012 FTC Privacy Report at 57-58; Charter Reply at 7; CTIA Comments at 123; Internet Commerce Coalition Reply at 1-2; *see also* NTCA Comments at 6 (noting that retroactive material changes can violate consumer expectations of privacy). The CPBR also highlights the need for advance notice of material changes to policies, and the need for additional protections such as express affirmative consent where such changes are retroactive. 2015 Administration CPBR Discussion Draft § 102(e).

563 2012 FTC Privacy Report at 57.

564 *See, e.g.*, Free State Foundation Comments at 9 ("By requiring ISPs create an 'opt out' policy regarding the collection of 'any information that is linked or linkable to an individual,' the Commission risks discouraging ISPs from offering consumers targeted marketing deals or selling advertisements to personally design consumer experiences.").

565 *See supra* para. 166.

566 We note that our requirements for customer opt-out approval serve as a floor, not a ceiling, to the level of customer approval to be provided. Thus, a carrier may set up its programs to solicit and receive customer opt-in approval if it so chooses.

567 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2523, para. 68.

568 *See, e.g.*, Access Now Comments at 6; Consumer Federation of California Comments at 14. *But see* EFF Comments at 6 (opposing removing the 30-day timeframe); OTI Comments at 24 (suggesting in the alternative a 7-day period).

569 *See, e.g.*, FTC Staff Comments at 22-23 (arguing that a privacy framework should "reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data").

570 ANA Comments at 27.

571 CTIA Comments at 97.

572 *See* Letter from Scott Bergmann, Vice President, Reg. Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Aug. 18, 2016) (CTIA Aug. 18, 2016 *Ex Parte*), Attach., ITIF White Paper, Why Broadband Discounts for Data are Pro-Consumer at 4-5 (ITIF White Paper) (describing Alan Westin's groupings of consumers by privacy preference, including "Privacy Fundamentalists" likely to value privacy highly). *But see* Consumer Watchdog Comments at 6 (citing Hoofnagle et al.'s criticisms of Westin's categorizations and Turow, *Tradeoff Fallacy*, which suggests consumer disclosure of data is due to resignation rather than actively trading on their personal information).

573 ITIC Comments at 14-15; FTC Staff Comments at 22-23.

574 ACA Comments at 31; *see also* SIIA Comments at 10; Letter from Joshua Seidemann, Vice President of Policy, NTCA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 14, 2016) (NTCA Oct. 14, 2016 *Ex Parte*) (arguing that the rules should not require opt-in approval for marketing services such as hardware/software systems and alarm/security services).

575 Access Now Comments at 10; *see also, e.g.*, Consumer Action Comments at 2; Consumer Watchdog Comments at 6 ("Opt-out consent is insufficient. In fact, it is not really consent.").

576 *See, e.g.*, Letter from Francis M. Buono, Senior Vice President, Legal Regulatory Affairs, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Sept. 22, 2016) (Comcast Sept. 22, 2016 *Ex Parte*); Letter from Michelle R. Rosenthal, Senior Corporate Counsel, T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 3 (filed Sept. 13, 2016) (T-Mobile Sept. 13, 2016 *Ex Parte*); NCTA Reply at 42-43; ICC Comments at 4; CTA Comments at 8.

577 *See, e.g.*, EFF Comments at 8 (arguing that implied consent in general "eliminate[s] all customer control over PII for a large range of activities, including marketing," and that this is inconsistent with the statute); EPIC Comments at 20 (claiming that "allow[ing] the use of personal information to market additional service offerings without any customer consent conflicts with Section 222(c) of the Communications Act," since it does not obtain the required customer approval); OTI Comments at 37-38 (arguing that there is no implied approval for marketing, and that marketing is not "necessary to, or used in" provision of service); Public Knowledge May 9, 2016 *Ex Parte* at 1 ("While there is precedent establishing that an opt-out system is sufficient to show customer approval, there is no authority for the proposition that a customer 'impliedly' approves of a carrier using his or her information for the purposes of Section 222(c)."); Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, WC Docket no. 16-106, at 1 (filed May 27, 2016); Paul Vixie Comments at 13 (arguing that implied consent for marketing "denies consumer any choice or control").

578 FTC Staff Comments at 16. This same rationale applies to other telecommunications carriers. We note that, as discussed below, limited types of first-party marketing (of categories of service to which a customer subscribes, and services necessary to, or used in, those services) do not require customer approval.

579 *See, e.g.*, Comcast Comments at 49-50; *see also* AT&T Reply at 9 ("Until now, all online companies have been free to use nonsensitive customer-specific information to engage in first-party marketing without any consent mechanism."); Verizon Comments at 24, 31 (asserting that for decades, businesses have "sen[t] ads or promotions to customers for the provider's and its affiliates' products or services"); NTCA Comments at 45-46 (suggesting that "[c]ustomers largely expect firms that have access to their data to use their data" and that "consumers expect providers to identify the services and uses that best meet their needs"); T-Mobile Comments at 8-9 (arguing that customers expect their information to be used for different purposes, including marketing, as adjusted to the sensitivity of the information); ACA Comments at 31.

580 *See supra* note 208; *see also* ACLU Comments at 8-9; Access Now Comments at 9; CDT Reply at 6; Public Knowledge Comments at 29-30.

581 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).

582 *See*47 CFR § 64.1200; 16 CFR Part 310; *see also, e.g.*, Mich. Comp. Laws § 445.111a (2016); N.D. Cent. Code § 51-28-09 (2016).

583 Federal Trade Commission, Biennial Report to Congress Under the Do Not Call Registry Fee Extension Act of 2007, FY 2014 and 2015 at 1 (2015), https://www.ftc.gov/reports/biennial-report-congress-under-do-not-call-registry-fee-extension-act-2007-fy-2014-2015.

584 *See*47 CFR § 64.1200(d)(3); 16 CFR § 310.4(b)(1)(iii).

585 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) ("CAN SPAM Act").

586 16 CFR §§ 316.1-316.6.

587 47 U.S.C. § 222(d).

588 *See supra* Part III.B.3 (noting that the categories of CPNI and PII are not mutually exclusive).

589 *See, e.g.*, EFF Comments at 8 (arguing that access to all customer PI includes access to communications content, contrary to Stored Communications Act); OTI Comments at 38-39 (sensitive information not useful for exceptions and exposes customers to greater risk of harm); Access Now Comments at 9 ("The proposal as written does not provide meaningful limits on sharing CPNI, which can include sensitive user information, such as location and browsing habits. Instead, the proposal should only permit the sharing of CPNI to the extent that any PII or other private data is scrubbed and only 'whenever reasonably necessary to prevent future cyber security threats or risk of vulnerabilities.' Further, the language should only permit the sharing of information for cybersecurity attacks or risk of vulnerabilities only to the extent it does not risk user privacy or security.").

590 18 U.S.C. § 2510-2522 (ECPA); 47 U.S.C. § 1001 et seq. (CALEA); 47 U.S.C. § 605 (Section 705); 6 U.S.C. § 1503(c)(1) (CISA).

591 *See*47 U.S.C. § 222(c)(1).

592 We note that the need for providers to transmit and disclose certain types of customer PI (including IP addresses and the contents of communications) in the course of providing service in no way obviates customers' privacy interests in this information.

593 *See 2015 Open Internet Order*, 30 FCC Rcd at 5748, para. 339 ("[A] broadband Internet access service provider's representation to its end-user customer that it will transport and deliver traffic to and from all or substantially all Internet endpoints necessarily includes the promise to transmit traffic to and from those Internet end points back to the user.").

594 *See* Cincinnati Bell Comments at 6; Audience Partners Comments at 11; NCTA Comments at 74-75.

595 *1998 CPNI Order*, 13 FCC Rcd at 8083, para. 30.

596 *1998 CPNI Order*, 13 FCC Rcd 8061; *1999 CPNI Reconsideration Order*, 14 FCC Rcd 14409.

597 The current voice rules also permit the use and sharing of CPNI without additional customer approval for certain first-party marketing purposes.

598 47 CFR § 64.2005(a).

599 *See, e.g.*, NTCA Comments at 47 ("[C]ustomers generally expect that their broadband providers may use or share the customers' proprietary information with affiliates to market voice, video, or any types of communications-related services tailored to their needs and preferences"); AT&T Oct. 4, 2016 *Ex* Parte at 2-3 (noting that wireline carriers routinely offer, and consumers expect, "double- or triple-play options and other service packages that combine home broadband Internet with voice and video services."); WTA

Comments at 8 (assuming that existing rules include MVPD service with fixed and mobile voice services as "communications-related" services).

600 *See, e.g.*, Comcast Sept 22, 2016 *Ex Parte* at 2; T-Mobile Sept. 13, 2016 *Ex Parte* at 3; *but see* OTI Comments at 37-38; Public Knowledge Comments at 30-31.

601 *See* Verizon Sept. 29, 2016 *Ex Parte*.

602 *See 1998 CPNI Order*, 13 FCC Rcd at 8097-98, para. 48; 47 CFR § 64.2005(c)(3).

603 *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14434, para. 45; 47 CFR § 64.2005(b)(1). Such adjunct-to-basic functions fall within the telecommunications systems management exception to the definition of "information services" in the Act. *See*47 U.S.C. § 153(24) ("the term "information service' ... does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service"); *2015 Open Internet Order*, 30 FCC Rcd at 5766, para. 367 n.1029. In the *2015 Open Internet Order*, we concluded that DNS, caching, and network-oriented, security-related blocking functions including parental controls and firewalls fall within the telecommunications systems management exception and are akin to adjunct-to-basic services. *See 2015 Open Internet Order*, 30 FCC Rcd at 5766-72, paras. 367-73.

604 In each case here and below, whether the particular function is a part of the telecommunications service or a separate service "necessary to, or used in" the telecommunications service may depend on the particular circumstances of the underlying telecommunications service and the customer, and we need not address this distinction to determine that the statutory limitation applies.

605 *See* NTCA Comments at 45-47; WTA Comments at 10; Letter from Loretta Polk, Vice President & Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 14, 2016) (NCTA Oct. 14, 2016 *Ex Parte*); WTA Reply at 11.

606 *See, e.g.*, ACA Oct. 18, 2016 *Ex Parte* at 4.

607 *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14433, para. 43.

608 *1998 CPNI Order*, 13 FCC Rcd at 8080, n.98; 14 FCC Rcd at 14434-35, n.132.

609 *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14433-34, paras. 44-46.

610 *See* Sandvine Comments at 17; Cincinnati Bell Comments at 9; ACA Comments at 40; WTA Comments at 23-24; Lehr et al. Comments at 3; Feamster ISP Data Use Comments at 7-8.

611 *2015 Open Internet Order*, 30 FCC Rcd at 5700, para. 215; 47 CFR § 8.2(f). As we further elaborated in the *2015 Open Internet Order*, reasonable network management includes, but is not limited to network management practices that are primarily used for, and tailored to, ensuring network security and integrity, including by addressing traffic that is harmful to the network; network management practices that are primarily used for, and tailored to, addressing traffic that is unwanted by end users; and network practices that alleviate congestion without regard to the source, destination, content, application, or service. *2015 Open Internet Order*, 30 FCC Rcd at 5701-02, para. 220.

612 *See* NCTA Oct. 14, 2016 *Ex Parte* at 1 (expressing the need for carriers to use customer PI for internal purposes such as improving network performance, quality of service, and customer satisfaction).

613 Since telecommunications carriers must be able to provide secure networks to their customers, we include security research within the scope of research allowed under this limitation. Security research also falls under the exception covered in Part III.D.2.b, *infra*, regarding uses of customer PI to protect the rights and property of a carrier, or to protect users from fraud, abuse, or unlawful use of the networks.

614 *See, e.g.*, Antonakakis et al. Comments.

615 Feamster ISP Data Use Comments at 7-8.

616 Comcast Comments at 60; *see also* Letter from Nick Feamster et al., to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106 (filed Aug. 6, 2016) (Security Researchers Aug. 6, 2016 *Ex Parte*); Future of Privacy Forum Comments at 12; Feamster ISP Data Use Comments at 3-4, 7-8; Lehr et al. Comments at 2-3, 8; NCTA Comments at 76-77; Nominum Comments at 5-6.

617 NCTA Oct. 14, 2016 *Ex Parte* at 1.

618 *See, e.g.*, CDT Reply at 12 ("For example, marketing and social science research are very much attenuated from the direct interests of BIAS customers, and allowing those forms of research may lead to abuses of purported research data that subvert the intent of the NPRM to protect consumer privacy from such uses in the first place.").

619 Security Researchers Aug. 6, 2016 *Ex Parte*; M3AAWG Comments at 5 (explaining that "researchers attempt to use anonymous data to identify signs of a security problem, either on the host ISP network or pointing at signs on another network"); CDT Reply at 12 (stating that "the FCC must develop generic protections that bind security researchers as a condition of receiving BIAS data").

620 This would include, for instance, practicing data minimization and not using more identifiable information than necessary for the research task.

621 47 CFR § 64.2005(c)(2); *see also*47 CFR § 20.3 (defining ""commercial mobile radio service" as including mobile broadband Internet access service").

622 Rural Wireless Association Comments at 4; *see also* American Association of Law Libraries Comments at 3; Consumer Action Comments at 2 (recognizing that "when one does business with an internet service provider, it needs to share limited information about customers with certain other companies to provide service and prepare billing statements"); CCA Oct. 13, 2016 *Ex Parte* at 5 (explaining need for carriers to share information with third parties acting on behalf of the carrier); NTCA Oct. 14, 2016 *Ex Parte* at 2 (recognizing need to share information with third parties or affiliates for billing and similar purposes). Also, as noted below, to the extent that the carrier is using an agent to perform acts on its behalf, the carrier's agents, acting in the scope of their employment, stand in the place of the carrier, both in terms of rights and liabilities. *See infra* note 637.

623 *See*47 U.S.C. § 222(d)(2) (stating that Section 222 does not prohibit a telecommunications carrier from using, disclosing, or permitting access to CPNI obtained from its customers, either directly or indirectly through its agents "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services").

624 *See, e.g.*, M3AAWG Comments at 2; Nominum Comments at 4; Charter Reply at 27-30; NCTA Comments at 76; NCTA Reply at 50-52; CTIA Reply at 83-85; Lehr et al. Comments at 7-9; Letter from Christopher L. Shipley, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3-4 (filed Aug. 4, 2016) (INCOMPAS Aug. 4, 2016 *Ex Parte*).

625 *See, e.g.*, CTIA Comments at 138-39; Email Sender & Provider Coalition Comments at 6-7; NTCA Comments at 46-47 ("NTCA supports the ability of BIAS to use 'customer proprietary information' ... to protect users or others from cyber security threats or vulnerabilities ...."); *see also* Comcast Comments at 59.

626 6 U.S.C. § 1503(c)(1). We do not assume that the scope of our exception is coterminous with the definition of cyber threat information in CISA. As noted, however, to the extent information is allowed to be shared pursuant to CISA, our rules do not inhibit such sharing.

627 As proposed, this includes any form of customer PI, not merely calling party phone numbers. *See* FTC Staff Comments at 18-19; USTelecom Comments at 16; West Telecomm. Serv. Reply at 4-5.

628 Email Sender & Provider Coalition Comments at 6-7; Antonakakis et al. Comments at 3; Comcast Comments at 59.

629 *See, e.g.*, West Telecomm. Serv. Reply Comments at 3-5; FTC Staff Comments at 18; USTelecom Comments at 16-18; *see also* NTCA Comments at 46-47 ("NTCA supports the ability of BIAS to use 'customer proprietary information' ... to address such issues as 'spoofing' and unlawful "robocalls.').

630 USTelecom Comments at 17 ("CPNI sharing in such circumstances is limited to just what is needed to investigate the source of the call such as the calling party telephone number, the called party telephone number, and the date and time of the call.").

631 Access Now Comments at 8-9; *see also* CDT Reply at 12 (explaining need for protections on disclosure for security purposes); EFF Comments at 9 (advocating for limits on disclosures for security purposes).

632 Feamster ISP Data Use Comments; Antonakakis et al. Comments at 2, 4, 6-8; Comcast Comments at 60; CDT Reply at 10-11.

633 As noted above, CISA permits the sharing of cybersecurity threat indicators "notwithstanding any other provision of law." 6 U.S.C. § 1503(c)(1). These provisions should also alleviate the concern expressed in the interim update on information sharing from the Communications Security, Reliability, and Interoperability Council (CSRIC), that our rules may conflict with CISA. CSRIC Working Group 5, Information Sharing Barriers at 7-8 (June 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Info_Sharing_Report_062016.pdf.

634 *See, e.g.*, Security Researchers Aug. 6, 2016 *Ex Parte*. Feamster et al. suggest that security research receive a specific exemption, so long as security disclosures be limited to those that: promote security, stability, and reliability of networks; do not violate privacy; and benefit research in a way that outweighs privacy risks. They also highlight particular categories of researchers to whom disclosure represents less privacy risk. While we decline to include this specific exemption and its criteria, we note that similar steps to mitigate privacy risks and determine trustworthy recipients can be useful factors in determining reasonableness.

635 *See, e.g.*, CCA Comments at 25 (expressing concern that "the proposal to potentially limit sharing of a vast amount of information with affiliates that provide communications-related services would be concerning for competitive wireless carriers with corporate structuring that tends to include vendors and affiliates for the everyday provision of mobile broadband services"); CTIA Comments at 129-130 (arguing that "sharing a customer's name with an ISP's longstanding agent (for which the ISP has assumed liability) presents a diminished privacy risk relative to an ISP's selling a customer's web browsing activity to an anonymous data broker"); Letter from Aaron N. Goldberger, Associate General Counsel, Neustar, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Sept. 9, 2016); Verizon Reply at 14-15 (arguing that the rules should not contain special restrictions for sharing with affiliates and contractors); Level 3 Comments at 12-13; AT&T Reply at 9, 34-35.

636 *See supra* Part III.D.1.

637 47 U.S.C. § 217 ("In construing and enforcing the provisions of this chapter, the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person.").

638 Texas 9-1-1 Entities Comments at 2 (noting the need for customer PI that may be associated with alternative emergency calls, including "data, video, text, and other non-legacy voice services").

639 *See, e.g.*, Access Now Comments at 8; EFF Comments at 9.

640 FTC Staff Comments at 16-17.

641 *But see* FTC Staff Comments at 17.

642 CDD Comments at 20; FTC Staff Comments at 24-25; Hughes Comments at 4-5; Hughes Oct. 14, 2016 *Ex Parte* at 2.

643 *See* ACA comments at 52-53 (arguing that providers can best determine the timing of solicitations most relevant to the context of the interaction); CTIA Comments at 143-44; NTCA Comments at 53-54.

644 *See, e.g.*, NTCA Comments at 54 ("NTCA supports proposals that each BIAS provider be permitted to determine the best method for soliciting customer approval."); USTelecom Comments at 12-13 ("[T]he Commission should ... allow carriers the flexibility to determine the appropriate methods for notifying its customers and to maintain records of choice selections in ways that make sense in the context of the specific provider-customer relationship.").

645 47 CFR § 64.2008(d)(3)(iv).

646 *See, e.g.*, NTCA Comments at 55 ("NTCA supports the proposition that providers may offer customers access to privacy policies and an ability to effectuate related choices through a variety of means, including via telephone or on-line interactions. Providers should

have latitude to determine the most effective course of providing notice to their customers through those methods."); USTelecom Comments at 12-13.

647 NCTA Oct. 20, 2016 *Ex Parte* at 8.

648 We intend for this requirement to mirror the requirements for a provider's provision of its notice of privacy policies.

649 *See, e.g.*, Hughes Comments at 5-6; Sprint Comments at 13-14; CTIA Comments at 104-05; NTCA Comments at 41-42; Rural Wireless Association Comments at 7; WTA Comments at 11-12.

650 WTA Reply at 9-10.

651 ACA Comments at 38-39.

652 *See, e.g.*, Hughes Oct. 14, 2016 *Ex Parte* at 2 (arguing that providers should be required to "update consumers' decisions regarding privacy preferences when they are affirmatively communicated to the provider").

653 NTCA Comments at 38 (requesting that the rules account for context).

654 *See, e.g.*, Letter from Jennifer Manner, Senior Vice President, Regulatory Affairs, Hughes Network Systems, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, Attach. at 1 (filed July 26, 2016) (requesting 10-day timeframe "to implement a consumer's request to opt-in or opt-out of permitted uses of their customer PI."); Hughes Oct. 14, 2016 *Ex Parte* Attach. at 1 (same).

655 *See 1998 CPNI Order*, 13 FCC Rcd at 8151, para. 116 (explaining that "the language of Section 222(d)(3) stating that carriers may 'provide inbound telemarketing, referral, or administrative services to the customer *for the duration of the call*' suggests that Congress expressly limited the duration of approval where it wanted to so specify, and thus the absence of similar language in Section 222(c)(1) evidences that Congress did not limit as a statutory matter the time period within which customer approval remains valid").

656 47 CFR § 64.2007(a)(2); *Broadband Privacy NPRM*, 31 FCC Rcd at 2552, para. 147.

657 *See, e.g.*, Letter from Patricia Cave, Director, Government Affairs, WTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2-3, n.4 (filed Aug. 22, 2016) (WTA Aug. 22, 2016 *Ex Parte*).

658 *See infra* note 690.

659 *Broadband Privacy NPRM*, 31 FCC Rcd at 2557, para. 167; *see also* Access Now Comments at 11-12 ("[T]he ultimate policy cannot create flexibility to excuse companies or actions from failing to provide adequate protections."); National Consumers League Comments at 2 (encouraging adoption of "high baseline data security protections"); American Association of Law Libraries Comments at 4; Greenlining Institute Comments at 45-48; Consumer Action Comments at 2; Access Humboldt et al. Comments at 5.

660 *See, e.g.*, CenturyLink Comments at 32; Comcast Reply at 26; DMA Comments at 24; National Consumers League Comments at 9; New York Attorney General Reply at 3; S^2ERC Center Comments at 3; Jon Leibowitz Comments at 10-11; FTC Staff Comments at 27-28; Letter From Chris Calabrese, VP of Policy, Center for Democracy & Technology, to Marlene Dortch, Secretary, FCC, at 4 (filed Sept. 29, 2016) (CDT Sept. 29, 2016 *Ex Parte*).

661 *See* FTC Staff Comments at 27-28 (outlining the FTC's "technology-neutral, process-based approach to security [it has applied] for two decades"); FTC, Data Security, https://www.ftc.gov/datasecurity ("[A] company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.").

662 *See infra* note 682.

663 *See*47 U.S.C. §§ 551(c)(1), 338(i)(4) (directing cable operators and satellite carriers, respectively, to "take such actions as are necessary to prevent unauthorized access to [subscriber information]"); *see also Cox Consent Decree*, 30 FCC Rcd at 12302, para. 3 ("Congress and the Commission have made clear that cable operators such as Cox must 'take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.'").

664 *See infra* note 681.

665 *See, e.g.*, NTCA Comments at 59-60; CTIA Comments at 156-58.

666 *See infra* Appx A.

667 *See generally Broadband Privacy NPRM*, 31 FCC Rcd at 2557, para. 167 ("Strong data security protections are crucial to protecting the confidentiality of customer PI.").

668 47 U.S.C. § 222(a).

669 *See TerraCom Consent Decree*, 30 FCC Rcd at 7075, para. 2 ("The failure to reasonably secure customers' proprietary information violates a carrier's duty under the Communications Act ..."); *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 ("We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.").

670 *See* Paul Vixie Comments at 31 ("The textbook security objectives are normally confidentiality, integrity, and availability in the enterprise case."); International Association of Privacy Professionals Comments at 2 ("Data security is concerned with the confidentiality, integrity and availability of any information."); NTCA Comments at 58-59.

671 *See, e.g.*, Techopedia, CIA Triad of Information Security, https://www.techopedia.com/definition/25830/cia-triad-of-information-security (last visited Oct. 5, 2016); *see also*44 USC § 3552(b)(3) (defining "integrity," "confidentiality," and "availability" as the constituent elements of "information security"); Office of Management and Budget, Circular No. A-130, Managing Information as a Strategic Resource at 36 (2016), https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf (defining "[s]ecurity control" as "the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information").

672 *See* ATIS, *ATIS Telecom Glossary: Confidentiality* (Sept. 12, 2016), http://www.atis.org/glossary/definition.aspx?id=6609; *see also*44 U.S.C. § 3552(b)(3)(B). Our discussion of "confidentiality" as part of the CIA triad of data security principles is not intended to suggest that the term has the same meaning under Section 222 of the Act as it has in the CIA context.

673 *See* ATIS, *ATIS Telecom Glossary: Integrity* (Sept. 12, 2016), http://www.atis.org/glossary/definition.aspx?id=458; *see also*44 U.S.C. § 3552(b)(3)(A).

674 *See* ATIS, *ATIS Telecom Glossary: Availability* (Sept. 12, 2016), http://www.atis.org/glossary/definition.aspx?id=5637; *see also*44 U.S.C. § 3552(b)(3)(C).

675 NTCA Comments at 58. Additionally, one commenter notes that increasing security may affect availability. *See* Paul Vixie Comments at 31 ("We believe availability to be fully on par with the other objectives mentioned for a utility-like service such as broadband service. A desire for security must NOT be allowed to potentially degrade availability."); *see also* International Association of Privacy Professionals Comments at 2 ("Data security is concerned with the confidentiality, integrity and availability of any information.").

676 *See supra* note 670.

677 *But see* FTC Staff Comments at 27-28 ("[T]he proposed rule text would impose strict liability on companies for 'ensuring' security."); CenturyLink Comments at 32-33; CTIA Comments at 159-161.

678 *See* Federal Trade Commission, Start with Security: A Guide for Business at 1 (2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (2015 FTC Security Guide for Business).

679 *See, e.g.*, GMR Transcription Services, Inc., Complaint, F.T.C. File No. 122-3095 (2014), https://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf (GMR Transcription Services Complaint); GeneLink, Inc., Complaint, F.T.C. File No. 112-3095 (2014) https://www.ftc.gov/sites/default/files/documents/cases/140107genelinkcmpt.pdf (GeneLink Complaint); Accretive Health, Inc., Complaint, F.T.C. File No. 122-3077 (2014), https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf; *see also FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015) (upholding FTC authority to bring data security cases under the Section 5 "unfairness" prong).

680 *See, e.g.*, Md. Code Ann., Com. Law § 14-3503(a) (2016); Utah Code Ann. § 13-44-201 (2016); Fla. Stat. § 501.171(2) (2016); Cal. Civ. Code § 1798.81.5(b)-(c) (2016).

681 *See* 2015 Administration CPBR Discussion Draft § 105(a)(2); *see also* 2012 White House Privacy Blueprint at appx. A ("Consumer Privacy Bill of Rights").

682 *See* National Institute for Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity at 2 (2014) http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (NIST CSF) ("The [NIST CSF] is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks — different threats, different vulnerabilities, different risk tolerances — and how they implement the practices in the [NIST CSF] will vary.").

683 *See, e.g.*, FTC Staff Comments at 27-28; National Consumers League Comments at 9 (citing Kamala D. Harris, Cal. Dep't of Justice, *California Data Breach Report 2012-2015* 5 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf) ("What constitutes *reasonable* data security today will not constitute reasonable data security tomorrow.") (emphasis added); Direct Marketing Association Comments at 24 ("Adequate protections for consumers can be effectively achieved by requiring BIAS providers to maintain 'reasonable' data security practices ...."); Jon Leibowitz Comments at 10-11; Electronic Transactions Association Comments at 2; New York Attorney General Reply at 3; S^2ERC Comments at 3; Online Trust Alliance Comments at 3; CompTIA Comments at 1-2; ViaSat Comments at 6-7; CDT Sept. 29, 2016 *Ex Parte* at 4; Letter From Harold Feld, Senior VP, Public Knowledge, to Marlene Dortch, Secretary, FCC at 3 (filed Oct. 3, 2016) (Public Knowledge Oct. 3, 2016 *Ex Parte*).

684 *See* CenturyLink Comments at 32; Comcast Comments at 22; Verizon Comments at 65; T-Mobile Comments at 47; NCTA Reply at 54; CCA Reply at 10; WTA Aug. 22, 2016 *Ex Parte* at 3.

685 *See, e.g.*, ACA Reply at 9-10; WTA Reply at 12-13; CenturyLink Comments at 32-33; T-Mobile Comments at 47-48.

686 WTA Reply at 12; *see also* U.S. Small Business Administration Reply at 3 ("The record in this proceeding would support any effort by the FCC to mitigate the disproportionate compliance burden its proposal would have on small BIAS providers.").

687 *See* FTC Staff Comments at 27-28.

688 *See, e.g.*, CenturyLink Comments at 32 ("[A]ll providers should adopt reasonable data security safeguards based [on contextual factors proposed in the *NPRM*].").

689 *See, e.g.*, WTA Aug. 22, 2016 *Ex Parte* at 3 ("WTA also argued that size should be a factor for consideration when assessing the implementation of reasonable security measures in order to avoid unreasonably holding small carriers with only a handful or two of employees to the same standard as providers that employ armies of technical and security professionals and drive industry best-practices.").

690 WTA Aug. 22, 2016 *Ex Parte* at 2-3; *see also* RWA Reply at 2 ("[U]nlike large or nationwide BIAS providers, [our] members do not generally collect, store, analyze, and exploit [CPNI]"); WTA Comments at 19 ("Small BIAS providers also do not engage in the collection and retention of sensitive consumer information to the extent that other industry participants that are subject to the FTC enforcement do."); CCA Comments at 33 ("[M]any CCA carrier members that fall under CCA's proposed definition of small provider do not share customer information with third parties for advertising purposes."); NTCA Comments at 1 ("As a general matter ... NTCA members do not broker their customers' information."); ACA Comments at 5 (explaining that "ACA members generally do not use their customers' information for purposes requiring opt-in consent—often because they lack the incentive or resources to do so").

691 *See* ACA Comments at 8 ("Most ACA members have few employees: half of ACA's members have ten or fewer employees."); Education and Research Consortium et al. Comments at 10; RWA Comments at 10-12; WISPA Comments at 26-27; WTA Aug. 22, 2016 *Ex Parte* at 3.

692 *See* RWA Comments at 12 ("Saddling small carrier employees with qualification requirements in rural markets (where workforce demands are often already difficult to meet) is counterproductive and may force small rural carriers into unnecessary additional hires, solely for the purpose of meeting such requirements."). ACA Oct. 18, 2016 *Ex Parte* at 2 (urging the Commission to "[r]ecognize the limited financial resources of smaller ISPs in determining whether their data security practices are 'reasonable.'") (internal formatting omitted). Our decision not to adopt minimum required security practices should further allay concerns about the impact of the rule on small providers. *See, e.g.*, WTA Aug. 22, 2016 *Ex Parte* at 3 ("Because risk management requires tough decisions regarding which

risks are reasonably acceptable in light of an organization's activities, size and resources, WTA urged the Commission to provide flexibility for small carriers and refrain from imposing specific security requirements beyond a generalized duty to employ reasonable security measures."); RWA Reply at 11 (citing WTA Comments at 21) ("[A]llow each BIAS provider to determine the particulars of and design its own risk management program, taking into account the probability and criticality of threats and vulnerabilities, as well as the nature and scope of a provider's business activities and the sensitivity of the underlying data."); ACA Reply at 44 ("[E] xempt small providers from the specific minimum data security requirements ...."); CTIA Reply at 10.

693 *See* ACA Comments at 23; CCA Comments at 42; WTA Comments at 18-25; U.S. Small Business Administration Reply at 3-4; Letter From Joshua Seidemann, Vice President of Policy, NTCA, to Marlene Dortch, Secretary, FCC at 2-3 (filed Sept. 16, 2016) (NTCA Sept. 16, 2016 *Ex Parte*).

694 *See* National Consumers League Reply at 21 ("[P]rotecting consumers' data is a part of running a modern company."). *But see* ACA Oct. 18, 2016 *Ex Parte* at 2 ("[The Order] should explicitly state that a higher relative cost for a smaller ISP to implement a practice on a per customer basis compared to a larger ISP is a factor in determining whether an ISP's implementation of a practices is reasonable.").

695 *See supra* Part III.D.

696 The State Privacy and Security Coalition argues that the security rule proposed in the *NPRM* would be too burdensome when applied to non-sensitive information. *See* State Security and Privacy Coalition Comments at 5, 11-12; *see also* Letter From Michelle Rosenthal, Senior Corporate Counsel, Government Affairs, Federal Regulatory, T-Mobile, to Marlene Dortch, Secretary, FCC at 2 (filed Sept. 14, 2016) (T-Mobile Sept. 14, 2016 *Ex Parte*) ("The standard should be limited to either sensitive CPNI or CPNI that is likely to lead to an economic or physical harm in the event of an unauthorized disclosure."). We believe the modifications we have made to the proposal, including our decision not to adopt minimum required security practices, sufficiently address this concern.

697 *Contra* National Consumers League Comments at 9; *but see* ACLU Comments at 6. As explained above, we have determined that it is both feasible and appropriate to draw a distinction between sensitive and non-sensitive information under our rules. *See supra* Part III.D.1.

698 *See supra* para. 242. Where sensitive and non-sensitive customer PI are commingled, a carrier should err on the side of treating the information as sensitive.

699 *See* Access Now Comments at 11; CTIA Comments at 96-97; IAB Comments at 11.

700 *See* 2015 FTC Security Guide for Business at 1.

701 *See, e.g.*, FTC Staff Comments at 27-28 (expressing support for a formulation of the rule that includes the "technical feasibility" factor).

702 *But see* AT&T Comments at 78 ("The NPRM's discussion of 'reasonable' data security also ignores many factors that are highly relevant to what security measures should be adopted, such as the nature of the threats that ISPs face and the costs of security measures."); NTCA Sept. 16, 2016 *Ex Parte* at 4-5, n.5; CCA Oct. 13, 2016 *Ex Parte* at 6.

703 *See* National Consumers League Reply at 19.

704 *But see* Access Now Comments at 11 ("[T]he ultimate policy cannot create flexibility to excuse companies or actions from failing to provide adequate protections."); American Association of Law Libraries Comments at 4; Consumer Action Comments at 2; Access Humboldt et al. Comments at 5.

705 *See TerraCom Consent Decree*, 30 FCC Rcd at 7075, paras. 1-2; *AT&T Consent Decree*, 30 FCC Rcd at 2808, para. 2; *Cox Consent Decree*, 30 FCC Rcd at 12303, para 4.

706 *See TerraCom NAL*, 29 FCC Rcd at 13335, paras. 29-30.

707 *See generally TerraCom Consent Decree; AT&T Consent Decree; Cox Consent Decree.*

708 *See AT&T Consent Decree*, 30 FCC Rcd at 2808, para. 2.

709 *See, e.g.*, Information Technology Industry Council Comments at 15 ("[The] proposed requirements contradict existing cybersecurity public policy — such as that embedded in the [NIST Cybersecurity Framework] — that risk management is a continuous process demanding flexibility ..."); NTCA Sept. 16, 2016 *Ex Parte*.

710 *See* Communications, Security, Reliability and Interoperability Council, Cybersecurity Risk Management Best Practices: Working Group 4: Final Report (March 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (final report of a Commission federal advisory committee charged with developing "implementation guidance to help communication providers use and adapt the voluntary NIST Cybersecurity Framework").

711 In late August, FTC staff issued a blog post as part of its data security education work showing how the NIST CSF and the FTC's data security work complement each other. *See* Andrea Arias, FTC, The NIST Cybersecurity Framework and the FTC (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc (FTC Staff Guidance on NIST CSF).

712 CTIA Reply at 83-85.

713 *See* Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501-1510 (2016); *see also supra* para. 212.

714 *See, e.g.*, Federal Trade Commission Act, 15 U.S.C. § 45 (FTC Act provision setting forth the "unfair or deceptive" standard that guides FTC oversight of commercial data security practices); 42 U.S.C. § 1320d-2(d); 45 CFR §§ 164.302-164.318 (Health Insurance Portability and Accountability Act (HIPAA) "Security Rule" and related implementing regulations); 15 U.S.C. §§ 6801-6809; 16 CFR §§ 314.1-314.5 (Gramm-Leach-Bliley Act (GLBA) and its implementing regulations); Md. Code Ann., Com. Law § 14-3503(a); Utah Code Ann. § 13-44-201; Fla. Stat. § 501.171(2); Cal. Civ. Code § 1798.81.5(b)-(c) (examples of state laws on data security).

715 *See, e.g.*, 2015 FTC Security Guide for Business; Federal Communications Commission, CSRIC Best Practices, https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm (last visited Oct. 5, 2016).

716 *See, e.g.*, NIST, Cybersecurity Framework, http://www.nist.gov/cyberframework.

717 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2559-69, paras. 174-209.

718 Charter Reply at 31; *see also* CTIA Comments at 151; Lenard and Wallsten Comments at 36; DMA Comments at 22 (arguing that minimum requirements "would merely add additional 'box checking'"); Cincinnati Bell Comments at 8 ("[The Commission] should future-proof its rules by encouraging BIAS providers to keep pace with rapid developments in the industry (*i.e.*, act reasonably)."); ViaSat Comments at 7. *But see* National Consumers League Reply at 19; CDT Sept. 29, 2016 *Ex Parte* at 4.

719 For example, National Consumers League recommends adoption of multi-factor authentication as a required "minimum baseline." National Consumers League Comments at 14-16; *see also* AAJ Comments at 8. Yet the record includes discussion of a variety of techniques for robust customer authentication, not all of which would necessarily qualify as "multi-factor" in all circumstances. *See, e.g.*, Steven Bellovin Reply at 2 (recommending as a customer authentication method the use of data from commercial brokers to dynamically generate "unusual" security questions); Lorrie Faith Cranor Reply at 4 (observing that "[m]ulti-factor methods may or may not be necessary for routine transactions" but recommending that carriers always make such methods available to their customers); *see also* Consumers' Research Comments at 21 ("Log-in preferences vary widely, so when the Commission considers mandating a certain log-in technique, it is not listening to customers who are frustrated by onerous authentication methods that make account management an ordeal"); Cincinnati Bell Comments at 8-9 ("Instead of forcing rigid syntax rules (e.g., requiring certain characters), which may actually provide impostors with information as to the proper format of a valid password, ISPs should be allowed to offer flexible password strength and security features similar to current banking industry and Government agency practices when users set up access to their account information.").

720 *But see* ITTA Comments at 23 (opposing a "one-size-fits-all" approach to data security); AT&T Comments at 79-80 (criticizing the "rigidity of the proposed rules"); ACA Comments at 23 ("The Commission's proposed prescriptive data security requirements would impose overwhelming costs and burdens on small providers.").

721 *See, e.g.*, CCA Comments at 41 ("CCA is concerned that if the FCC adopts its proposed specific data security requirements, it would quell the natural progression of best practices that currently is evolving, and ultimately force BIAS providers to prioritize compliance over an adaptable security risk-based management model that is required to address the evolving cyber threat landscape.")

(internal quotation omitted); NCTA Reply at 55 ("[T]he specific data security obligations proposed or considered in the Notice ... are overly prescriptive, not calibrated to incentivize protection for sensitive data, and inconsistent with state and federal policy."); WTA Comments at 18 ("Small providers do everything in their power to make sure that vulnerabilities are minimized, but they cannot be required to dedicate precious network resources to combat a vulnerability that is not likely to be a substantial threat to the rest of the network and other services provided to their customers."); T-Mobile Comments at 47 ("Providers must have the flexibility to allocate resources in accordance with the assessed risk to the provider and its customers, particularly as technology and the threat environments evolve."); AT&T Comments at 79 ("[T]he NPRM proposes that companies must 'promptly remedy *any*' security concerns that [risk management] assessments identify. On its face, this would require ISPs to address any issue identified by a security assessment, regardless of whether it is material, regardless of cost, regardless of the sensitivity of the underlying data, and regardless of the risk of a breach.").

722 *See, e.g.*, Cincinnati Bell Comments at 8 ("[The Commission] should future-proof its rules by encouraging BIAS providers to keep pace with rapid developments in the industry (*i.e.*, act reasonably)."); *see also* WTA Comments at 19 ("Nor should the Commission establish safe harbors with respect to minimum data security standards as this could be seen by some as all that is required, rather than encouraging providers to take additional steps as appropriate to manage their cyber risk."). *But see* Hughes Oct. 14, 2016 *Ex Parte* at 3 (supporting adoption of a safe harbor).

723 *See* FTC Staff Comments at 29.

724 *See, e.g.*, *2015 Open Internet Order*, 30 FCC Rcd at 5659-69, paras. 133-53 (setting forth the "no-unreasonable interference/disadvantage standard" and the "factors to guide application of the rule"); *see also Implementing Public Safety Broadband Provisions of the Middle Class Tax Relief and Job Creation Act of 2012*, Order, 27 FCC Rcd 9652, 9662-64, para. 25 (2012) (articulating as "guidance" several "factors [the Commission] would likely find to be supportive of a public interest finding favorable to merit a grant" of a special temporary authorization); NCTA Comments at 87 ("A "reasonableness' standard administered on a case-by-case basis makes sense, since it provides companies with the flexibility to adapt and innovate with regard to the manner in which they safeguard data."); CompTIA Comments at 2 (recommending implementation of "a case-by-case framework mirroring the FTC's implementation of Section 5 authority").

725 *See* S^2ERC Comments at 3 ("[L]everaging the FCC's expertise to provide interpretive and technical guidance could bolster consumer privacy and simplify compliance for new and smaller BIAS providers."); T-Mobile Sept. 14, 2016 *Ex Parte* at 2 ("The final rule should include a reasonableness standard that can be supplemented by further FCC guidance as to what constitutes 'reasonable security,' and that can evolve with changing technology and threat environments.").

726 *See, e.g.*, FTC Security Guide for Business at 1 ("Distilling the facts of [more than fifty FTC data security enforcement actions] down to their essence, here are ten lessons to learn that touch on vulnerabilities that could affect your company, along with practical guidance on how to reduce the risks they pose.").

727 *See* 2015 Administration CPBR Discussion Draft at § 105.

728 *See, e.g.*, CenturyLink Comments at 37-38; Charter Reply at 31; NCTA Reply at 57; *see also* FTC Staff Guidance on NIST CSF ("[A]s the FTC's enforcement actions show, companies could have better protected consumers' information if they had followed fundamental security practices like those highlighted in the [NIST CSF].").

729 *See, e.g.*, Access Now Comments at 11 ("[A]ccess controls, authentication safeguards, and notification and patching systems are all considerations in the NIST Framework.").

730 *See, e.g.*, Ohlhausen Comments at 1 ("We [*i.e.*, the FTC] conduct extensive consumer and business outreach and guidance; coordinate workshops to foster discussions about emerging privacy and data security issues; coordinate on international privacy efforts; and advocate public policies that protect privacy, enhance data security, and improve consumer welfare."); *see also* 2015 FTC Security Guide for Business. This document imparts "lessons learned from the more than 50 law enforcement actions [regarding data security] the FTC has announced so far." *Id.* at 1.

731 *See, e.g.*, National Institute for Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability And Accountability Act (HIPAA) Security Rule at 15-17 (2008), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf (NIST guidance for HIPAA Security Rule risk analyses).

732 *See* FCC, CSRIC Best Practices, https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm.

733 *See* FCC, CSRIC, Membership List, https://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_Membership_03_17_15.pdf (CSRIC membership as of March 17, 2015); *see also* CenturyLink Comments at 10-11; NTCA Sept. 16, 2016 *Ex Parte* at 2.

734 FTC Staff Comments at 28.

735 *See* Access Now Comments at 12 ("Digital rights like privacy and freedom of expression are material issues that require board-level oversight in information and communication technology companies."); National Consumers League Comments at 18-19.

736 *See, e.g.*, WTA Aug. 22, 2016 *Ex Parte* at 3; RWA Comments at 12.

737 *See* NTCA Comments at 62; Sprint Comments at 19; Greenlining Institute Comments at 47; American Association of Law Libraries Comments at 4; National Consumers League Comments at 17-18.

738 *See 1998 CPNI Order*, 13 FCC Rcd at 8198, para. 198; *see also*47 CFR § 64.2009(b).

739 *See, e.g.*, International Association of Privacy Professionals Reply at 3-5 ("More than 10,000 IAPP members have already been certified under the association's various bodies of knowledge" such as the Certified Information Privacy Professional (CIPP) program, Certified Information Privacy Manager (CIPM) program, and Certified Information Privacy Technologist (CIPT) program, which are "accredited by the American National Standards Institute (ANSI) under the International Organization for Standardization's (ISO) standard 17024: 2012 ...").

740 *See* Greenlining Institute Comments at 45-47; Electronic Frontier Foundation Comments at 16; American Association of Law Libraries Comments at 5; AAJ Comments at 7-8; Access Humboldt et al. Comments at 5. Third party recipients of customer PI may also be subject to FTC jurisdiction. *But see* S^2ERC Comments at 14-15.

741 *See* National Consumers League Comments at 21; EFF Comments at 16.

742 *See*47 U.S.C. § 217; *Long Distance Direct, Inc.*, Apparent Liability for Forfeiture, 15 FCC Rcd 3297, 3300, para. 9 (2000) (clarifying that Section 217 imposes liability for acts of independent contractors).

743 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2564, para. 193.

744 *See* Lorrie Faith Cranor Reply at 3-6; Steven Bellovin Reply at 1-2; National Consumers League Comments at 14-16.

745 *See* Lorrie Faith Cranor Reply at 4 (suggesting that multi-factor authentication methods "should always be offered to customers who want to use them"); Steven Bellovin Reply at 1 (describing the use of smart-phone apps, commercial data brokers, and written requests as alternate authentication methods); S^2ERC Comments at 15 ("[O]ne mechanism for improving customer authentication processes might be eliminating the usage of certain identifiers .... such as Social Security Number and mother's maiden name."); Mozilla Comments at 7; National Consumers League Comments at 14-15; Paul Vixie Comments at 26-31.

746 *See* Lorrie Faith Cranor Reply at 4 ("[Providers] should establish authentication procedures that are not unduly burdensome to their customers performing routine transactions, but that may require extra steps in higher-risk situations (for example when a mobile customer requests an account change but claims to have lost their phone).").

747 *See* Lorrie Faith Cranor Reply at 4 ("Due to changing technology and differences in the ways BIAS providers interact with their customers, I recommend allowing providers some flexibility in establishing authentication procedures informed by periodic risk assessments and updated to respond to the changing technology and security landscape."); *Cf.* National Consumers League Comments at 15 (advocating for an FCC advisory council to regularly assess the efficacy of multi-factor authentication methods and recommend updates).

748 *See* Lorrie Faith Cranor Reply at 6 ("[Account change notification] is a currently implemented best practice and makes sense to continue.").

749 *See, e.g.*, EPIC Comments at 24; EFF Comments at 6-7; Mozilla Comments at 7.

750 *See* 2015 FTC Guide for Business at 2 (advising businesses not to "collect personal information you don't need," and to "[h]old on to information only as long as you have a legitimate business need").

751 *See* 2015 Administration CPBR Discussion Draft at § 104.

752 *See*47 U.S.C. §§ 551(e), 338(i)(6) ("Destruction of information").

753 *See*16 CFR § 682.3(a); *see also* FTC Staff Comments at 28-29 (discussing the Disposal Rule). There are also state laws on data disposal that may provide additional guidance. *E.g.*, Ark. Code Ann. § 4-110-104(a); Kan. Stat. Ann. § 50-7a03; N.J. Stat. Ann. § 56:8-162.

754 *See* EPIC Comments at 23; OTI Comments at 41; Paul Vixie Comments at 31; WTA Comments at 20-21.

755 *See* 2015 FTC Guide for Business at 6-7.

756 *See infra* para. 269.

757 *See, e.g.*, ACA Comments at 23-28; WISPA Comments at 31; CCA Comments at 38; CTIA Comments at 154-56; NCTA Comments at 87-89.

758 *See, e.g.*, CTIA Comments at 155-56 ("Rather than imposing the prescriptive regulation proposed in the NPRM, the Commission should consider a flexible reasonableness standard for data security, akin to the FTC model.").

759 *See supra* note 68.

760 *See supra* note 659.

761 *See, e.g.*, *Broadband Privacy NPRM*, 31 FCC Rcd at 2536-37, n.181.

762 *See* ACA Comments at 57-58; RWA Comments at 10-12.

763 *See generally* Lorrie Faith Cranor Reply at 1 (outlining "how authentication requirements may address the growing problem of mobile phone account hijacking and related fraud"); Steven Bellovin Reply; *see also* ACA Comments at 53 (characterizing the voice authentication rules as "[o]verly prescriptive"); Letter From Catherine M. Hilke, Assistant General Counsel, Verizon, to Marlene Dortch, Secretary, FCC at 1 (filed Sept. 23, 2016) (Verizon Sept. 23, 2016 *Ex Parte*) ("Harmonization also would provide the Commission with the opportunity to update its existing but outdated voice rules, including those related to authentication that may inhibit providers from taking advantage of new, more secure technologies.").

764 The rules specify authentication procedures for different kinds of customer interactions: in person, over the telephone, and online. *See*47 CFR § 64.2010(b)-(d). Authentication online or during a customer-initiated telephone call requires the use of a password. *See id.* at § 64.2010(b), (c).

765 *See, e.g.*, WTA Comments at 19 (discussing the costs that would accrue to smaller providers in complying with "multiple regulatory regimes").

766 *See infra* Part III.I.

767 The data breach notification requirements adopted in this Report and Order extend to breaches involving a carrier's vendors and contractors. *See*47 U.S.C. § 217.

768 *See, e.g.*, Access Now Comments at 12.

769 We note that these obligations are not mutually exclusive with other data breach notification obligations stemming from other state, local, or federal laws, or contractual obligations. *See* Part III.J.

770 *See, e.g.*, Lenard and Wallsten Paper at 28; FBI/Secret Service Reply at 3-4; CenturyLink Comments at 41-42; CTIA Comments at 176; Comcast Comments at 61-62; AT&T Comments at 80-81; INCOMPAS Comments at 16; Letter from Jacquelyne Flemming, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed July 28, 2016) (AT&T July 28, 2016 *Ex Parte*).

771 *See, e.g.*, XO Communications Comments at 6 (explaining that data breach notifications based on customer harm "increases the likelihood that the consumer will be motivated to read the notice and take appropriate action, such as monitoring relevant accounts, to prevent and mitigate potential harm, including identity or financial theft"); INCOMPAS Comments at 16 (arguing that without an intent or harm standard, customers will not understand the potential impact of breaches in the notification they receive); AT&T Comments at 81 (asserting that over-reporting will distract attention from genuine data security).

772 *See, e.g.*, XO Communications Comments at 9-10 (asserting that "consumers and other notification recipients will so regularly receive such notices that they will inevitably stop reading them because it will become impossible to discern which notices involve a true threat to their identity or finances, from those that pose effectively no risk."); CompTIA Comments at 4; ICC Comments at 15; State Privacy and Security Coalition Comments at 4-5; AT&T Comments at 81; Comcast Comments at 62-63 ("If customers receive such meaningless breach notifications, they are more likely to disregard the notifications that are meaningful—not only from their ISP, but generally.").

773 *See, e.g.*, CenturyLink Comments at 41 (asserting that "[o]ver-notification would also impose substantial disruptions on the consumer-BIAS provider relationship" and that the "harm to public perception and brand value of the BIAS provider that would result is both unnecessary and unfair — and could even, in some cases, lead consumers to opt out of broadband use entirely."); WISPA Comments at 20 ("Consumers should not be overwhelmed with inconsequential notices that potentially create unwarranted distrust of its providers."); INCOMPAS Comments at 16; T-Mobile Comments at 51-52 ("Notifications involving breaches that pose no harm — which cannot offer the consumer any meaningful steps to take in response — serve only to confuse customers and corrode faith in providers' practices based on misconceptions as to the consequences of a purported 'breach.'"); Verizon Comments at 69 ("[T]he provider responsible for these excessive breach notifications will risk losing the customer's trust for no good reason: for sending notifications when there has been no harm (or even risk of harm) to the customer's privacy interests.").

774 *See, e.g.*, ACA Comments at 35 ("Moreover, the costs of providing notifications and associated breach costs are sky high—one recent estimate was well over $130 per person." citing Richard Kissel, Hyunjeong Moon, U.S. Dep't of Commerce, Draft NISTIR 7621 Revision 1, *Small Business Information Security: The Fundamentals* 2 (2014)); State Privacy and Security Coalition Comments at 8-9 ("[B]reach notice incidents are expensive. The average cost per record of a data breach including both out of pocket costs and harm to good will currently exceeds $200 per record." citing Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis* (2015), *available at* https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF); CTIA Comments at 175 (asserting that reporting of minor non-harmful breaches is costly to ISPs and of no use to consumers).

775 *See generally* Nat'l Conference of State Legislatures, *Security Breach Notification Laws; see also* Jill Joerling, Data Breach Notification Laws: An argument For a Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J. L. & Pol'y 467 (2010).

776 For example, Connecticut does not require entities to disclose a breach if an investigation determines that no harm is likely. *See*Conn. Gen. Stat. § 36a-701b(b)(1); *see also*Ark. Code § 4-110-105(d) (notice not required if no reasonable likelihood of harm); Fla. Stat. § 501.171(6)(b) (notice not required if reasonably determined that breach has not and will not likely result in identity theft or any other financial harm); Iowa Code § 715C.2(6) (no notice required if no reasonable likelihood of financial harm has resulted or will result from the breach); Or. Rev. Stat. § 646A.602(1)(a) (no notice required if no reasonable likelihood of harm has resulted or will result from the breach); N.J. Stat. Ann. § 56:8-163(a) (notice not required if determined that misuse of the information is not reasonably possible); *see also* State Privacy and Security Coalition Comments at 13("A large majority of state breach notice laws (41 out of 47) contain a 'harm trigger' to distinguish between these circumstances and to avoid over-notification.").

777 *Discussion Draft of H.R._, Data Security and Breach Notification Act of 2015 Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. On Energy and Commerce*, 114th Cong. 15 (2015), http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-RichJ-20150318.pdf, (prepared statement of Jessica Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n); *see also* Letter from James J.R. Talbot, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket N0. 16-106, at 2 (filed Aug. 23, 2016) (AT&T Aug. 23, 2016 *Ex Parte*) (asserting that "the Commission should reduce

excessive reporting by adopting the approach taken by many states of not requiring notification where a provider determines that there is no reasonable likelihood of harm to any customer resulting from the breach).

778 *See, e.g.*, AAJ Comments at 7.

779 *See supra* note 776.

780 *See* AAJ Comments at 7.

781 Some comments could be construed as supporting a standard of this kind. *See, e.g.*, CTIA Comments at 176 ("The Commission should require notification only if a breach causes harm or is likely to cause harm.").

782 *See* Access Now Comments at 13 ("There are standard practices for response to breaches involving data such as credit card information or social security numbers. However, there is no standard practice for breaches that involve PII that cannot easily be tied to financial harm, such as personal photos. Stronger responses to a broader array of breaches would increase user trust in BIAS providers.").

783 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2575-76, para. 237 n.373 (citing *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, Report and Order, 26 FCC Rcd 9114, 9122, para. 22 (2011) (agreeing that the term "'harm' is a broad concept that encompasses financial, physical, and emotional harm")).

784 Privacy Rights Clearinghouse Comments at 6 ("Privacy harms are broad and nuanced, and breach victims often suffer or are at risk of suffering harms that can't be qualified as financial or economic in nature."); LGBT Technology Partnership Comments at 1-2 ("All around the country, LGBT people still face signification discrimination including bullying, rejection by families, loss of employment and even the possibility of physical harm simply for their LGBT identity ... For this reason, LGBT individuals are fiercely protective of their privacy and may face drastic consequences if that privacy is breached."); *see also* TRUSTe & Nat'l Cyber Sec. Alliance, *U.S. Consumer Privacy Index 2016, available at* https://staysafeonline.org/download/datasets/17482/DPD[4].pdf. (showing that 68 percent of consumers were more concerned about not knowing how personal information was collected online than losing their principal income) (Consumer Privacy Index 2016).

785 *See, e.g.*, DMA Comments at 28; ANA Comments at 31; ITI Comments at 11; WISPA Comments at 20-22; ACA Comments at 36-37.

786 Access Now Comments at 2 (Nathan White); *see also* 2012 FTC Privacy Report at 7-9; 2015 Administration CPBR Discussion Draft, at § 4(g) (defining ""privacy risk" as "the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress, or physical, financial, professional, or other harm to an individual.").

787 *See, e.g.*, Access Now Comments at 13.

788 *Cf.* XO Communications Comments at 8-9 (asserting that breach notification should be sensitivity-based); State Privacy and Security Coalition Comments at 13 ("Harm exists where the unauthorized acquisition creates a material or significant risk of identity theft, fraud, or in some cases, breach of very sensitive personal information such as private medical data ..."); CenturyLink Comments at 16 ("Consumers expect that their sensitive information will be treated differently than information that is not sensitive, such as information that is readily and publicly available and thus poses no risk of identity theft or consumer harm."); AT&T July 28, 2016 *Ex Parte* at 1.

789 *See, e.g.*, CTIA Comments at 96-97 (asserting that "any privacy rules that the Commission promulgates should protect data based on their sensitivity"); CenturyLink Comments at 16.

790 *See supra* Part III.D.

791 *See, e.g.*, FBI/Secret Service Reply at 3 (explaining that information about customers can be exploited by criminal groups to steal the identities of these customer or to target them for other criminal purposes, such as to implant malicious software on their devices, to extort money from them by encrypting devices, to compromise other online account the customer maintains, or to make them the target of any number of fraudulent schemes).

792 *See, e.g.*, WTA Comments at 8-9, 17 (raising concerns about the impact on smaller providers of providing multiple notices).

793 ACA Comments at 41-42 (arguing for the superiority of a data breach notification rule that provides a "safety valve for good faith disclosures so that small providers can avoid counterproductive strict liability enforcement actions associated with inflexible and overly prescriptive regimes.").

794 *See, e.g.*, WTA Aug. 22, 2016 *Ex Parte* at 1 (explaining that its small rural local exchange carrier members typically either refrain entirely from any use of CPNI for marketing purposes or alternatively providing customers the option to opt-out of marketing upon signing up for service, and that any sharing of information typically occurs "solely between the RLEC and its affiliates that provide services to their customers or third-parties that provide services related to the provision of telecommunications services, including but not limited to billing, help-desk representatives, and installation contractors").

795 It also will depend on, among other things, the scope and magnitude of potential harm if the data were unencrypted.

796 *See, e.g.*, OTI Comments at 33 ("Customer proprietary information, such as financial details included in applications for Lifeline service, can include highly sensitive information that must be adequately protected."); American Association for Justice Comments at 7; OTI Comments at 29; Access Now Comments at 13; AT&T Comments at 85.

797 *See* American Association for Justice Comments at 7; OTI Comments at 29, 30-31 ("[C]onsumers may need to take action to protect themselves against inadvertent breaches of private information, which could harm consumers just as much as intentional breaches.").

798 American Association for Justice Comments at 7 ("Whether a data breach was intentional or inadvertent has no bearing on the severity of the breach or the amount of information that is compromised."); Access Now Comments at 12; *see also* Online Trust Alliance Comments at 4

799 *See* Paul Vixie Comments at 11 ("It is not always easy—or even possible—to determine what an intruder has accessed when a computer is breached."); *see also* OTI Comments at 29-30 (explaining that if an accidental breach is discovered, there is a possibility that a malicious breach took place as well).

800 *See, e.g.*, XO Comments at 10-11; NTCA Comments at 34; WTA Comments at 8; CTIA Comments at 11.

801 *See, e.g.*, INCOMPAS Comments at 15-16; ITTA Comments at 23; CompTIA Comments at 4; WTA Comments at 8-9; Internet Commerce Coalition Comments at 15; State Privacy and Security Coalition Comments at 17; CTIA Comments at 177-78.

802 *See, e.g.*, WTA Comments at 8-9; T-Mobile Comments at 51; State Privacy and Security Coalition Comments at 17.

803 We note that this aspect of our definition of "breach" is consistent with our prior definition. *See 2007 CPNI Order*, 22 FCC Rcd at 6978.

804 American Association for Justice Comments at 7.

805 AT&T Aug. 23, 2016 *Ex Parte* at 2.

806 ACA Comments at 35; AT&T Comments at 78; CTIA Comments at 175.

807 *See, e.g.*, Alaska Stat. § 45.48.090(7); Haw. Rev. Stat. § 487N-1; Mass. Gen. Laws ch. 93H § 1(a) (financial account/credit or debit number can be *with or without* required access codes or passwords) (emphasis added); Minn. Stat. § 325E.61(1)(e)-(f); Mont. Code Ann. § 30-14-1704(4)(b); Ohio Rev. Code Ann. § 1349.19(A)(7)(a); Okla. Stat. § 24-162(6); Utah Code Ann. § 13-44-102(3); Ark. Code § 4-110-103(7); Del. Code Ann. tit. 6 § 12B-101(4); Ky. Rev. Stat. § 365.732(1)(c)); Mich. Comp. Laws § 445.63(3)(r); Miss. Code Ann. § 75-24-29(2)(b); Nev. Rev. Stat. § 603A.040; N.H. Rev. Stat. Ann. § 359-C:19(IV); N.J. Stat. Ann. § 56:8-161(10); 73 Pa. Stat. § 2302; 11 R.I. Gen. Laws § 11-49.2-5(c); Tenn. Code App. § 47-18-2107(a)(3); Va. Code Ann. § 18.2-186.6(A); W. Va. Code § 46A-2A-101(6); D.C. Code § 28-3581(3).

808 National Consumers League Comments at 24-25 ("Breaches indicate lapses or vulnerabilities in security that companies will be forced to recognize and fix. NCL believes that an ancillary benefit of these breach notification requirements is the creation of incentives for companies to share information in order to minimize the impact for themselves and for customers." (citations omitted)).

809 FBI/Secret Service Reply at 6.

810 *Cf.* Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. § 3(a)(5) (2015) (requiring 10,000 individuals); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. § 4 (2015) (requiring 10,000 individuals); Updated Data Breach Notification 2 (2015), *in* Letter from Shaun Donovan, Dir., Office of Mgmt. & Budget, Exec. Office of the President, to the Hon. John A. Boehner, Speaker of the H.R. (Jan 13, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (OMB proposed legislation and text for the *Personal Data Breach Notification and Protection Act* to the House of Representatives and the Senate, requiring 10,000 individuals).

811 *See supra* para. 246.

812 FBI/Secret Service Reply at 5 (arguing that early notification to federal law-enforcement agencies would help assess the intrusion, secure evidence, facilitate interagency coordination, and consider whether there is a need to further delay customer notification).

813 *See, e.g.*, Letter from Jacquelyne Flemming, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Sept. 21, 2016) (AT&T Sept. 21, 2016 *Ex Parte*) (arguing that providers should be allowed an opportunity to distinguish actual breaches from merely suspicious activity or conduct); CenturyLink Comments at 43 ("Ultimately, any notification timeline should be tied initially to the determination that a breach has occurred."); *see also* S^2ERC Comments at 16 ("A clearer definition of what constitutes the ""discovery" of a breach may be necessary to aid in compliance with the timeline requirements.").

814 FBI/Secret Service Reply at 5 ("Early notification to the Federal Law Enforcement Agencies will enable law enforcement to assess the intrusion and engage meaningfully with the Service Provider when it may be possible to obtain vital evidence that could become obscured or destroyed over time. Early notification will also permit the Federal Law Enforcement Agencies to coordinate their efforts so that any law enforcement response can maximize the resources available to address and respond to the intrusion ... Another benefit of early notification to the Federal Law Enforcement Agencies is that early notice will allow law enforcement agencies sufficient opportunity to determine whether there is a need for delayed notice to customers ...").

815 *See*, *e.g.*, Hughes Comments at 7 (recommending a 30 day renewable time from for notices to the Commission and law enforcement to ease compliance); WISPA Comments at 32 ("The proposed deadlines would require notification to Federal law enforcement and customers much more quickly than nearly all state laws require such that it may be difficult for even larger providers to comply with the Commission's proposals.") (footnote omitted); INCOMPAS Comments at 14-15, 17-18; ACA Comments at 35-36, 54-55.

816 AT&T Aug. 23, 2016 *Ex Parte* at 2 (supporting a framework requiring Commission notification without unreasonable delay and within seven (7) business days as opposed to 7-10 days); AT&T July 28, 2016 *Ex Parte* at 2 (supporting business day framework for notification deadlines); *see* ViaSat Comments at 7 (proposing that BIAS providers should have ten (10) total "business" days to notify consumers, the Commission, and federal law enforcement as opposed to the "10 days" proposed in the NPRM); *but see* Online Trust Alliance May 27, 2016 *Ex Parte* at 3-4 (supporting ten (10) business day standard for customer breach notification deadline but seven (7) calendar day standard for Commission and law enforcement breach notification); Hughes Network Systems, LLC July 26, 2016 *Ex Parte* at 1-2 (supporting general 30 day requirement for data breach reporting).

817 Letter from Thomas Cohen, Attorney, Kelley Drye & Warren, LLP, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 4 (filed Oct. 5, 2016) (American Cable Association Oct. 5, 2016 *Ex Parte*) (arguing that small providers should be allowed to notify the Commission of smaller breaches at the same time that customers are notified).

818 *See, e.g.*, AT&T Aug. 23, 2016 *Ex Parte* at 2 (proposing a modified notification framework that accounts for ongoing data breach investigations stretching beyond the initial 30 day window).

819 *See* FBI/Secret Service Reply at 5.

820 *Id.*

821 *See id.* at 6.

822 *See*47 CFR § 64.2011(b)(3).

823 National Consumers League Comments at 32 (stating that this requirement "strikes the appropriate balance between customers' need to know and the ability of federal law enforcement to properly investigate the origins of the breach."); FTC Staff Comments at 33.

824 *See*Ariz. Rev. Stat. § 18-545(C); Ark. Code § 4-110-105(c); Cal. Civ. Code § 1798.82(c) (*amended by* 2015 Cal. Assem. B. 739); Conn. Gen. Stat. § 36a-701b(d); D.C. Code § 28-3852(d); Ga. Code Ann. § 10-1-912(c); Ky. Rev. Stat. § 365.732(4); La. Stat. Ann. § 51:3074(D); Me. Rev. Stat. tit. 10, § 1348(3); Minn. Stat. § 325E.61(1)(c); Mont. Code Ann. § 30-14-1704(3); Nev. Rev. Stat. § 603A.220(3); N.J. Stat. Ann. § 56:8-163(c)(2); N.Y. Gen. Bus. Law § 899-aa(4); N.D. Cent. Code § 51-30-04; 11 R.I. Gen. Laws § 11-49.3-4(b); S.C. Code Ann. § 39-1-90(C); Tex. Bus. & Com. Code Ann. § 521.053(d).

825 S^2ERC Comments at 16 ("The three-day notification delay requirement considered at the request of law enforcement is understandable but such regulations are often not in the best interest of consumers. Such delays may allow criminals to wipe out the assets of a customer using stolen PI before the customer becomes aware of the threat. Restitution following such an incident is not always complete and is rarely timely or convenient for the victims. Additionally, the delay requirement may raise the liability of BIAS providers significantly as criminals may continue to rack up damages during the waiting period. At the very least, BIAS providers should not be liable for harms that occur after a breach is reported to law enforcement — especially when these harms could have been prevented with earlier notification.").

826 FBI/Secret Service Reply at 4.

827 *See, e.g.*, ACA Comments at 56-57 (asserting that the Commission "should create a one-stop shop for Commission and law enforcement notifications to avoid the need to [*sic*] duplicative notification").

828 *See*47 CFR § 0.457.

829 *See supra* Part III.F.2.

830 *See, e.g.*, Comcast Comments at 63 (stating that "the Commission should follow other well-established breach laws and allow at least 30 days after discovery of a breach to notify consumers"); Hughes Comments at 6-7 (stating that "a more equitable solution would be to stipulate that broadband service providers must report a breach within 30 days from the discovery of that breach, with leave to extend the reporting period by 30 day increments if the broadband service provider can demonstrate that more time is needed to determine the scope of the breach, to conduct risk assessments, and to restore reasonable integrity to the network"); AT&T Aug. 23, 2016 *Ex Parte* at 2 (supporting a framework to notify affected customers without unreasonable delay and no later than 20 business days after notification to the Commission).

831 *See, e.g.*, OTI Comments at 43.

832 State Privacy and Security Coalition Comments at 14 ("When a breach or suspected breach occurs, a company's top priorities are to ascertain the nature of the event, restore the security and integrity of the affected system, and determine the scope of the incident and who was affected. Time is of the essence. A requirement to report very quickly after discovery of a breach takes important resources away from remediation and investigation."); Hughes Comments at 6-7 ("This minimal modification of the proposed rule will give time for quick action while recognizing the real time needed accurately to respond to a reported breach.").

833 *See, e.g.*, State Privacy and Security Coalition Comments at 13-14; INCOMPAS Aug. 4, 2016 *Ex Parte* at 3.

834 FBI/Secret Service Reply at 5 ("The Federal Law Enforcement Agencies are primarily concerned with breaches involving suspected criminal activity, and would support a more relaxed reporting timeline for those breaches not involving potential criminal activity.").

835 FTC Staff Comments at 33.

836 *See* ACA Comments at 54-55; Jill Joerling, Data Breach Notification Laws: An Argument For a Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J. L. & Pol'y 467, 477 (2010).

837 RWA Comments at 13.

838 ACA Comments at 34-35.

839 *See* RWA Comments at 13 (arguing for a 45-day notification timeline where state law does not mandate a specific timeline); ACA Comments at 34-35 (arguing for an "as soon as reasonably practical" standard); Letter from Rebecca Murphy Thompson, Executive Vice President and General Counsel, Competitive Carriers Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No.

16-106, at 4 (filed Oct. 19, 2016) (CCA Oct. 19, 2016 *Ex Parte*) (arguing for a 60-day customer notification timeline for small providers).

840 *See, e.g.*, AT&T Aug. 23, 2016 *Ex Parte* at 2 (proposing a modified notification framework that accounts for ongoing data breach investigations stretching beyond the initial 30 day window).

841 *See, e.g.*, AT&T July 28, 2016 *Ex Parte* at 2 ("To allow providers adequate time to identify all affected customers and prepare relevant information for them and any other relevant support such as call centers they can contact with follow-up questions, providers should be allowed up to 20 business days after making that determination to notify customers.").

842 *See, e.g.*, OTI Comments at 42; NTCA Comments at 68; *see also* Access Now Comments at 12 (asserting that remediation options should be clearly indicated and accessible in breach notices).

843 *See generally*Cal. Civ. Code § 1798.82(d) (California); Haw. Rev. Stat. § 487N-2(d) (Hawaii); 815 ILCS § 530/10(a) (Illinois); Iowa Code § 715C.2(5) (Iowa); Md. Code Com. Law § 14-3504 (Maryland); Mass. Gen. Laws § 93H-3(b) (Massachusetts); Mich. Comp. Laws § 445.72(6) (Michigan); Mo. Rev. Stat. § 407.1500.2(4) (Missouri); N.H. Rev. Stat. § 359-C:20(IV) (New Hampshire); N.Y. Gen. Bus. Law § 899-aa(7) (New York); N.C. Gen. Stat § 75-65(d) (North Carolina); Or. Rev. Stat. § 646A.605(5) (Oregon); Vt. Stat. tit. 9 § 2435(b)(5) (Vermont); Va. Code § 18.2-186.6,A (Virginia); W.V. Code § 46A-2A-102(d) (West Virginia); Wyo. Stat. § 40-12-501(e) (Wyoming); P.R. Laws tit.10 § 4053 (Puerto Rico).

844 National Consumers League Comments at 30. Several states currently require data breach notices to contain information about both credit monitoring and credit freezes. *See*Conn. Gen. Stat. § 36a-701b(b); 815 Ill. Comp. Stat § 530/10(a); Mass. Gen. Laws Ch. 93H § 3(b); 10-1-912(c); W. Va. Code § 46A-2A-102(d). *But see* FTC Staff Comments ("While contacting the national credit reporting agencies may be appropriate in certain circumstances, it may not be helpful in others and could create a false sense of security.").

845 *See, e.g.*, Cal. Civ. Code § 1798.82(d) (requiring approximate date of breach and types of personal information that were or are reasonably believed to have been subject to a breach); Fla. Stat. § 501.171(4)(f) (requiring estimated date range of breach and a description of the personal information accessed or reasonably believed to have been accessed); Iowa Code § 715C.2(5) (requiring approximate date of the breach and the type of personal information obtained as a result of the breach); N.H. Rev. Stat. Ann. § 359-C:20(IV) (requiring approximate date of breach and the type of personal information obtained as a result of the breach).

846 Several states already require this. *See*815 Ill. Comp. Stat § 530/10(a); Md. Code. Ann., Com. Law. § 14-3504(g); N.C. Gen. Stat. § 75-65(d).

847 *See*45 CFR § 164.404(d)(1) (HIPAA); N.Y. Gen. Bus. Law § 899-aa(5); Arizona Rev. Stat. § 44-7501(D); Ark. Code § 4-110-105(e); Colo. Rev. Stat. § 6-1-716(1)(c).

848 National Consumers League Comments at 29 ("In addition to a choice between written and electronic notifications required in 47 U.S.C. § 64.7006(a)(1), BIAS providers should be required to post and maintain substitute breach notifications in a clearly marked section of their websites.").

849 Some states, however, allow for substitute notice depending on the cost and number of affected individuals. *See, e.g.*, Me. Stat. tit. 10 § 1347(4)(C) ($5,000 or 1,000 residents); Mich. Comp. Laws § 445.72(12)(5)(d) ($250,000 and 500,000 residents).

850 National Consumers League Comments at 33.

851 *Id.*

852 *But see* Hughes Comments at 9 ("A six month recordkeeping requirement will ensure that customers' records are retained for a reasonable period following the termination of service and give the Commission and law enforcement agencies sufficient access to records to conduct investigations of consumer complaints.").

853 Greenlining Institute Comments at 16 ("Commenters believe that a uniform regime is not only easier for the carriers, easier of enforcement, and easier for customers to understand, it is also consistent with the Open Internet Order in terms of law and policy."); WTA Comments at 17 ("There is no reason that BIAS providers should have different customer notification requirements for breaches, particularly when many BIAS providers also provide voice and/or video service as part of a bundle. Providing more than one notice

could also cause consumer confusion and would be more burdensome and costly than simply requiring one notice per affected customer."); INCOMPAS Comments at 17-18.

854 *See supra* paras. 263, 284.

855 *See, e.g.*, Privacy Rights Clearinghouse Comments at 6 ("Under no circumstances should any consumer, especially those who are members of vulnerable communities, have to choose between their rights to privacy and foregoing broadband service."); Access Now Comments a 7 ("To ensure user protection, consent must be freely and unambiguously given. This means, for instance, that the use of a service must not be contingent on consumer approval for the sharing of personal information with third parties or for the use of information for other purposes than the one it was originally collected."); ACLU Comments at 6 (arguing that requiring customers to sign away their privacy rights as a condition of service, or certain kinds of service should be prohibited as it would "create a gaping loophole that would quickly be exploited"); NTCA Comments at 71 (stating it does "not oppose disallowing practices that enable providers to deny service if customers do not relinquish certain rights").

856 *Broadband Privacy NPRM*, 31 FCC Rcd at 2682, para. 285 (proposing to "prohibit BIAS providers from making service offers contingent on a customer surrendering his or her privacy rights").

857 *See supra* note 855; *see also* Letter from Eric G. Null, New America's Open Technology Institute, to Marlene H. Dortch, Secretary, FCC, GN Docket No 16-106 at 3 (filed Sept. 12, 2016) ("Low-income individuals often rely on a single device, meaning the single ISP used by that person has access to extensive information about the individual. Pay-for-privacy would be particularly problematic in the Lifeline context. Lifeline subscribers, who are among the most vulnerable populations, should not be forced to give up their privacy for an Internet connection.").

858 Atomite Comments at 6.

859 *See supra* Part III.A.

860 47 U.S.C. § 222(a).

861 47 U.S.C. § 222(c)(1).

862 47 U.S.C. § 201(b) (requiring that all charges, practices, classifications, and regulation for and in connection with a telecommunications service be "just and reasonable," and prohibiting "unjust and unreasonable" charges, practices, classifications, or regulations). Thus, we disagree with CTIA's assertions that the "term 'approval' must reflect the common law contract law principle that neither take-it-or-leave-it offers nor financial inducements are unconscionable." CTIA Reply at 29, n.102. Congress directed the Commission to "execute and enforce" the provisions of the Act, including the prohibition on "unjust or unreasonable" practices.

863 47 U.S.C. § 202(a) ("It shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communication service, directly or indirectly, by any means or device, or to make or give any undue or unreasonable preference or advantage to any particular person, class of persons, or locality, or to subject any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage."); *see Broadband Privacy NPRM*, 31 FCC Rcd at 2593, para. 294, 2596, paras. 305-06.

864 *2015 Open Internet Order*, 30 FCC Rcd at 5659-60, paras. 133-37.

865 *2015 Open Internet Order*, 30 FCC Rcd at 5659, para. 135. The no-unreasonable interference/disadvantage standard requires that "Any person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not unreasonably interfere with or unreasonably disadvantage (i) end users' ability to select, access, and use broadband Internet access service or the lawful Internet content, applications, services, or devices of their choice, or (ii) edge providers' ability to make lawful content, applications, services, or devices available to end users. Reasonable network management shall not be considered a violation of this rule." *Id.* at 5609, para. 21. *See also*47 CFR § 8.11, No unreasonable interference or unreasonable disadvantage standard for Internet conduct.

866 *See, e.g.*, AT&T Comments at 59 ("Banning discounts in exchange for information-sharing would, by definition, increase the price and lower the output of any affected service, including broadband Internet access."); ADTRAN Comments at 12 (arguing that financial incentive "business models of providing discounts in return for access to consumers' proprietary information have been well-received

by consumers both in the bricks-and-mortar world, as well as specifically in the provision of BIAS services where they have been offered as an option"); CDT Comments at 3 (asserting that BIAS providers should have flexibility under the rules to encourage customer opt-in, "including offering monetary rewards in exchange for customer opt-in"); CenturyLink Comments at 30 (stating that "any outright prohibition adopted by the Commission would disserve consumers, who might miss out on services they want and value propositions they appreciate"); Free State Foundation Comments at 9 (arguing a ban on financial incentives would "deprive consumers of their choice to enjoy free or ... inexpensive services and applications"); NTCA Comments at 71-72 ("Providers should have the flexibility, within the boundaries of notice, choice and security, to offer consumers packages that meet their needs."); Cincinnati Bell Comments at 10 ("Once the basic privacy requirements are established on such a basis, the Commission should not prohibit BIAS providers from offering enhanced levels of security for customers who are willing to pay the extra cost that is necessary to support such services."); Sprint Comments at 20-21; T-Mobile Comments at 44; Comcast Reply at 18-19; CTIA Aug. 25, 2016 *Ex Parte* at 2-3 (arguing that financial incentives "can lead to significant cost savings for all consumers, enable more valuable services for consumers, and mirror much of the economic activity that consumers expect"); *see also id.* Attach., ITIF White Paper, Why Broadband Discounts for Data are Pro-Consumer.

867 *See, e.g.*, Consumer Watchdog Comments at 6 (arguing that "'pay-for-privacy' polices can rapidly become coercive and predatory, especially when applied to lower-income subscribers"); Consumer Action Comments at 2 (urging the Commission "to do everything in its power to ensure that companies don't snare consumers to wittingly or unwittingly give up their privacy rights in exchange for free services or devices"); EFF Comments at 9 (expressing concern that financial incentive practices "are prone to abuse"); EPIC Comments at 25-26; OTI Comments at 45 (explaining that financial incentive "programs are concerning because they could be crafted to induce or, worse, coerce customers into giving up privacy protections all so BIAS providers can further develop their advertising businesses"); California AG Comments at 4 ("Consumers *pay* their ISPs for their Internet connection; they do not and should not be expected to also 'pay' with their personal information as well"); Common Sense Kids Action Comments at 14 (emphasizing that "[p]rivacy should not be a privilege reserved for those with time, money, and technical expertise"); Letter from Ariel Fox Johnson, Senior Policy Counsel, Common Sense Kids Action, to Marlene H. Dortch, Secretary, FCC, WC 16-106, at 1 (filed Sept. 9, 2016); Color of Change Oct. 20, 2016 *Ex Parte* at 5.

868 We limit the heightened disclosure and consent requirements discussed herein to financial incentive practices offered by BIAS providers. The record reveals concerns about these practices specific to BIAS, and as such, we limit our requirements to such services.

869 *Broadband Privacy NPRM*, 31 FCC Rcd at 2581, para. 258; Consumers' Research Comments at 8 (stating that many consumers exchange financial incentives for consent, "based on their own preferences").

870 *See* TPI Comments, Attach., Thomas Lenard and Scott Wallsten White Paper, An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking at 35-36 (discussing Freedompop, which allows subscribers to earn additional broadband capacity, voice minutes, or text messages by performing specified actions with their third party advertisers (e.g., completing a questionnaire or purchasing a product or service); *see also* Chantal Tode, Flyers on United, American can now exchange location data for miles, Mobile Marketer (Aug. 22, 2016), http://www.mobilemarketer.com/cms/news/database-crm/23473.html.

871 *See supra* note 866.

872 MMTC et al. Comments at 8; *see also* APPI Comments at 3 ("If the Commission were to prohibit financial inducements that were designed to support low-income broadband adoption, more vulnerable AAPI consumers would be deterred from online use.").

873 *See supra* note 867.

874 CFC Comments at 9.

875 ACLU Comments 6 (asserting that "the underprivileged (and disproportionately minority) population that lacks the discretionary income to devote to privacy will lose a right available for purchase by more affluent Americans"); NBCSL Comments at 1 (expressing concern about financial incentive practices for "people of color and low income consumers" because they "face particular risks to their privacy from companies that offer free or low cost services that actually come at the cost of giving up control of personal data"); Public Knowledge et al. Comments at 2 ("In households with low income elasticity, even moderate price discrimination between privacy and no-privacy offerings can become coercive inducements. Such inducements could force low-income consumers to choose between exercising their privacy rights, and having a broadband connection at all.").

876 Letter from Access Humboldt, et al. to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106 at 5 (filed Sept. 7, 2016), citing Karl Bode, *Think Tank Argues that Giving up Privacy is Good for the Poor*, Techdirt (Aug. 18, 2016), https://www.techdirt.com/articles/20160816/07164935254/think-tank-argues-that-giving-up-privacy-is-good-poor.shtml) ("AT&T charges its U-Verse broadband customers $528 to $792 more every year (up to $62 more per month) to opt out of the company's Internet Preferences program, which uses deep packet inspection to track your online behavior — down to the second. Not only is that not anything close to a discount, but AT&T makes opting out as cumbersome as possible.")).

877 CDT Comments at 3 ("However, because such inducements to consent raise serious public policy concerns, these programs must be transparent and must not be coercive."); *see also* CenturyLink Comments at 30 (arguing the Commission should allow "properly informed customers" to "voluntarily [] enter contracts for lower monthly rates or to accept other financial inducements in exchange for their consent to the use and/or sharing of their information"); Letter from Jon Leibowitz to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed May 10, 2016) ("So long as broadband providers provide sufficient notice, consumers [] have the ability to make informed choices about how they value their personal data."); Greenlining Institute Comments at 14 ("There is nothing wrong with a consumer, after being fully informed, choosing to trade access to his or her personal data in return for enhanced services."); MMTC et al. Comments at 8 (arguing that "financial inducement programs that require informed consent should not be seen as presumptively coercive").

878 Notices that contain material misrepresentations or omissions will not be considered accurate.

879 CDT Comments at 25.

880 *See supra* Part III.C.

881 We observe that BIAS providers are already requiring opt-in consent for financial incentive programs. *See* U-verse with AT&T GigaPower Internet Preferences, AT&T, https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1011211 (last visited Sept. 12, 2016) (website has been taken down); *see also* Adria Tomaszewski, *Verizon Smart Rewards Gives Back to Wireless Customers* (July 21, 2014), http://www.verizonwireless.com/news/article/2014/07/smart-rewards-gives-back-to-wireless-customers.html?null ("Customers may be required to enroll in Verizon Selects, part of Precision Market Insights from Verizon, as part of the Smart Rewards registration process and will receive 2,500 bonus points for being part of Verizon Selects and 500 Rewards points per participating line each month."); Torod Neptune, *How Verizon Selects from Verizon Wireless Works* (Dec. 3, 2012), http://www.verizonwireless.com/news/article/2012/12/verizon-selects.html ("We are asking customers to opt-in to Verizon Selects because of the types of information being used and because the capabilities provided to third-party marketers gives them the ability to reach customers directly with more relevant infomation[[*sic*].").

882 Mobile Futures Comments at 7 ("The FCC should not adopt paternalistic rules that deprive consumers of the choice to voluntarily share personal information in exchange for benefits."); Comcast Comments at 58 (arguing that the Commission should not take a "paternalistic view of 'consumers' ability to make informed choices"); Public Knowledge White Paper at 64 ("Congress clearly intended that consumers should have control of their own information.").

883 *Broadband Privacy NPRM*, 31 FCC Rcd at 2586-88, paras. 273-75.

884 *See*47 U.S.C. § 208; 47 CFR §§ 1.716 to 1.719; FCC, Consumer Help Center, https://consumercomplaints.fcc.gov/hc/en-us (last visited Oct. 5, 2016); *GS Texas Ventures, LLC*, Order, 29 FCC Rcd 10541, 10543, para. 6 (WCB 2014) (invalidating an arbitration clause precluding formal complaints to the Commission); Letter from National Association of Consumer Advocates (NACA), Public Justice, Public Citizen, Public Knowledge, AAJ, and Consumers Union to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Sept. 21, 2016) (discussing need to protect the Commission's complaint procedures from contractual waivers); *see also 2015 Open Internet Order*, 30 FCC Rcd at 5718, para. 267 n.687 (permitting mandatory third-party arbitration "so long as it is subject to *de novo* review by the Commission").

885 *See* OTI Comments at 47 ("[T]he FCC should ensure that there is an easy and clear process for consumer complaints at the FCC."); WISPA Comments at 34-36.

886 *See* AAJ Comments at 1-3, 6; Consumer Federation of California Comments at 12; Consumers Union Reply at 6; EPIC Comments at 27; NACA, Public Citizen, and 22 Other Public Interest Organizations Comments at 2-8; OTI Comments at 46; Privacy Rights Clearinghouse Comments at 7; Letter from Dallas Harris, Policy Fellow, Public Knowledge to Marlene H. Dortch, Secretary, FCC,

WC Docket No. 16-106, at 1 (filed Aug. 3, 2016); Smithwick & Belendiuk, P.C. Comments 1-11. *See also* Letter from 38 Public Interest Organizations to Chairman Tom Wheeler, Sept. 7, 2016, at 4-5.

887 *See* AT&T Comments at 114-15; Comcast Reply at 53-55; Consumers' Research Comments at 5-6; CTIA Comments at 50-59; ITTA Comments at 24-25; NCTA Reply at 64-65; Sprint Comments at 20-21; T-Mobile Comments at 55; Verizon Reply at 38-45.

888 *See* CFPB, Arbitration Agreements, 81 Fed. Reg. 32830 (May 24, 2016); *Arbitration Study*, CFPB (Mar. 10, 2015), http://www.consumerfinance.gov/data-research/research-reports/arbitration-study-report-to-congress-2015/. *See also* Consumer Federation of California Comments at 12 (discussing the CFPB report); CTIA Comments at 54 (same); AAJ Comments at 4-5 (discussing the CFPB's report and NPRM).

889 *See*47 U.S.C. § 222; *see also* Level 3 Comments at 5 (noting that even with an enterprise exemption, the Commission would retain the power to evaluate providers' compliance with Section 222 and to bring enforcement actions where necessary); *2007 CPNI Order*, 22 FCC Rcd at 6942-43, para. 25.

890 *See*47 CFR § 64.2010(g).

891 *See 2007 CPNI Order*, 22 FCC Rcd at 6943, para. 25 (determining that carriers who contract with enterprise customers need not comply with the Commission's carrier authentication rules so long as the carrier's contracts with its business customers (1) are serviced by dedicated account representatives as the primary contacts, and (2) specifically address the carrier's protection of CPNI).

892 *See id.*

893 Level 3 Comments at 3; *see also* XO Comments at 5 (noting that the business customers it serves negotiate service-level agreements with various privacy and data protection provisions based on individual customer needs).

894 *See* Level 3 Comments at 4 (stating that, because enterprise service is not personal service, "end users in the enterprise context do not have the same expectation of privacy in the use of the service and are not expected to risk exposing private information the way individual, mass-market consumers using their personal phones might"); Verizon Comments at 63 (noting that the Commission has "sensibly recognized that the privacy rules that apply to consumers may not make sense for businesses"); Letter from Nicholas G. Alexander, Associate General Counsel, Federal Affairs, Level 3 Communications, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 1 (filed Aug. 5, 2016) (Level 3 Aug. 5, 2016 *Ex Parte*); *see also* XO Comments at 3.

895 Verizon Comments at 63; *see al*so Verizon Oct. 13, 2016 *Ex Parte* at 1 (arguing the Commission should allow "business customers to bind themselves to alternative privacy and data security regimes as their privacy and data security needs may differ from those of consumers.").

896 Level 3 Aug. 5, 2016 *Ex Parte* at 1.

897 INCOMPAS et al. Aug. 4, 2016 *Ex Parte* at 2.

898 *See*47 CFR § 64.2010(g); *2007 CPNI Order*, 22 FCC Rcd at 6943-44, para. 25.

899 *See* Christopher L. Shipley, Attorney & Policy Advisor, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 21, 2016) (INCOMPAS Oct. 21, 2016 *Ex Parte*).

900 *See* Level 3 Aug. 5, 2016 *Ex Parte* at 1 ("[W]e agreed that it would be reasonable for the Commission to adopt a general rule that requires carriers to address customer choice, transparency, data security, and data breach notification when selling to business customers so long as that rule does not specify how carriers are obligated to meet that requirement.").

901 *See* INCOMPAS et al. Aug. 4, 2016 *Ex Parte* at 1 (stating that the *Notice* "asserts that BIAS is a mass market retail service and that proposed rules would apply only to mass market customer relationships" and that the Commission should "adopt the same approach in the context of" voice services).

902 We clarify that the contract at issue need not be a fully negotiated agreement, but can take the shape of standard order forms. *See* INCOMPAS Oct. 21, 2016 *Ex Parte* at 2.

903 *See* XO Comments at 5.

904 *See* INCOMPAS et al. Aug. 4, 2016 *Ex Parte* at 1; *see also* Level 3 Comments at 5 (stating that, under the strictures of Section 222, enterprise service providers would still be required to protect customer information, limit their use of carrier information and protect its confidentiality, and obtain customer approval — or infer customer approval when it is clearly warranted under the circumstances — before using, disclosing, or permitting access to CPNI for any reason other than providing voice services, or services necessary to or used in the provision of voice service, unless a statutory exemption applies).

905 *See* Verizon Sept. 23, 2016 *Ex Parte* at 1; *see also* T-Mobile Sept. 13, 2016 *Ex Parte* at 1.

906 PRA approval, as defined herein, is not complete until the Commission publishes notice of OMB approval in the Federal Register.

907 *See infra* Appx. A, 47 CFR §§ 64.2003-64.2005. This implementation schedule also applies to the disclosure and consent requirements for financial incentive practices. *See id.*, § 64.2011(b).

908 T-Mobile Sept. 13, 2016 *Ex Parte* at 1.

909 *See id.* at 2, n.1; *see also* Verizon Sept. 23, 2016 *Ex Parte* at 1.

910 *See infra* Appx. A, 47 CFR § 64.2008.

911 47 CFR § 64.2011.

912 *See TerraCom NAL*, 29 FCC Rcd at 13339-41, paras. 39-44.

913 *See supra* Part III.F.1.

914 *See infra* Appx. A, 47 CFR § 64.2007.

915 *See supra* Part III.E; *see also*15 U.S.C. § 45.

916 *See, e.g.*, T-Mobile Sept. 13, 2016 *Ex Parte* at 1 (asking the Commission to consider "a 12-18 month implementation time period after rules are adopted"); *see also* T-Mobile Oct. 14, 2016 *Ex Parte*, Attach. at 3; Verizon Sept. 23, 2016 *Ex Parte* at 1 (arguing that the implementation steps "will take a significant amount of time to complete, requiring approximately 18 months from the date rules are adopted"); Verizon Oct. 13, 2016 *Ex Parte* at 1.

917 *See infra* Appx. A, 47 CFR § 64.2011(a).

918 *See supra* Part III.G.1.

919 *See supra* Part III.C.5 (explaining the benefits of harmonization, including consistency between privacy regimes for all telecommunications services, both to reduce possible consumer confusion, and to decrease compliance burdens for all affected telecommunications carriers, particularly small providers).

920 *See Enf. Bur. Privacy Advisory*, 30 FCC Rcd 4849 (2015).

921 *See infra* Appx. A, 47 CFR § 64.2004.

922 *See supra* Part III.D.1.

923 *See* WISPA Comments at 31 (arguing it should not "not be compelled to obtain new consents ...from its customers."); ACA Comments at 45; CCA Comments at 33; NTCA Comments at 55; USTelecom Comments at 19.

924 *See infra* Appx. A, 47 CFR § 64.2004 (c) ("A telecommunications carrier must make available a simple, easy-to-access method for customers to provide or withdraw consent at any time. Such method must be clearly disclosed, persistently available, and made available at no additional cost to the customer. The customer's action must be given effect promptly after the decision to provide or withdraw consent is communicated to the carrier.").

925 *See* USTelecom Comments at 19 ("[W]e support allowing small providers who have already obtained customer approval to use their customers' proprietary information to grandfather in those approvals for first and third party uses."). WTA argues that the Commission should permit "small BIAS providers to grandfather existing opt-out approvals as it has done in the past" citing the Commission's *2002 CPNI Order*, in which the Commission allowed carriers to use preexisting opt-out approval with the limitation that such approval only be used for marketing of communications-related services by carriers, their affiliates that provide communications-related services, and carriers' agents, joint venture partners and independent contractors. *See* Letter from Patricia Cave, Director, Government Affairs, WTA, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106 at 2 (filed Aug. 22, 2016); *see also 2002 CPNI Order*, 17 FCC Rcd at 14897, para. 85.

926 *See*47 CFR § 64.2008(a)(2).

927 *See, e.g.*, CTA Comments at 11 (expressing concern that certain Commission proposals would induce notice fatigue); *see also* INCOMPAS Comments at 10 (arguing that notice fatigue will lessen the effectiveness of consumer notices).

928 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2553, para. 151.

929 *See supra* Part III.C.5 (explaining that harmonizing our BIAS and voice definitions under Section 222 will simplify compliance for small providers who collect less customer information, use it for narrower purposes, and do not have the resources to maintain a bifurcated system); *see also supra* para. 14357 (eliminating the pre-existing every-two-year notice requirement from our Section 222 rules to reduce burdens smaller carriers); *supra* Part III.C.3 (declining to require a standardized format of privacy notices as it would decrease flexibility for small carriers); *id.* (only requiring providers to convey their notices of privacy policies to customers in another language, if the customer transacts business with the BIAS provider or other telecommunications carrier in that other language so as not to overburden small providers); *id.* (directing the CAC to develop a safe harbor standardized form, to be used by small providers if they choose so they can easily adopt a compliant form and format for their notices); *supra* para. 241 (clarifying that the data security standard is one of "reasonableness" rather than strict liability and establishing a non-exhaustive rather than prescriptive list of reasonable data security to allow easier compliance for small providers); *supra* Part III.F.1 (employing a harm-based trigger or data breaches to substantially reduce the burdens of smaller providers in reporting breaches of customer PI); *supra* Part III.F.3.a (changing the timeline for notifying customers of a data breach from 7-days to 30-days to allow more time for small providers to comply).

930 CCA asserts that "any compliance burdens produced by privacy rules will be compounded by many additional regulations including Title II regulation, enhanced transparency rules, and outage reporting requirements." *See* CCA Oct. 13, 2016 *Ex Parte* at 2. Consideration of the effect of separate requirements was taken into account in developing this implementation plan.

931 *See* CCA Reply Comments at 40-41 (advocating for 24-month extension after effective date of new privacy rules); *see also* WISPA Comments at 28-29 (same).

932 *See* WISPA Comments at 28 ("This additional time will enable small providers to assess their obligations, budget for lawyers, consultants, train personnel, and establish internal systems to ensure compliance.") *see also* ACA Comments at 8 (arguing that "very few of these [small] providers have in-house technical or compliance personnel with extensive expertise in privacy and data security compliance. Some are forced to outsource some of their security functions to outside vendors at a significant cost").

933 NTCA Oct. 14, 2016 *Ex Parte* at 4.

934 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2553, para. 151.

935 *See, e.g.*, CCA Reply at 40-41 (advocating for 24-month extension after effective date of new privacy rules); WISPA Comments at 28-29 (same); U.S. Small Business Administration Reply at 4 (same); ACA Comments at 46 (arguing the Commission "should extend the effective dates for small providers to comply with any new privacy and data security rules by at least one year beyond any general compliance deadline"); RWA Comments at 4 (explaining that "certain customer information is shared with billing system vendors, workforce management system vendors, consultants that assist with certain projects, help desk providers, and system monitoring solutions providers").

936 *See supra* Part III.D.2.a.

937 *See 2015 Open Internet Order*, 30 FCC Rcd at 5677-78, para. 172; *see also Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order, 30 FCC Rcd 14162, 14166-67, para. 10 (CGB Dec. 15, 2015) (*Small BIAS Provider Transparency*

Extension Order) (maintaining the 100,000 threshold for the small business extension as it "remains a reasonable basis to delineate which providers are likely to be most affected by the burden of complying with the enhanced disclosure requirements."); *Rural Call Completion*, WC Docket No. 13-39, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 16154, 16168-69, para. 27 (2013) (exempting smaller providers from the recording, retention, and reporting rules if they provide long-distance voice service that make the initial long-distance call path choice for less than 100,000 domestic retail subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the providers' affiliates)); RWA Reply at 5 (supporting the 100,000 threshold established in the *2015 Open Internet Order*).

938 *See* CCA Oct. 13, 2016 *Ex Parte* at 1-2; *see also Small BIAS Provider Transparency Extension Order*, 30 FCC Rcd at 141266, para. 10 (declining to broaden the small provider threshold, as it would "substantially increase the number of consumers who would be temporarily excluded from receiving the information that the Commission has deemed essential for them to make informed choices about broadband services.").

939 *See* WISPA Comments at 27-28 (seeking a two-year extension for all the Commission rules); CCA Reply at 40 ("If the Commission declines to adopt a small provider exemption ... CCA urges the Commission to allot those providers an extension of time to comply with new regulations."); RWA Reply at 7 ("If the Commission declines to adopt these broader exemptions, RWA urges the adoption of a 24-month extended compliance deadline for small providers.").

940 *See supra* Part III.E.1; *see also* WTA & Nex-Tech Apr. 25, 2016 *Ex Parte* at 2 (explaining how such data security proposals would unduly burden small carriers).

941 *See supra* Part III.D.1 *see also supra* para. 230.

942 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2511, 2588 paras. 27, 276. State law includes any statute, regulation, order, interpretation, or other state action with the force of law.

943 *See 1998 CPNI Order*, 13 FCC Rcd at 8075, para. 16 ("We conclude that, in connection with CPNI regulation, the Commission may preempt state regulation of intrastate telecommunications matters where such regulation would negate the Commission's exercise of its lawful authority ...."); *2002 CPNI Order*, 17 FCC Rcd at 14890-91, para. 70 ("Should states adopt CPNI requirements that are more restrictive than those adopted by the Commission, we decline to apply any presumption that such requirements would be vulnerable to preemption.").

944 *See 2002 CPNI Order*, 17 FCC Rcd at 14891, para. 71 (observing that "our state counterparts ... bring particular expertise to the table regarding competitive conditions and consumer protection issues in their jurisdictions, and privacy regulation, as part of general consumer protection, is not a uniquely federal matter"); *2007 CPNI Order*, 22 FCC Rcd at 6958, para. 60.

945 Letter from Kathleen McGee, Chief, Bureau of Internet and Technology, New York Attorney General, to Chairman Tom Wheeler, FCC, WC Docket No. 16-106 at 4 (filed June 30, 2016) (NY Attorney General *Ex Parte*); *see also* Letter from Bill Schuette, Michigan State Attorney General, et al., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 1 (filed Sept. 15, 2016) ("As Attorneys General, we are always concerned with protecting consumers' privacy and defending the protections our consumers have been afforded via our various state laws. It is of paramount importance that any federal regulations not impair states' ability to vigorously protect their citizens as they deem appropriate."); Letter from Karl A. Racine, District of Columbia Attorney General, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 1 (filed Oct. 12, 2016).

946 NY Attorney General *Ex Parte* at 4; *see also* California Office of Attorney General Reply at 2; PA PUC Reply at 4 (arguing that the Commission "should not preclude state authorities from developing privacy standards based upon independent state law so long as those standards do not unduly burden interstate commerce and advance a compelling state interest"); Greenlining Institute Comments at 51 (explaining that "neither federal nor state agencies have sufficient resources to fully protect consumers, and it is important that "cooperative federalism' be maintained in this vital area").

947 *See, e.g.*, Hughes Comments at 7 ("Hughes also supports the FCC preempting state privacy laws to the extent that they are inconsistent with any rules adopted by the Commission."); ViaSat Comments at 7 (agreeing with our adopted method, by stating for example, "that the Commission make clear that any data breach notification requirements adopted in this proceeding preempt all *inconsistent* state requirements") (emphasis added); CTIA Comments at 183 (arguing that the Commission should be clear "about the extent to which it would preempt state law requirements" so providers can avoid having to address conflicting state and federal notice requirements).

948 *1998 CPNI Order*, 13 FCC Rcd at 8075-76, para. 16; *see also 2002 CPNI Order*, 17 FCC Rcd at 14890, para. 69. We reject ITTA's argument that we lack authority to preempt inconsistent state laws regarding non-CPNI customer PI because its argument is premised on the incorrect assumption that our legal authority under Section 222 is limited to CPNI. *See infra* Part IV.A.2 (concluding that the Commission has authority to reach customer PI under Section 222(a) of the Act); *contra* Letter from Michael J. Jacobs, Vice President Regulatory Affairs, ITTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed Aug. 9, 2016) ("State Attorneys General, furthermore, have jurisdiction ... to enforce their own privacy and unfair practice laws, which the FCC would not be empowered to preempt in light of its own lack of statutory authority regarding non-CPNI consumer information.").

949 The Commission reviews petitions for preemption of CPNI rules on a case-by-case basis. *See 2002 CPNI Order*, 17 FCC Rcd at 14893, para. 74 ("By reviewing requests for preemption on a case-by-case basis, we will be able to make preemption decisions based on the factual circumstances as they exist at the time and on a full and a complete record."); *see also id.* at 14890-93, paras. 69-74 (recognizing the potential burdens associated with different regulatory requirements); ViaSat Comments at 8 (expressing concern about being subject to "a potentially confusing patchwork of conflicting breach notification requirements at the state level").

950 *See, e.g.*, California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22577(a); California Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code § 22947.1(k); Cal. Civ. Code § 1798.82(h); Conn. Gen. Stat. § 36a-701b(a); N.Y. Gen. Bus. L. §§ 899-aa(1)(a), (b); La. Stat. § 51:3073(4); Fla. Stat. § 501.171(1)(g).

951 PA PUC Reply at 2.

952 *See, e.g.*, NY Attorney General *Ex Parte* at 4; *see also* National Consumers League Comments at 33-34 (stating our approach "will ensure that States will be able to continue to innovate in protecting consumers' data, set a high bar for consumer protection, and help to clarify the baseline that BIAS providers must adhere to").

953 *See 2002 CPNI Order*, 17 FCC Rcd at 14890-92, paras. 69-71; *see also Broadband Privacy NPRM*, 31 FCC Rcd at 2588, para. 277.

954 ACA Comments at 56-57; *see also* ACA Reply at 5.

955 *See supra* note 946.

956 State Privacy and Security Coalition Comments at 5 (arguing that "requiring notification in many situations that involve no risk of harm makes "notice fatigue' more likely with consumers ignoring notice of serious breaches that actually create risk"); *see also* ACA Comments at 57 ("By reducing the number of government-level notifications that BIAS providers must make from over 50 notifications to a single notification, the Commission will significantly reduce the costs that BIAS providers must assume in the event of a breach while preserving the benefits of notifications to the customer.").

957 *See* National Consumers League Comments at 34 (explaining that "[i]t is NCL's hope that the robust and comprehensive data security and breach notification set out by the FCC will also serve as a model for other states and agencies").

958 CTIA Comments at 183-84 (asking "would the Commission's [] rule for notice to customers trump that request?").

959 *See* 47 U.S.C. § 1.3; *see also WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969) (waivers must show a deviation will serve the public interest).

960 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2602-03, para. 3; 47 CFR § 64.2011.

961 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2610, para. 4 (adding § 64.7007 Effect on State Law to new Subpart GG); *see also infra* Appx. A § 64.2012.

962 *See* ACA Comments at 57 (supporting the creation of "a single privacy and data security framework for providers of multiple services as a means of reducing compliance burdens and consumer confusion"); *see also* WTA Reply at 19 (arguing that in complying with state and federal privacy regulations, "'[p] articularly for small providers, '[i]nevitability of parallel enforcement underscores the need for harmonization"').

963 *See* 47 CFR Subpt. U; *see also Broadband Privacy NPRM*, 31 FCC Rcd at 2603-2610.

964 47 U.S.C. § 222; *see also*47 U.S.C. § 201(b) ("The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter.").

965 *See*47 U.S.C. § 222(a). The provision reads in full: "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier." *Id.*

966 47 U.S.C. § 222(c) (emphasis added).

967 *See 2015 Open Internet Order*, 30 FCC Rcd at 5820, para. 462.

968 *See, e.g.*, Comcast Comments at 67-68; NCTA Comments at 7-13; CTIA Comments at 19-22; USTelecom Comments at 28; U.S. Chamber of Commerce Comments at 4. *But see* Free Press Comments at 9 ("The logic for applying Section 222 to broadband is inexorable."); OTI Reply at 3-5; Free Press Reply at 5-7.

969 *See 2015 Open Internet Order*, 30 FCC Rcd at 5615, para. 47; *see also USTA v. FCC*, 825 F.3d 674 (D.C. Cir. 2016) (upholding the *2015 Open Internet Order* in full).

970 *See* OTI Reply at 4 ("It is presumed that use of a defined term retains its definition unless there is proof otherwise.").

971 *See, e.g.*, NCTA Comments at 13; Comcast Comments at 68.

972 *See*47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty ..."), (c) ("[A] telecommunications carrier that receives or obtains ...").

973 *See 2015 Open Internet Order*, 30 FCC Rcd at 5615, para. 47.

974 *See USTA v. FCC*, 825 F.3d at 702-03 (rejecting petitioners' Section 230-based argument against reclassification of BIAS as a telecommunications service). *But see* Comcast Comments at 67.

975 *But see* Comcast Comments at 67.

976 *See, e.g.*, 47 U.S.C. § 222(c)(3) (imposing a sharing condition on ""local exchange carrier[s]", but not on other telecommunications carriers, in their use and disclosure of "aggregate customer information").

977 We need not and do not construe BIAS as a "local exchange service," ""telephone exchange service," or "telephone toll service" in order to bring it within the reach of Section 222. Provisions of the statute that apply only to such limited categories, or to carriers that provide services in such categories, are not part of the statutory basis for any rules we adopt in this Report and Order as to BIAS. Rather, the rules we adopt for BIAS are rooted only in those aspects of Section 222 that govern "telecommunications carriers" and "telecommunications services" writ large.

978 *See*47 U.S.C. § 222(h)(1)(B).

979 *See*47 U.S.C. § 222(h)(1), (h)(3).

980 *See*47 U.S.C. § 222(h)(1)(A)-(B). Under 47 U.S.C. § 222(h)(1)(A), CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" other than subscriber list information.

981 *See supra* Part III.B.3.

982 *See*47 U.S.C. § 222(d)(3) (carving out an exception that permits the use or disclosure of CPNI for the provision of "any inbound telemarketing, referral or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of the use of such information to provide such service"). *But see* CTIA Comments at 16.

983 47 U.S.C. § 222(c)(3).

984 *See generally*47 U.S.C. §§ 251-261 ("Development of Competitive Markets"), §§ 271-276 ("Special Provisions Concerning Bell Operating Companies").

985 *See*47 U.S.C. § 222(c)(3). *But see* NCTA Comments at 9, n.13.

986 *See supra* Part III.B.4.

987 *See*H.R. Rep. No. 104-204, at 89 ("LECs have total control over subscriber list information .... Section 222 ensures that independent directory publishers have access to subscriber listing information gathered by all LECs.").

988 *See*47 U.S.C. § 222(e) (requiring the provision of subscriber list information "for the purpose of publishing directories in any format").

989 New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283 (2008). *See* CTIA Comments at 18; USTelecom Comments at 29.

990 *See*H.R. Rep. No. 110-442, at 7 (2007) ("Section 222 includes exceptions to its protections to allow wireline and wireless carriers to provide customer information to PSAPs in emergency situations. There is no similar provision governing or granting exceptions for VoIP service. H.R. 3403 would amend section 222 to add VoIP 911 service to the established 911 exceptions.").

991 We have exercised our ancillary jurisdiction to apply rules adopted under Section 222 to providers of interconnected VoIP services. *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59; *see also*47 CFR § 64.2003(o) (defining "telecommunications carrier or carrier" for purposes of the CPNI rules to include interconnected VoIP providers).

992 *See*47 U.S.C. § 222(a).

993 *See infra* Part IV.A.2.a; *see also* Free Press Reply at 7-8 (arguing that CTIA "counsels the Commission against 'atomistic interpretation of Section 222(a)'" while at the same time urging the Commission to "ignore the entirety of the statute in favor of focusing on 'atomistic' references to telephone and voice services").

994 *See, e.g.*, CTIA Comments at 23 ("The Commission implicitly acknowledged Section 222's inapplicability to ISPs' provision of broadband service by forbearing from applying its CPNI rules in the *Open Internet Order*.") (capitalization omitted).

995 *2015 Open Internet Order*, 30 FCC Rcd at 5820, para. 462.

996 *See USTA v. FCC*, 825 F.3d 674 (upholding the *2015 Open Internet Order* in its entirety). Insofar as any commenter in this proceeding requests reconsideration of the classification decision in the *2015 Open Internet Order*, the request is untimely. *See*47 CFR §§ 1.106, 1.429.

997 *See*47 U.S.C. § 222(a).

998 *See* Black's Law Dictionary 615 (10th ed. 2014) (defining a "duty" as "[a] legal obligation that is owed or due to another and that needs to be satisfied; that which one is bound to do, and for which somebody else has a corresponding right").

999 *AT&T Corp. v. Iowa Utils. Bd.*, 525 U.S. 366, 378 (1999) (holding that the last sentence in Section 201(b) "means what it says: The FCC has rulemaking authority to carry out the 'provisions of this Act,'" including provisions added by the Telecommunications Act of 1996); *1998 CPNI Order*, 13 FCC Rcd at 8073-74, para. 14; *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27 n.94 ("Section 201(b) authorizes the Commission to 'prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act,' including section 222."). *But see* USTelecom Comments at 29-30 ("But, unlike several other provisions that include an enforceable mandate for which the Commission has direct authority to create governing regulations, subsection (a) merely sets forth a duty without granting authority to the Commission to further define or enforce that duty.") (internal citation omitted).

1000 *See*47 U.S.C. § 222(a).

1001 *See id.*

1002 *But see* CTIA Comments at 24 ("The term 'customer proprietary information' appears nowhere in the Communications Act, and the Commission lacks authority to create it ...").

1003 *See Morales v. TransWorld Airlines*, 504 U.S. 374, 383-84 (1992).

1004 *See* EFF Comments at 2; OTI Comments at 18-19; Free Press Reply at 8.

1005 *See*47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, *equipment manufacturers* ...") (emphasis added).

1006 We reject any argument that the reference in Section 222(a) to equipment manufacturers is nothing more than a cross-reference to obligations contained in Section 273. Such an interpretation would give no independent meaning to Section 222(a), and therefore would be inconsistent with established principles of statutory construction. It would also be contrary to the plain meaning of Section 222(a), which contains no reference to and is plainly broader than Section 273; nothing in Section 273 applies broadly to every telecommunications carrier, as Section 222(a) clearly does.

1007 *Compare*47 U.S.C. § 222(a) (titled "In General" and beginning "Every telecommunications carrier has a duty ...") (capitalization omitted) *with*47 U.S.C. § 251(a) (titled "General Duty of Telecommunications Carriers" and beginning "Each telecommunications carrier has the duty ...") (capitalization omitted). Also, like in Section 222, the "general duty" announced in subsection (a) of Section 251 is accompanied by more specific duties announced in the subsections that follow. *See*47 U.S.C. § 251(b) (""Obligations of All Local Exchange Carriers") (capitalization omitted), (c) (""Additional Obligations of Incumbent Local Exchange Carriers") (capitalization omitted).

1008 *See* Free Press Comments at 10 ("Section 222 begins with a general duty for telecommunications carriers to protect the 'proprietary information' of customers. Subsections of 222 further elaborate on, but do not narrow the scope of that general duty to protect privacy."). *But see* CenturyLink Comments at 14 (arguing that "Section 222(a) sets forth the general objective of the provision" while "[t]he specifics are then supplied by the following subsections"); T-Mobile Comments at 17 (arguing "Section 222(a) is nothing more than a general introductory provision"); Washington Legal Foundation Comments at 5.

1009 Letter From Scott Bergmann, Vice President, Regulatory Affairs, CTIA, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106 at 8 (filed Sept. 16, 2016) (CTIA Sept. 16, 2016 *Ex Parte*).

1010 *But see id.* (arguing that Section 222(a) "lacks the regulatory terminology present in Section 706(a)").

1011 *But see* ADTRAN Comments at 5-6.

1012 *See* Public Knowledge White Paper at 16 ("Congress recognized that it could not accurately forecast what specific information might become either personally or competitively sensitive in the future as communications technologies evolved and converged to include video service and other media. Rather than wait for Congress to do a study, Congress simply delegated the authority to the FCC to consider what rules, what type of information and what specific services should be covered over time."); *see also* EFF Comments at 1-2 ("Congress enacted Section 222 following a tradition of sector-specific privacy regimes to address unique problems. Telecommunications as a telephone service posed all of the same privacy risks to consumers that modern day broadband communications does, as voice communications of sensitive information simply become digital transmissions. The Commission is now at a critical point to determine telecommunications providers' statutory obligations under Section 222 to protect consumer privacy.").

1013 *See* OTI Reply at 4-5 ("[T]he information collection capabilities of internet providers were primitive when Congress passed Section 222 and therefore the internet likely was not front-and-center on the collective minds of Congress .... Congress was not legislating against today's factual backdrop, where ISPs can monitor everyone's internet traffic, but Congress left the statute broad enough that the FCC could address that issue.").

1014 *See*47 U.S.C. § 251 (imposing a "general duty" on telecommunications carriers and more specific duties on subcategories of carriers); *see also* Public Knowledge White Paper at 17-19. CTIA attempts to distinguish other such provisions by arguing that they do not "define in their subsequent subsections the duties *of different regulated entities* identified in their initial subsections." CTIA Reply at 18. In fact, Section 251 does define specific duties of different regulatees in subsections (b) (all local exchange carriers) and (c) (incumbent local exchange carriers), and Section 628 does apply specific duties to cable operators, satellite cable programming

vendors, and common carriers, *see*47 U.S.C. § 548(c), (j). In any event, CTIA does not explain what it believes to be the significance of this distinction.

1015 47 U.S.C. § 548; *see also* Public Knowledge White Paper at 17-18.

1016 47 U.S.C. § 548(b).

1017 47 U.S.C. § 548(c).

1018 *Id.* at (c)(2). The "minimum" required regulations include, *inter alia*, "establish[ing] effective safeguards to prevent a cable operator which has an attributable interest in a satellite cable programming vendor or a satellite broadcast programming vendor from unduly or improperly influencing the decision of such vendor to sell, or the prices, terms, and conditions of sale of, satellite cable programming or satellite broadcast programming to any unaffiliated multichannel video programming distributor." *Id.* at (c)(2)(A).

1019 *National Cable & Telecomms. Ass'n v. FCC*, 567 F.3d 659, 661 (D.C. Cir. 2009) (*NCTA II*); *see also Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 707 (D.C. Cir. 2011).

1020 *Id.* at 664; *see also PGA Tour v. Martin*, 532 U.S. 661 (2001) ("[T]he fact that a statute can be applied in situations not expressly anticipated by Congress does not demonstrate ambiguity. It demonstrates breadth.") (quoting *Pa. Dept. of Corr.v. Yeskey*, 524 U.S. 206, 212 (1952)).

1021 *NCTA II*, 567 F.3d at 665.

1022 *See* OTI Reply at 3 ("In the mid-nineties, when the Telecommunications Act was written, Congress was of course concerned with incumbent telephone services given their ability to use the data they collected in routing traffic to gain competitive advantages and target specific customers. However, Congress's concerns over some specific telephone issues does not freeze the entire statute in time, nor did those specific concerns narrow the statute to telephone services ever after. If Congress had intended to write a statute that applied to telephone services only, it could have easily done so.").

1023 *NCTA II*, 567 F.3d at 666.

1024 Verizon Comments at 54. Verizon argues that both the House bill and the Senate bill originally would have protected a category of customer information broader than the eventual definition of CPNI, but that "Congress ultimately rejected both approaches." *See id.* at 55. There is no evidence that Congress would have, without explanation, adopted an approach that is narrower than either chamber's bill. And, in fact, the Senate bill (which, as Verizon points out, was intended to apply broadly to "customer-specific proprietary information," S. Rep. No. 104-23 at 24), contained in its text language almost identical to what Congress ultimately enacted, creating "a duty to protect the confidentiality of proprietary information relating to other common carriers, to equipment manufacturers, and to customers." S. 652, 104th Cong., 1st Sess. § 301(d); *id.* sec. 222(a), § 256(c)(2)(E).

1025 CTIA Comments 26; *see also* Washington Legal Foundation Comments at 5.

1026 T-Mobile Comments at 16.

1027 *See Hibbs v. Winn*, 542 U.S. 88, 101 (2004) ("A statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant ....") (quoting 2A N. Singer, Statutes and Statutory Construction § 46.06, 181-186 (rev. 6th ed. 2000)); *see also* OTI Reply at 7-8.

1028 *See RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S.Ct. 2065, 2071 (2012) ("It is an old and familiar rule that, where there is, in the same statute, a particular enactment, and also a general one, which, in its most comprehensive sense, would include what is embraced in the former, the particular enactment must be operative, and the general enactment must be taken to affect only such cases within its general language as are not within the provisions of the particular enactment. This rule applies wherever an act contains general provisions and also special ones upon a subject, which, standing alone, the general provisions would include.") (citing *United States v. Chase*, 135 U.S. 255, 260 (1890)).

1029 *But see* AT&T Comments at 106-07; CTIA Comments at 27-28; NCTA Comments at 16-17.

1030 47 U.S.C. § 222(h)(3) (defining "subscriber list information" as identifying information that the carrier or an affiliate has published or intends to publish in a directory format).

1031 *See*47 U.S.C. § 222(e)

1032 *See*47 U.S.C. § 222(g).

1033 *But see* CTIA Comments at 27.

1034 NCTA Comments at 17.

1035 *But see, e.g.*, AT&T Comments at 106-07 (arguing that the construction of Section 222(a) proposed in the NPRM would create conflict with subsections (e) and (g)).

1036 *See Whitman v. American Trucking*, 531 U.S. 457, 468 (2001) (*Whitman*) ("Congress, we have held, does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes."); *see also USTA v. FCC*, 825 F.3d at 703 (citing *Whitman* in rejecting the argument that language in Section 230 of the Act settles the regulatory status of broadband service as an information service).

1037 *See*47 U.S.C. § 222(d)(1).

1038 *See*47 U.S.C. § 222(c)(1). *But see* Verizon Reply at 27.

1039 *Whitman*, 531 U.S. at 468.

1040 *See*47 U.S.C. § 222(a).

1041 *See Utility Air Regulatory Group. v. EPA*, 134 S. Ct. 2427, 2444 (2014); *see also* Comcast Comments at 75, n.200.

1042 *See Furnishing of Customer Premises Equipment and Enhanced Services by American Telephone & Telegraph Co.*, CC Docket No. 85-26, Order, 102 F.C.C.2d 655, 692-93, para. 64 (1985) (discussing 47 CFR § 64.702 (1984) and noting that "customer proprietary information ... belongs to the customers, and many may not want it to be made public").

1043 *See*47 U.S.C. §§ 222(c), 201, 202; *see also TerraCom NAL*, 29 FCC Rcd at 13335-41, paras. 31-44.

1044 *See Utility Air Regulatory Group*, 134 S. Ct. at 2444.

1045 *Id.* at 2442-43.

1046 *See supra* Part III.B.

1047 *But see* Comcast Comments at 71-72 ("The term proprietary information was used in Section 222(a) simply because the provision covers information exchanged with three different types of entities — customers, telecommunications carriers, and equipment manufacturers — and so using the term CPNI, a term that applies solely to *customers* as addressed in Section 222(c), would not have been appropriate.").

1048 *But see id.*

1049 For instance, the subsection could have read: "Every telecommunications carrier has a duty to protect the confidentiality of customer proprietary network information, and of proprietary information of, and relating to, other telecommunication carriers and equipment manufacturers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."

1050 *See*S. Conf. Rep. No. 104-230, 205 (1996).

1051 *See, e.g.*, ITTA Comments at 6-7; CTIA Comments at 28.

1052 *See*47 U.S.C. § 222(b). Furthermore, subsections (e) and (g) impose affirmative obligations on carriers in certain circumstances to share SLI, which by definition is not CPNI. *See*47 U.S.C. §§ 222(e), (g), (h)(1), (h)(3).

1053 *See, e.g.*, Comcast Comments at 74 ("The Conference Report [for the 1996 Act] adopted the House's proposed CPNI definition, but eliminated the catch-all provision from the CPNI definition ultimately codified in Section 222.").

1054 *See Oncale v. Sundowner Offshore Servs., Inc.*, 523 U.S. 75, 79 (1998) ("[I]t is ultimately the provisions of our laws rather than the principal concerns of our legislators by which we are governed."); *cf. NCTA II*, 567 F.3d at 665 ("Thus, even if legislative history could carry petitioners all the way from statutory language that literally authorizes the Commission's action to the proposition that the statute unambiguously forecloses the agency's view, *this* legislative history [i.e., that attending adoption of Section 628 of the Act] cannot.").

1055 *See, e.g.*, AT&T Comments at 104-05; CTIA Comments at 30-32*; see also 2007 CPNI Order*, 22 FCC Rcd at 6928, para. 1 ("In this Order, [we ... strengthen] our rules to protect the privacy of customer proprietary network information (CPNI) ..."); *1998 CPNI Order*, 13 FCC Rcd at 8066-67, para. 4 (providing an overview of the rules being adopted in that order regarding CPNI).

1056 *See 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

1057 *TerraCom NAL*, 29 FCC Rcd at 13330, para. 14. *But see* CTIA Comments at 30-31 (contending that the reference to "proprietary or personal customer information" in paragraph 64 of the *2007 CPNI Order* is best read as limited to CPNI); *see also Lifeline and Link Up Reform and Modernization et al.*, Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order, 30 FCC Rcd 7818, 7895-96, para. 234 (2015) (reminding carriers that the duty to protect customer information "includes all documentation submitted by a consumer or collected by an [[eligible telecommunications carrier] to determine a consumer's eligibility for Lifeline service, as well as all personally identifiable information contained therein").

1058 *But see* ITTA Comments at 3-4 (arguing that "the Commission *did* address [[whether Section 222(a) covers customer information other than CPNI] and affirmatively decided that subsection 222(a) afforded no such 'broader' protections."). ITTA cites as the basis for this claim a discussion in the *1999 CPNI Reconsideration Order* of the relationship between Sections 222 and 272(c)(1). *See id.* at 4, n.10 (citing *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14488, para. 147). Contrary to ITTA's claim, the Commission did not "affirmatively" address the scope of customer information covered under Section 222(a).

1059 *See 1998 CPNI Order*, 13 FCC Rcd at 8068-69, para. 7 ("Prior to the 1996 Act, the Commission had established CPNI requirements applicable to the enhanced services operations of AT&T, the BOCs, and GTE, and the CPE operations of AT&T and the BOCs, in the *Computer II*, *Computer III*, *GTE ONA*, and *BOC CPE Relief* proceedings.") (internal footnotes omitted).

1060 *See 1998 CPNI Order*, 13 FCC Rcd at 8068, para. 6 (explaining that the proceeding was initiated "[i]n response to various informal requests for guidance from the telecommunications industry regarding the obligation of carriers under new section 222").

1061 We expressly disavow any prior Commission statement that could be read as endorsing such a view. *See FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009) (holding that although an agency must acknowledge that it is changing course when it adopts a new construction of an ambiguous statutory provision, "it need not demonstrate to a court's satisfaction that the reasons for the new policy are *better* than the reasons for the old one ...." Rather, it is sufficient that "the new policy is permissible under the statute, that there are good reasons for it, and that the agency *believes* it to be better, which the conscious change of course adequately indicates.").

1062 *But see* Verizon Reply at 26.

1063 15 U.S.C. § 45(a)(2) (exempting "common carriers subject to the Acts to regulate commerce"), § 44 (defining "Acts to regulate commerce" as including "the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto"). *See also*47 U.S.C. § 153(51) (providing that "[a] telecommunications carrier shall be treated as a common carrier under [the Communications Act] only to the extent that it is engaged in providing telecommunications services").

1064 *See TerraCom NAL*, 29 FCC Rcd at 13325, para. 1 ("Today, we take action against two companies that collected names, addresses, Social Security numbers, driver's licenses, and other proprietary information (PI) belonging to low-income Americans and stored them on unprotected Internet servers that anyone in the world could access with a search engine and basic manipulation.").

1065 *See supra* Part III.B.

1066 *See supra* para. 343.

1067 *See*47 USC § 222(a).

1068 *See*47 USC § 222(c).

1069 *See id.*; *see also* CTIA Comments at 26 ("In short, the most natural reading of Section 222 is that subsection (a)'s general mandate is specifically set forth for customers in subsection (c) ...").

1070 *See supra* Part III.D.

1071 *See supra* Part III.D.1 (sensitive/non-sensitive distinction), Part III.E (sensitivity of the data as a factor), and III.F.1 (harm presumption with respect to sensitive data breaches).

1072 *See, e.g.*, WTA Comments at 19 (discussing the costs that would accrue to smaller providers in complying with "multiple regulatory regimes").

1073 *See supra* para. 358.

1074 Comcast Comments at 81.

1075 *See supra* Part III.D.

1076 *See supra* Part III.C.

1077 *See supra* Part III.E.

1078 *See supra* Part III.F.

1079 *See supra* Part III.G.1.

1080 AT&T Comments at 108; *see also* Comcast Comments at 81 ("Even if Section 222(a) confers an independent grant of authority, it is only the authority to adopt rules to 'protect the confidentiality of' proprietary information. This means that any authority the Commission may have under [[Section 222(a)] is limited to preventing proprietary information from being exposed without authorization and does not extend to defining its permissible uses such as for marketing or advertising."); Verizon Comments at 59 ("Section 222(a) is far too thin a reed to authorize the entire regulatory apparatus the Commission proposes to erect for PII that is not CPNI. Section 222(a) requires only that carriers 'protect the confidentiality' of information; it does not govern permissible uses of information."); Letter from Loretta Polk, Vice President and Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 21, 2016).

1081 *But see* Comcast Comments at 82 (urging the Commission to model its interpretation of Section 222(a) on the FTC's interpretation of different statutory language in the Gramm-Leach-Bliley Act).

1082 47 USC § 222(c) (capitalization omitted).

1083 47 USC § 222(b) (capitalization omitted).

1084 Public Knowledge et al. Reply at 4.

1085 *See* Verizon Comments at 60.

1086 *See*47 USC § 222(c)(1); *see also*47 U.S.C. § 222(d) (enumerating additional exceptions).

1087 *See 2002 CPNI Order*, 17 FCC Rcd at 14862-63, para. 2 (providing an overview of "opt-in" and "opt-out" approval requirements adopted in that order).

1088 *See supra* Part III.D.

1089 *See supra* Part III.D.

1090 *See supra* Part III.C.

1091 *See supra* Part III.G.1.

1092 *See supra* Part III.G.1.

1093 *See supra* Part III.E.

1094 *See supra* Part III.F.

1095 *See 2007 CPNI Order*, 22 FCC Rcd at 6943-45, paras. 26-32; *see also*47 CFR § 64.2011.

1096 *See*47 U.S.C. § 222(h)(1) ("customer proprietary network information"), (h)(2) ("aggregate customer information").

1097 *See supra* Part III.B.4.

1098 *See infra* Appx. A.

1099 *See*47 U.S.C. § 222(e), (g).

1100 47 U.S.C. §§ 201(b), 202(a); *see Broadband Privacy NPRM*, 31 FCC Rcd at 2596, paras. 305-06.

1101 *2015 Open Internet Order*, 30 FCC Rcd at 5609, para. 22, 5659-69, paras. 133-53.

1102 *Id.* at 5662, para. 141.

1103 *See supra* para. 297. *But see* Nokia Reply at 9 ("[F]or innovation to happen throughout the entire ecosystem, the Commission must avoid policy frameworks that impose *ex ante* prohibitions on potential sources of value creation particularly when those prohibitions are imposed on only one segment of the ecosystem: once again, in this instance, providers of BIAS.").

1104 *See supra* Part IV.A.2.

1105 *See*FCC and FTC, Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers, 65 Fed. Reg. 44053-02, 44054 (July 17, 2000).

1106 *See Broadband Privacy NPRM*, 31 FCC Rcd at 2598, para. 310.

1107 47 U.S.C. § 303(b); *see, e.g.*, *2015 Open Internet Order*, 30 FCC Rcd at 5725, paras. 285-87.

1108 *See* Public Knowledge White Paper at 20-21. *But see* T-Mobile Comments at 23; CTIA Comments at 71-73.

1109 *Cf., e.g.*, *Facilitating the Deployment of Text-To-911 and Other Next Generation 911 Applications*, PS Docket Nos. 11-153, 10-255, Report and Order, 28 FCC Rcd 7556, 7587-92, paras. 89-99 (2013); *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, PS Docket Nos. 15-80, 11-82, ET Docket No. 16-63, Report and Order, Further Notice of Proposed Rulemaking, and Order on Reconsideration, 31 FCC Rcd 5817, 5896-97, paras. 202-05 (2016).

1110 47 U.S.C. § 303(r); *see 2015 Open Internet Order*, 30 FCC Rcd at 5725, para. 287 (citing *Cellco P'ship v. FCC*, 700 F.3d 534, 543 (D.C. Cir. 2012)).

1111 47 U.S.C. § 316(a)(1); *see 2015 Open Internet Order*, 30 FCC Rcd at 5725, para. 287.

1112 *See*47 U.S.C. § 1302(a).

1113 *See* Greenlining Institute Comments at 18-19 ("[C]ommodification and use of the customer's personal information without informed consent [interferes] with a consumer's access to the BIAS telecommunications transport, and lessen consumer trust (and the public's trust) in the integrity of BIAS service."); Public Knowledge White Paper at 22-23 ("[P]rotection of CPNI may spur consumer

demand ... driving demand for broadband connections, and consequently encouraging more broadband investment and deployment consistent with Section 706.") (citing *2007 CPNI Order*, 22 FCC Rcd at 6927, para. 59).

1114 *But see* CTIA Comments at 67. ("[F]urther network investment will not take place if ISPs lack the incentives or resources to continue to deploy broadband infrastructure."); ACA Comments at 70-71 ("In fact, the proposed rules are more likely to shove a stick in the spokes of the virtuous circle than perpetuate it."); Washington Legal Foundation Comments at 7-9.

1115 *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59; *see also*47 CFR § 64.2003(o) (defining "telecommunications carrier or carrier" for purposes of the CPNI rules to include interconnected VoIP providers).

1116 We make no decisions in this Order on the regulatory classification of interconnected VoIP services.

1117 *See 2007 CPNI Order*, 22 FCC Rcd at 6955, para. 55; *see also United States v. Southwestern Cable*, 392 U.S. 157, 177-78 (1968) (setting forth the two-part "ancillary jurisdiction" test); *Comcast Corp. v. FCC*, 600 F.3d 642, 654 (D.C. Cir. 2010) (holding that ancillary jurisdiction must be "necessary to further its regulation of activities over which it does have express statutory authority"). We conclude that our jurisdiction to apply the rules in this Order to interconnected VoIP providers is just as strong as it was in 2007. In addition to the analysis in the *2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59, we observe that applying these obligations to interconnected VoIP providers is necessary to protect the privacy of customers of BIAS providers and other telecommunications services. Given the growth in interconnected VoIP and the extent to which it increasingly is viewed as a substitute for traditional telephone service, telecommunications carriers could be disadvantaged if they were subject to these requirements but other interconnected VoIP providers were not. Consumers' privacy interests could benefit to the extent that providers of competitive services are subject to the same obligations. Furthermore, in light of Congress's amendment of the Act, including Section 222, to apply E-911 obligations to interconnected VoIP, the 911 system could be disrupted to the extent that our harmonized Section 222 regime were no longer to apply to interconnected VoIP.

1118 *2007 CPNI Order*, 22 FCC Rcd at 6956, para. 56.

1119 *Id.* at 6956, para. 57.

1120 *See* NET 911 Act; *see also*47 U.S.C. § 222(d)(4), (f)(1), (g).

1121 47 U.S.C. § 222(d)(4), (f)(1), (g) (applying provisions of section 222 to "IP-enabled voice service"); § 615b(8) (defining "IP-enabled voice service" as having "the meaning given the term 'interconnected VoIP service' by section 9.3 of the Federal Communications Commission's regulations (47 CFR 9.3)").

1122 *See, e.g.*, *supra* para. 242.

1123 *See, e.g.*, *supra* para. 234 (removal of annual certifications requirement); para. 253 (customer authentication).

1124 *See supra* Part III.H.2. *But see* Voice on the Net Coalition Comments at 6.

1125 *See infra* Appx. B.

1126 *But see* Voice on the Net Coalition Comments at 4.

1127 *Central Hudson Gas & Electric Corp. v. Pub. Serv. Comm'n of N. Y.*, 447 U.S. 557 (1980).

1128 *Central Hudson*, 447 U.S. at 566; *see also U.S. West*, 182 F.3d at 1233.

1129 *Central Hudson*, 447 U.S. at 566; *NCTA v. FCC*, 555 F.3d at 1000; *U.S. West*, 182 F.3d at 1233.

1130 *NCTA v. FCC*, 555 F.3d at 1001 (2009) (internal citations omitted) ("The Tenth Circuit supposed that § 222 sought to promote a governmental interest in protecting against the disclosure of 'information [that] could prove embarrassing,' and it doubted whether this interest could be deemed "substantial.' We do not share the Tenth Circuit's doubt. For one thing, we have already held, in an analogous context, that 'protecting the privacy of consumer credit information' is a 'substantial' government interest. For another thing, we do not agree that the interest in protecting customer privacy is confined to preventing embarrassment as the Tenth Circuit

thought. There is a good deal more to privacy than that .... The Supreme Court knows this as well Congress: 'both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person.'").

1131 CTIA Comments at 81-82 (recognizing substantial interest in customers' control of their personal information); CTIA Sept. 16, 2016 *Ex Parte* at 18-19 (conceding substantial privacy interest in online ecosystem while questioning the breadth of the proposed rules); Consumer Federation of California Reply at 8-9 (enumerating state interests in privacy found throughout federal and state law).

1132 *See, e.g.*, *NCTA v. FCC*, 555 F.3d at 1001; *Ohio v. Akron Ctr. for Reprod. Health*, 497 U.S. 502, 529 (1990); *Carey v. Population Servs., Intern.*, 431 U.S. 678, 684 (1977); *Whalen v. Roe*, 429 U.S. 589, 599 (1977); *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965); *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 625 (1995); *Edenfield v. Fane*, 507 U.S. 761, 766 (1993). *US West v. FCC*, frequently cited in opposition to the constitutionality of this Order, acknowledges the "substantial state interest" in privacy, and that Section 222, in particular, has a "specific and dominant purpose" of protecting consumer privacy. 182 F.3d at 1234, 1236.

1133 *See, e.g.*, *2002 CPNI Order*, 17 FCC Rcd at 14875, para. 33.

1134 *See supra* note 1131.

1135 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213 (1890) ("If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation."); *see also* William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960) (enumerating privacy torts, including "[p]ublic disclosure of embarrassing private facts about the plaintiff").

1136 *See, e.g.*, *supra* note 696 (acknowledging potential for financial or physical harm).

1137 In implementing the Truth in Caller ID Act, the Commission found that "harm" was a broad concept encompassing financial, physical, and emotional harm. *See Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Report and Order, 26 FCC Rcd 9114, 9122, para. 22 (2011).

1138 2012 FTC Privacy Report at 7-9.

1139 2015 Administration CPBR Discussion Draft, § 4(g).

1140 *See, e.g.*, Comments of Laurence Tribe on behalf of CTIA, NCTA and USTelecom at 27-29 (Tribe Comments).

1141 *U.S. Dept. of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989) (cited in *NCTA v. FCC*, 555 F.3d at 1001); *see* OTI Reply at 18-19.

1142 *NCTA v. FCC*, 555 F.3d at 1001; *see* OTI Reply at 20.

1143 From their inception, FIPPs have recognized privacy as an individual's right to control *uses* of information about him—not merely to control their disclosures. *See* HEW Report at 40-41 (finding that privacy is affected by the recording, disclosure, and use of identifiable information).

1144 *See, e.g.*, 2012 FTC Privacy Report at i; 2012 White House Privacy Blueprint; Online Interest-Based Advertising Accountability Comments at 2; EPIC Comments at 2-3; Privacy Rights Clearinghouse at 2-3; McDonald Reply at 1; Charter Comments at 6-7; Internet Association Comments at 6-7; ITIC Comments at 4; USTelecom Comments at 11-12.

1145 The Federal Radio Act of 1927, and the original language of the Communications Act of 1934, prohibited carriers not only from publishing or divulging information relevant to communications, but also from making uses of the information solely to benefit themselves. *See* Max D. Paglin, A Legislative History of the Communications Act of 1934, 721 (1989); Communications Act of 1934 § 605, 48 Stat. 1103 (now codified at 47 U.S.C. § 605(a)); Public Knowledge Reply at 4.

1146 *See* Daniel Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L.J. 11131, 1133 (2011) (noting the existence of both subjective and objective privacy harms); OTI Reply at 20, 27.

1147 Consumer Privacy Index 2016; OTI Reply at 22.

1148 Consumer Privacy Index 2016. A Bain & Company survey of over 900 consumers found that two-thirds of them felt it should be "illegal for companies to collect or use ... data without getting prior consent." Bain & Company Press Release, *How can companies acquire customer data while building customer loyalty at the same time? Ask permission*, Bain & Company (May 11, 2015), http://bain.com/about/press/press-releases/Digital-privacy-survey-2015-press-release.aspx; OTI Reply at 23.

1149 Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It* 8, 13 (2009); OTI Reply at 23-24, n.69

1150 *2015 Open Internet Order*, 30 FCC Rcd at 5821, para. 464.

1151 Solove at 520; OTI Reply at 29.

1152 Rafi Goldberg, NTIA, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

1153 Consumer Privacy Index 2016; OTI Reply at 25.

1154 2012 FTC Privacy Report at 8-9.

1155 *U.S. West*, 182 F.3d at 1237.

1156 While we recognize that adopting these rules cannot protect customers from privacy violations that originate from entities that are not telecommunications providers, the fact that the rules do not create universal privacy protection does not mean that customers' privacy interests are not advanced. *See, e.g.*, *Williams-Yulee v. Florida Bar Ass'n*, 135 S. Ct 1656, 1668 (2015) (citing *R.A.V. v. St. Paul*, 505 U.S. 377, 387 (1992)) ("Although a law's underinclusivity raises a red flag, the First Amendment imposes no freestanding 'underinclusiveness limitation.'"); *id.* ("A State need not address all aspects of a problem in one fell swoop; policymakers may focus on their most pressing concerns. We have accordingly upheld laws—even under strict scrutiny—that conceivably could have restricted even greater amounts of speech in service of their stated interests."); *see also Trans Union Corp. v. F.T.C.*, 267 F.3d 1138, 1143 (D.C. Cir. 2001) (citing *Blount v. SEC*, 61 F.3d 938, 946 (1995))("A regulation is not fatally underinclusive simply because an alternative regulation, which would restrict more speech or the speech of more people, could be more effective ... a rule is struck for *under* inclusiveness only if it cannot fairly be said to advance any genuinely substantial government interest."). *But see* Tribe Comments at 22.

1157 *See supra* para. 87.

1158 *Central Hudson*, 447 U.S. at 569-70.

1159 *Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 188 (1999) (internal quotation marks omitted).

1160 *See supra* para. 198.

1161 The Commission has previously found, in the context of its voice CPNI rules, that "telecommunications consumers expect to receive targeted notices from their carriers about innovative telecommunications offerings that may bundle desired telecommunications services and/or products, save the consumer money, and provide other consumer benefits." *2002 CPNI Order*, 17 FCC Rcd at 14877, para. 36.

1162 *See supra* para. 193, note 553.

1163 *See, e.g.*, *2007 CPNI Order*, 22 FCC Rcd at 6949-52, paras. 44-46.

1164 *See supra* para. 193.

1165 *See supra* para. 193.

1166 As a functional matter, while opt-out consent has been described as the least restrictive form of obtaining customer approval, it is only "marginally less intrusive than opt-in for First Amendment purposes." *See* CDT Reply at 9, citing *NCTA v. FCC*, 555 F.3d at 1002.

1167 *See supra* para. 194.

1168 564 U.S. 552 (2011).

1169 *Sorrell*, 564 U.S. at 565.

1170 *See supra* Part. III.A.

1171 Indeed, if laws impacting expression were considered content-based for not being universal, nearly every privacy and intellectual property law would need to pass strict scrutiny.

1172 *Sorrell*, 564 U.S. at 573; ACLU Reply at 5. Similarly, use-based exceptions to Section 222 and our rules do not render the statute or rules content-based any more than purpose-based exceptions in HIPAA. *Cf.* OTI Reply at 11-12.

1173 T-Mobile Comments at 42-44; Washington Legal Foundation Comments at 14-15.

1174 *See Zauderer v. Office of Disc. Counsel*, 471 U.S. 626, 651 (1985); *see also, e.g.*, *Am. Meat Inst. v. U.S. Dep't of Agriculture*, 760 F.3d 18, 22 (D.C. Cir. 2014) (holding that country-of-origin labeling requirements were not unconstitutionally compelled speech); *N.Y. State Rest. Ass'n v. N.Y. City Bd. of Health*, 556 F.3d 114, 133 (2d Cir. 2009); *Nat'l Elec. Mfrs. Ass'n v. Sorrell*, 272 F.3d 104, 113-15 (2d Cir. 2001).

1175 *Id.*

1176 *See, e.g.*, Tribe Comments at 38-39.

1177 Black's Law Dictionary, 377 (10th ed. 2014).

1178 *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 516 (2009) (citing *Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Constr. Trades Council*, 485 U.S. 568, 575 (1988)).

1179 *Id.*

1180 *See* Letter from Mike Wendy, President, MediaFreedom to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Oct. 18, 2016).

1181 *See U.S. Telecom Ass'n v. FCC*, 825 F.3d at 742 ("[T]he communicative intent of the individual speakers who use such transmission networks does not transform the networks themselves into speakers."); *U.S. v. Western Elec. Co.*, 673 F. Supp. 525, 586 n. (D.D.C. 1987) (Greene, J.).

1182 *See*5 U.S.C. § 603.

1183 *Broadband Privacy NPRM*, Appx. B.

1 *See*5 U.S.C. § 603. The RFA, *see*5 U.S.C. §§ 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

2 *Broadband Privacy NPRM*, 31 FCC Rcd at 2611-32, Appx. B.

3 *See* Alaska Telephone Association Reply at 1-2; CCA Reply at 6; NTCA Reply at 15-16; RWA Comments at 2-13; WISPA Comments at 4-5, 31-33; WISPA Reply at 1-3, 31-43; U.S. Small Business Administration Reply.

4 *See*5 U.S.C. § 604.

5 *See supra* note 68.

6 *See supra* Part III.A.

7 *2015 Open Internet Order*, 30 FCC Rcd at 5820-22, paras. 462-64; *see also supra* Part III.A.

8 *See generally Broadband Privacy NPRM*, 31 FCC Rcd at 2500.

9 *See, e.g.*, *Broadband Privacy NPRM*, 31 FCC Rcd at 2510, para. 24.

10 *See* Letter from Paul Ohm, Professor, Georgetown University Law Center, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106 Attach., Testimony Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives at 3 (filed June 19, 2016) (Paul Ohm Testimony).

11 *See 2015 Open Internet Order*, 30 FCC Rcd at 5629, para. 80 (noting that "once a consumer chooses a broadband provider, that provider has a monopoly on access to the subscriber").

12 Letter from Kathleen McGee, Bureau Chief, Bureau of Internet and Technology, New York State Attorney General, to Tom Wheeler, Chairman, FCC, GC Docket No. 16-106 at 2 (filed June 30, 2016) (NY Attorney General June 30, 2016 *Ex Parte* Letter) (also claiming that BIAS providers can collect "not only a consumer's name, address and financial information but also every website he or she visited, the links clicked on those websites, geo-location information, and the content of electronic communications"); *see also, e.g.*, Letter from Christopher N. Olsen, Counsel to Ghostery, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106, Attach. at 3-5 (Ghostery Apr. 29, 2016 *Ex Parte* Letter); Consumer Action Comments at 1; Consumer Watchdog Comments at 4 ("The ISP is in a unique position to amass deeply revealing personal profiles, share the data with third parties or use it for its own purposes."); Public Knowledge et al. Comments, Attach. Public Knowledge White Paper, Protecting Privacy, Promoting Competition: A framework for Updating the Federal Communications Commission Privacy Rules for the Digital World at 51-52, 55-56 (Public Knowledge White Paper); AAJ Comments at 8 (explaining that "BIAS providers are now privy to an extensive amount of personal information about their customers"); EFF Comments at 1.

13 *See* Alaska Telephone Association Reply at 1-2; CCA Reply at 6; NTCA Reply at 15-16; RWA Comments at 2-13; WISPA Comments at 4-5, 31-33; WISPA Reply at 1-3, 31-43.

14 *See, e.g.*, ACA Comments at 38-39, 46-51, 57-58; ACA Reply at 4, 14-20; CCA Reply at 12-13, 25-26, 35, 40-41; Education & Research Consortium et al. Comments at 5, 8-10; NTCA Comments at 18, 41-43, 49-51, 55; Rural Wireless Association Comments at 2-14; USTelecom Comments at 19; WISPA Comments at 4-5, 28-29, 31-33; WISPA Reply at 31-43; WTA Comments at 2-3, 10-17; WTA Reply at 5-10, 13; WTA & Nex-Tech Apr. 25, 2016 *Ex Parte* at 1.

15 *See* ACA Reply at 4; Alaska Telephone Association Reply at 1-2; WISPA Reply at 41; WTA Comments at 2-3; WTA Reply at 5-6.

16 *See* ACA Comments at 46-49; CCA Reply at 40-41; WISPA Comments at 28-29.

17 *See* ACA Comments at 57-58; RWA Comments at 6-7; WTA Comments at 12.

18 *See* ACA Comments at 38-39, 46; ACA Reply at 4; CCA Reply at 25-26, 35; NTCA Comments at 41-43; WTA Comments at 14-17; WTA Reply at 8-10. *But see* ACA Reply at 14-15 (asking for standardized notices with a safe harbor); NTCA Comments at 41-42 (same).

19 *See* USTelecom Comments at 19; NTCA Comments at 55; WISPA Comments at 31; WTA Comments at 10, 16.

20 *See* NTCA Comments at 49-51.

21 *See* CCA Reply at 12-13; WISPA Comments at 31-33; WISPA Reply at 31-43; WTA Reply at 13.

22 *See* ACA Reply at 4; WISPA Comments at 31-33; WISPA Reply at 31-43.

23 Education & Research Consortium et al. Comments at 8-10.

24 *See infra* Appx. B, Part I.F.

25 5 U.S.C. § 604(a)(3).

26 Letter from Darryl L. DePriest, Chief Counsel for Advocacy, and Jamie Belcore Saloom, Assistant Chief Counsel, Office of Advocacy, U.S. Small Business Administration, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed June 27, 2016) (SBA Comments).

27 U.S. Small Business Administration Reply at 3.

28 U.S. Small Business Administration Reply at 4.

29 *See supra* Part III.I.4.

30 *See supra* Part III.E.

31 *See supra* Part III.E.1.

32 5 U.S.C. § 604.

33 5 U.S.C. § 601(6).

34 5 U.S.C. § 601(3) (incorporating by reference the definition of ""small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

35 15 U.S.C. § 632.

36 *See supra* Part III.I.4.

37 *See*5 U.S.C. §§ 601(3)-(6).

38 *See* Small Bus. Admin., Office of Advocacy, *Frequently Asked Questions about Small Business* 1 (2016), https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2016_WEB.pdf.

39 5 U.S.C. § 601(4).

40 Indep. Sector, The New Nonprofit Almanac and Desk Reference (2010).

41 5 U.S.C. § 601(5).

42 U.S. Census Bureau, Statistical Abstract of the United States: 2012, Section 8, page 267, tbl. 429, https://www.census.gov/compendia/statab/2012/tables/12s0429.pdf/ (data cited therein are from 2007).

43 The 2007 U.S. Census data for small governmental organizations are not presented based on the size of the population in each such organization. There were 89,476 local governmental organizations in 2007. If we assume that county, municipal, township, and school district organizations are more likely than larger governmental organizations to have populations of 50,000 or less, the total of these organizations is 52,095. As a basis of estimating how many of these 89,476 local government organizations were small, in 2011, we note that there were a total of 715 cities and towns (incorporated places and minor civil divisions) with populations over 50,000. U.S. Census Bureau, City and Town Totals Vintage: 2011, http://www.census.gov/popest/data/cities/totals/2011/index.html. If we subtract the 715 cities and towns that meet or exceed the 50,000 population threshold, we conclude that approximately 88,761 are small. U.S. Census Bureau, Statistical Abstract of the United States: 2012, Section 8, page 267, tbl. 429, https://www.census.gov/compendia/statab/2012/tables/12s0429.pdf/ (data cited therein are from 2007).

44 U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Carriers," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517110&search=2012NAICSSearch.

45 13 CFR § 121.201, NAICS code 517110.

46 U.S. Census Bureau, 2012 NAICS Definitions, "517919 All Other Telecommunications,", http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517919&search=2012NAICSSearch.

47 13 CFR § 121.201, NAICS code 517919.

48 U.S. Census Bureau, 2007 Economic Census, Subject Series: Information, Table 5, "Establishment and Firm Size: Employment Size of Firms for the United States: 2007 NAICS Code 517110" (2010).

49 *See id.*

50 U.S. Census Bureau, 2007 Economic Census, Subject Series: Information, ""Establishment and Firm Size," NAICS code 5179191 (2010) (receipts size).

51 http://www.census.gov/cgi-bin/sssd/naics/naicsrch.

52 *See*13 CFR § 120.201, NAICS Code 517110.

53 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

54 13 CFR § 121.201, NAICS code 517110.

55 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

56 13 CFR § 121.201, NAICS code 517110.

57 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

58 *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

59 *Id.*

60 13 CFR § 121.201, NAICS code 517110.

61 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

62 *See Trends in Telephone Service*, at tbl. 5.3.

63 *Id.*

64 *Id.*

65 *Id.*

66 *Id.*

67 5 U.S.C. § 601(3).

68 Letter from Jere W. Glover, Chief Counsel for Advocacy, SBA, to William E. Kennard, Chairman, Federal Communications Commission (filed May 27, 1999). The Small Business Act contains a definition of "small business concern," which the RFA incorporates into its own definition of "small business." 15 U.S.C. § 632(a); 5 U.S.C. § 601(3). SBA regulations interpret "small business concern" to include the concept of dominance on a national basis. 13 CFR § 121.102(b).

69 13 CFR § 121.201, NAICS code 517110.

70 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

71 *See Trends in Telephone Service*, at tbl. 5.3.

72 *Id.*

73 13 CFR § 121.201, NAICS code 517110.

74 *Trends in Telephone Service*, tbl. 5.3.

75 http://www.census.gov/cgi-bin/ssd/naics/naicsrch.

76 13 CFR § 121.201, NAICS code 517911.

77 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

78 *See Trends in Telephone Service*, at tbl. 5.3.

79 *Id.*

80 13 CFR § 121.201, NAICS code 517911.

81 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

82 *See Trends in Telephone Service*, at tbl. 5.3.

83 *Id.*

84 13 CFR § 121.201, NAICS code 517911.

85 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

86 *Id.*

87 *Trends in Telephone Service*, at tbl. 5.3.

88 *Id.*

89 13 CFR § 121.201, NAICS code 517110.

90 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

91 *Trends in Telephone Service*, at tbl. 5.3.

92 *Id.*

93 NAICS Code 517210. *See* http://www.census.gov/cgi-bin/ssd/naics/naicsrch.

94 *Trends in Telephone Service*, at tbl. 5.3.

95 *Id.*

96 *Amendment of the Commission's Rules to Establish Part 27, the Wireless Communications Service (WCS)*, Report and Order, 12 FCC Rcd 10785, 10879, para. 194 (1997).

97 *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (filed Dec. 2, 1998) (*Alvarez Letter 1998*).

98 47 CFR § 2.106; *see generally*47 CFR §§ 27.1-27.70.

99 13 CFR § 121.201, NAICS code 517210.

100 *Id.*

101 *Trends in Telephone Service*, tbl. 5.3.

102 *Id.*

103 *See Amendment of Parts 20 and 24 of the Commission's Rules — Broadband PCS Competitive Bidding and the Commercial Mobile Radio Service Spectrum Cap; Amendment of the Commission's Cellular/PCS Cross-Ownership Rule*, Report and Order, 11 FCC Rcd 7824, 7850-52, paras. 57-60 (1996) (*PCS Report and Order*); *see also*47 CFR § 24.720(b).

104 *See PCS Report and Order*, 11 FCC Rcd at 7852, para. 60.

105 *See Alvarez Letter 1998*.

106 *See Broadband PCS, D, E and F Block Auction Closes*, Public Notice, Doc. No. 89838 (rel. Jan. 14, 1997).

107 *See C, D, E, and F Block Broadband PCS Auction Closes*, Public Notice, 14 FCC Rcd 6688 (WTB 1999). Before Auction No. 22, the Commission established a very small standard for the C Block to match the standard used for F Block. *Amendment of the Commission's Rules Regarding Installment Payment Financing for Personal Communications Services (PCS) Licensees*, Fourth Report and Order, 13 FCC Rcd 15743, 15768, para. 46 (1998).

108 *See C and F Block Broadband PCS Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 2339 (2001).

109 *See Broadband PCS Spectrum Auction Closes; Winning Bidders Announced for Auction No. 58*, Public Notice, 20 FCC Rcd 3703 (2005).

110 *See Auction of Broadband PCS Spectrum Licenses Closes; Winning Bidders Announced for Auction No. 71*, Public Notice, 22 FCC Rcd 9247 (2007).

111 *Id.*

112 *See Auction of AWS-1 and Broadband PCS Licenses Closes; Winning Bidders Announced for Auction 78*, Public Notice, 23 FCC Rcd 12749 (WTB 2008).

113 *Id.*

114 47 CFR § 90.814(b)(1).

115 *Id.*

116 *See* Letter from Aida Alvarez, Administrator, SBA, to Thomas Sugrue, Chief, Wireless Telecommunications Bureau, Federal Communications Commission (filed Aug. 10, 1999) (*Alvarez Letter 1999*).

117 *See Correction to Public Notice DA 96-586 "FCC Announces Winning Bidders in the Auction of 1020 Licenses to Provide 900 MHz SMR in Major Trading Areas,"* Public Notice, 18 FCC Rcd 18367 (WTB 1996).

118 *See Multi-Radio Service Auction Closes*, Public Notice, 17 FCC Rcd 1446 (WTB 2002).

119 *See 800 MHz Specialized Mobile Radio (SMR) Service General Category (851-854 MHz) and Upper Band (861-865 MHz) Auction Closes; Winning Bidders Announced*, Public Notice, 15 FCC Rcd 17162 (2000).

120 *See 800 MHz SMR Service Lower 80 Channels Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 1736 (2000).

121 *See generally*13 CFR § 121.201, NAICS code 517210.

122 *See Reallocation and Service Rules for the 698-746 MHz Spectrum Band (Television Channels 52-59)*, Report and Order, 17 FCC Rcd 1022 (2002) (*Channels 52-59 Report and Order*).

123 *See id.* At 1087-88, para. 172.

124 *See id.*

125 *See id.*, at 1088, para. 173.

126 *See Alvarez Letter 1999*.

127 *See Lower 700 MHz Band Auction Closes*, Public Notice, 17 FCC Rcd 17272 (WTB 2002).

128 *See id.*

129 *See id.*

130 *Service Rules for the 698-746, 747-762 and 777-792 MHz Band; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Section 68.4(a) of the Commission's Rules Governing Hearing Aid-Compatible Telephones; Biennial Regulatory Review—Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services; Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission's Rules; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band; Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010; Declaratory Ruling on Reporting Requirement under Commission's Part 1 Anti-Collusion Rule*, Second Report and Order, 22 FCC Rcd 15289, 15359 n. 434 (2007) (*700 MHz Second Report and Order*).

131 *See Auction of 700 MHz Band Licenses Closes*, Public Notice, 23 FCC Rcd 4572 (WTB 2008).

132 *700 MHz Second Report and Order*, 22 FCC Rcd 15289.

133 *See Auction of 700 MHz Band Licenses Closes*, Public Notice, 23 FCC Rcd 4572 (WTB 2008).

134 *See Service Rules for the 746-764 MHz Bands, and Revisions to Part 27 of the Commission's Rules*, Second Report and Order, 15 FCC Rcd 5299 (2000) (*746-764 MHz Band Second Report and Order*).

135 *See id.* at 5343, para. 108.

136 *See id.*

137 *See id.* at 5343, para. 108 n.246 (for the 746-764 MHz and 776-794 MHz bands, the Commission is exempt from 15 U.S.C. § 632, which requires Federal agencies to obtain SBA approval before adopting small business size standards).

138 *See 700 MHz Guard Bands Auction Closes: Winning Bidders Announced*, Public Notice, 15 FCC Rcd 18026 (WTB 2000).

139 *See 700 MHz Guard Bands Auction Closes: Winning Bidders Announced*, Public Notice, 16 FCC Rcd 4590 (WTB 2001).

140 13 CFR § 121.201, NAICS codes 517210.

141 *Amendment of Part 22 of the Commission's Rules to Benefit the Consumers of Air-Ground Telecommunications Services, Biennial Regulatory Review—Amendment of Parts 1, 22, and 90 of the Commission's Rules, Amendment of Parts 1 and 22 of the Commission's Rules to Adopt Competitive Bidding Rules for Commercial and General Aviation Air-Ground Radiotelephone Service*, Order on Reconsideration and Report and Order, 20 FCC Rcd 19663, paras. 28-42 (2005).

142 *Id.*

143 *See* Letter from Hector V. Barreto, Administrator, SBA, to Gary D. Michaels, Deputy Chief, Auctions and Spectrum Access Division, Wireless Telecommunications Bureau, Federal Communications Commission (filed Sept. 19, 2005).

144 The service is defined in section 90.1301 *et seq.* of the Commission's Rules, 47 CFR § 90.1301 *et seq.*

145 *See* *Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Report and Order, 18 FCC Rcd 25162, Appx. B (2003), *modified by* *Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Order on Reconsideration, 20 FCC Rcd 14058, Appx. C (2005); *Service Rules for Advanced Wireless Services in the 1915-1920 MHz, 1995-2000 MHz, 2020-2025 MHz and 2175-2180 MHz Bands; Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Notice of Proposed Rulemaking, 19 FCC Rcd 19263, Appx. B (2005); *Service Rules for Advanced Wireless Services in the 2155-2175 MHz Band*, Notice of Proposed Rulemaking, 22 FCC Rcd 17035, Appx. (2007).

146 *See* 47 CFR Part 101, Subparts C and I.

147 *See* 47 CFR Part 101, Subparts C and H.

148 Auxiliary Microwave Service is governed by Part 74 of Title 47 of the Commission's Rules. *See* 47 CFR Part 74. Available to licensees of broadcast stations and to broadcast and cable network entities, broadcast auxiliary microwave stations are used for relaying broadcast television signals from the studio to the transmitter, or between two points such as a main studio and an auxiliary studio. The service also includes mobile TV pickups, which relay signals from a remote location back to the studio.

149 *See* 47 CFR Part 101, Subpart L.

150 *See* 47 CFR Part 101, Subpart G.

151 *See id.*

152 *See*47 CFR §§ 101.533, 101.1017.

153 13 CFR § 121.201, NAICS code 517210.

154 13 CFR § 121.201, NAICS code 517210 (2007 NAICS). The now-superseded, pre-2007 CFR citations were 13 CFR § 121.201, NAICS codes 517211 and 517212 (referring to the 2002 NAICS).

155 *Amendment of Parts 21 and 74 of the Commission's Rules with Regard to Filing Procedures in the Multipoint Distribution Service and in the Instructional Television Fixed Service and Implementation of Section 309(j) of the Communications Act—Competitive Bidding*, Report and Order, 10 FCC Rcd 9589, 9593, para. 7 (1995).

156 47 CFR § 21.961(b)(1).

157 47 U.S.C. § 309(j). Hundreds of stations were licensed to incumbent MDS licensees prior to implementation of Section 309(j) of the Communications Act of 1934, 47 U.S.C. § 309(j). For these pre-auction licenses, the applicable standard is SBA's small business size standard of 1500 or fewer employees.

158 *Auction of Broadband Radio Service (BRS) Licenses, Scheduled for October 27, 2009, Notice and Filing Requirements, Minimum Opening Bids, Upfront Payments, and Other Procedures for Auction 86*, Public Notice, 24 FCC Rcd 8277 (2009).

159 *Id.* at 8296 para. 73.

160 *Auction of Broadband Radio Service Licenses Closes, Winning Bidders Announced for Auction 86, Down Payments Due November 23, 2009, Final Payments Due December 8, 2009, Ten-Day Petition to Deny Period*, Public Notice, 24 FCC Rcd 13572 (2009).

161 The term "small entity" within SBREFA applies to small organizations (nonprofits) and to small governmental jurisdictions (cities, counties, towns, townships, villages, school districts, and special districts with populations of less than 50,000). 5 U.S.C. §§ 601(4)-(6). We do not collect annual revenue data on EBS licensees.

162 U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Carriers," (partial definition), http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517110&search=2012.

163 13 CFR § 121.201, NAICS code 517110.

164 U.S. Census Bureau, 2007 Economic Census, Subject Series: Information, Receipts by Enterprise Employment Size for the United States: 2007, NAICS code 517510 (rel. Nov. 19, 2010).

165 *Id.*

166 13 CFR § 121.201, NAICS Code 517410.

167 13 CFR § 121.201, NAICS Code 517919.

168 U.S. Census Bureau, 2012 NAICS Definitions, "517410 Satellite Telecommunications," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517410&search=2012.

169 U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ4, Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the United States: 2012, NAICS code 517410 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ4&prodType=table.

170 *Id.*

171 U.S. Census Bureau, 2012 NAICS Definitions, "517919 All Other Telecommunications," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517919&search=2012.

172 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ4&prodType=table.

173 U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Carriers," (partial definition), http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517110&search=2012.

174 13 CFR § 121.201, NAICS code 517110.

175 U.S. Census Bureau, 2007 Economic Census, Subject Series: Information, ""Establishment and Firm Size," NAICS code 517110 (rel. Nov. 19, 2010).

176 *Id.*

177 47 CFR § 76.901(e). The Commission determined that this size standard equates approximately to a size standard of $100 million or less in annual revenues. *Implementation of Sections of the 1992 Cable Act: Rate Regulation*, Sixth Report and Order and Eleventh Order on Reconsideration, 10 FCC Rcd 7393, 7408 (1995).

178 NCTA, Industry Data, Number of Cable Operating Companies (June 2012), http://www.ncta.com/Statistics.aspx (visited Sept. 28, 2012). Depending upon the number of homes and the size of the geographic area served, cable operators use one or more cable systems to provide video service. *See Annual Assessment of the Status of Competition in the Market for Delivery of Video Programming*, Fifteenth Report, 28 FCC Rcd 10496, 10505-06, para. 24 (2013) (*15th Annual Competition Report)*.

179 *See* SNL Kagan, "Top Cable MSOs — 12/12 Q", http://www.snl.com/InteractiveX/TopCableMSOs.aspx?period=2012Q4&sortcol=subscribersbasic&sortorder=desc. We note that, when applied to an MVPD operator, under this size standard (i.e., 400,000 or fewer subscribers) all but 14 MVPD operators would be considered small. *See* NCTA, Industry Data, Top 25 Multichannel Video Service Customers (2012), http://www.ncta.com/industry-data. The Commission applied this size standard to MVPD operators in its implementation of the CALM Act. *See Implementation of the Commercial Advertisement Loudness Mitigation (CALM) Act*, Report and Order, 26 FCC Rcd 17222, 17245-46, para. 37 (2011) (*CALM Act Report and Order*) (defining a smaller MVPD operator as one serving 400,000 or fewer subscribers nationwide, as of December 31, 2011).

180 47 CFR § 76.901(c).

181 The number of active, registered cable systems comes from the Commission's Cable Operations and Licensing System (COALS) database on Aug. 28, 2013. A cable system is a physical system integrated to a principal headend.

182 47 CFR § 76.901 (f) and notes ff. 1, 2, and 3.

183 *See* SNL KAGAN at www.snl.com/interactivex/MultichannelIndustryBenchmarks.aspx.

184 47 CFR § 76.901(f) and notes ff. 1, 2, and 3.

185 *See* SNL KAGAN at www.snl.com/interactivex/TopCable_MSOs.aspx.

186 The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to section 76.901(f) of the Commission's rules. *See*47 CFR § 76.901(f).

187 http://www.census.gov/cgi-bin/ssssd/naics/naicsrch.

188 13 CFR § 121.201; NAICS Code 517919

189 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ4&prodType=table.

190 *See supra* Part III.C.

191 *See supra* Part III.D.

192 *See id.*

193 *See supra* Part III.B.4.

194 *See supra* Part III.E.

195 *See supra* Part III.F.

196 *See id.*

197 *See supra* Part III.G.2.

198 *See id.*

199 *See id.*

200 *See id.*

201 *See supra* Part III.C.

202 5 U.S.C. § 603(c)(1)-(c)(4).

203 *See supra, e.g.*, Parts III.E.1; III.F.1

204 *See, e.g.*, ACA Comments at 57-58; WTA-NexTech Ex Parte at 1-2.

205 *See supra* paras.153-155.

206 *See supra* paras. 143, 152.

207 *See supra* para. 171.

208 *See supra* Part III.D.4.

209 *See supra* Part III.D.5.

210 *See supra* Part III.E.2.

211 *See supra* Part III.F.1.

212 *See supra* Part III.F.2.

213 *See supra* Part III.F.3.

214 *See supra* Part.

215 *See supra* Part III.I.1.

216 *See supra* Part III.I.3.

217 *See supra* Part III.I.1.

218 *See id.*

219 *See id.*

220 *See supra* Part III.I.2.

221 *See supra* Part III.I.4.

222 *See id.*

223 *See supra* Appx. B, Part I.B.

224 *See supra* Part III.E.1.

225 *See*5 U.S.C. § 801(a)(1)(A).

226 *See*5 U.S.C. § 604(b).

227 Indeed, the Obama Administration itself told the European Union that the FTC framework was strong and that nothing more, from a regulatory perspective, was needed to protect online consumers against predatory practices.

228 Statement of Chairman Tom Wheeler, Hearing before the U.S. House of Representatives Subcommittee on Communications and Technology, "Oversight of the Federal Communications Commission," Preliminary Transcript at 141 (Nov. 17, 2015).

229 *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, 2637 (2016) (Statement of Commissioner Jessica Rosenworcel).

230 Commissioner Jessica Rosenworcel Responses to Questions for the Record Submitted to the House Energy and Commerce Subcommittee on Communications and Technology's Hearing on "Oversight of the Federal Communications Commission" at 3 (July 12, 2016), *available at* http://bit.ly/2eOhvkg.

231 Federal Trade Commission Bureau of Consumer Protection Staff Comments at 8.

232 *Order* at para. 30.

233 EPIC Comments at 15.

234 Anmol Sachdeva, Google quietly updates privacy policy to drop ban on personally identifiable web tracking, *The Tech Portal* (Oct. 21, 2016), *available at* http://bit.ly/2dIvcmY.

235 Robert McMillan & Damian Paletta, Privacy Debate Flares With Report About Yahoo Scanning Emails, *Wall Street Journal* (Oct. 5, 2016), *available at* http://on.wsj.com/2dI7***o***vW.

236 Oscar Raymundo, Apple keeps track of all the phone numbers you contact using iMessage, *MacWorld* (Sept. 28, 2016), *available at* http://bit.ly/2ev8QVi.

237 Patrick Nelson, Twitter location data reveals users' homes, workplaces, *NetworkWorld* (May 18, 2016), *available at* http://bit.ly/1XmHAYf.

238 Dennis Bednarz, Amnesty International rates Microsoft's Skype among worst in privacy, *WinBeta* (Oct. 23, 2016), *available at* http://bit.ly/2f8RnDv.

239 *See, e.g.*, CTIA Comments at 16-23; Comcast Comments at 67.

240 Interestingly, when deciding that the section 222(e) exception for subscriber list information does not apply to broadband subscriber information, the order takes pains to examine the intent of Congress regarding the exception and analyzes the publishing technologies and information sharing practices that were in place at the time of enactment. In deciding that the rest of section 222 applies to broadband, however, the order breezes right past Congressional intent. Accordingly, section 222(e) is focused on "telephone books" or ""direct equivalents" (no "functional equivalents" here) but somehow section 222(c) covers applications.

241 *See, e.g.*, CTIA Comments at 27; AT&T Comments at 105-107; Verizon Comments at 57-58.

242 Verizon Comments at 58-59 (citing Whitman v. American Trucking Ass'ns, Inc., 531 U.S. 457, 468 (2001); Dole Food Co. v. Patrickson, 538 U.S. 468, 476 (2003)).

243 CTIA Comments at 34.

244 47 U.S.C. § 222(h).

245 AT&T Comments at 101.

246 *Id.* at 102.

247 Even under the Commission's erroneous theory, to which I do not subscribe, that section 222(a) provides independent authority, this type of information would have to be excluded because section 222(a) likewise uses the term proprietary. Accordingly, section 222(a) also does not cover PII. Verizon also makes the point that, at most, section 222(a) requires "that carriers 'protect the confidentiality' of information; it does not govern permissible *uses* of information" and, therefore, "is far too thin a reed to authorize the entire regulatory apparatus the Commission proposes to erect for PII that is not CPNI." Verizon Comments at 59.

248 *See, e.g.*, Verizon Comments at 56 ("The fact that the Commission has only now — after 18 years — claimed to discover new authority within Section 222 over all PII held by all telecommunications carriers, rather than only CPNI, belies that novel statutory interpretation. As the Supreme Court has cautioned, '[w]hen an agency claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy, we typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance."D') (citing Utility Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2444 (2014) (citation and internal quotation marks omitted)).

249 For example, the order now claims that a broad definition of protected information is required to better align FCC rules with the FTC approach. Putting aside for a moment the fact that the FCC does not actually line up with the FTC approach in several key respects, the FCC cannot exceed the limits of the authority delegated to it by Congress. As one commenter noted: "The law is clear that an agency cannot 'use its definitional authority to expand its own jurisdiction."D' Comcast Comments at 68 (citing Am. Bankers Ass'n v. SEC, 804 F.2d 739, 754-55 (D.C. Cir. 1986)).

250 Of course, IP addresses do not qualify as CPNI in any event, as commenters have demonstrated. *See, e.g.*, Comcast Comments at 77-81.

251 *See, e.g.*, AT&T Oct. 17, 2016 *Ex Parte* at 4.

252 *Id.*

253 *See also* AT&T Comments at 108-113; CTIA Comments at 59-73.

254 *See, e.g.*, Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech, et al., Working Paper, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* at 24-25 (filed May 27, 2016); EPIC Comments at 16 ("The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company."); Comcast Comments at 26-34; Verizon Comments at 16-24.

255 *See, e.g.*, ITTA Oct. 21, 2016 *Ex Parte* at 2-3 (noting that "Web browsing and app usage history are not considered sensitive by the FTC" that "the FTC's Privacy Report endorsed an opt-out approach towards web browsing data used for behavioral advertising" and that "[a]gainst the backdrop of the longstanding, embedded commercial practice of consumers benefiting from targeted advertising based on web browsing history, consumers do not have the same expectations of privacy in this context as they do with other categories of information.").

256 T-Mobile Oct. 14, 2016 *Ex Parte* at 2. *See also, e.g.*, Comcast Comments at 26-34; Verizon Comments at 17-24.

257 *See, e.g.*, Comcast Comments at 44-52; T-Mobile Oct. 14, 2016 *Ex Parte* at 1-2.

258 *See, e.g.*, Comcast Comments at 43; ITTA Oct. 21, 2016 *Ex Parte* at 3.

259 Comcast Comments at 43.

260 *See, e.g.*, Internet Commerce Coalition Oct. 18, 2016 *Ex Parte* at 2-3 (describing how ISPs and Internet companies use a combination of "white lists" and "black lists" that "isolate and exclude data categorized as sensitive by the FTC"); AT&T Oct. 17 *Ex Parte* at 3 ("Like any other Internet company, a broadband provider can avoid the use of sensitive information by categorizing website and app usage based on standard industry interest categories established by the Interactive Advertising Bureau ('IAB') and other leading industry associations. This process involves correlating non-content web address or app information (e.g., visit to a sports website) with a pre-established "white list" of permissible interest categories (e.g., sports lover) available from the IAB. The list of interest categories can be refined as needed to exclude any sensitive categories."); American Association of Advertising Agencies et. al Oct. 21, 2016 *Ex Parte* at 2 ("[C]ompanies across the Internet, including ISPs, have for decades used a combination of administrative and technical controls to limit the use of sensitive data for marketing and advertising purposes, absent consumer consent. These practices were developed to comply with the FTC's privacy framework and the self-regulatory program administered by the DAA."); Future of Privacy Forum Reply at 8; Google Oct. 3, 2016 *Ex Parte* at 1; NCTA Oct. 20, 2016 *Ex Parte* at 3-5; INCOMPAS Oct. 21, 2016 *Ex Parte* at 3.

261 ITIF Oct. 20, 2016 *Ex Parte* at 2.

262 Comcast Comments at 48; Technology Policy Institute Oct. 17, 2016 *Ex Parte* at 2 ("All available research suggests that opt-in consent dramatically reduces participation. Any data classified under opt-in is less likely to be available to support services, innovation, and competition, as we and others discussed in previous filings.") (citing Tom Lenard and Scott Wallsten, Technology Policy Institute, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking* (May 2016); Avi Goldfarb, Catherine E. Tucker and Liad Wagman, *Comments on Notice of Proposed Rule Making: 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'* (May 20, 2016)).

263 Comcast Comments at 48 (citing Mindi Chahal, *Consumers less likely to "opt in' to marketing than to 'opt out,' Marketing Week* (May 7, 2014), https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/).

264 *Id.* at 52.

265 And even if the Commission "fixed" the definition, it would still be precluded by the statute from placing restrictions on a broadband provider's purchase or use of third-party data. *See, e.g.*, Comcast Comments at 75-76.

266 *See, e.g.*, NCTA Oct. 20, 2016 *Ex Parte* at 8 ("The FCC has recognized that the statute permits carriers to use customer data to market products and services distinct from the underlying telecommunications service from which the data is collected. In interpreting the

degree to which Section 222 accommodates first party marketing, the Commission stated that the relevant inquiry should focus on 'the customer's reasonable expectations of privacy in connection with CPNI."D') (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, para. 41 (1999) (*1999 CPNI Order*)).

267 *See* 2012 FTC Privacy Report at 41-42; Internet Commerce Coalition Oct. 18, 2016 *Ex Parte* at 4 (explaining that "first-party marketing of an ISP's other products and services should be permissible based on implied consent, as both the FTC and Administration have previously concluded"); NCTA Oct. 20, 2016 *Ex Parte* at 8 (noting that "both the FTC and White House privacy frameworks afford companies flexibility to use customer data to engage in first-party marketing and advertising of their own services based on implied consent") (citing 2012 FTC Privacy Report at 40 ("[M]ost first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice"); The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 17 (2012) ("[C]ompanies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it.")); ITTA Oct. 21, 2016 *Ex Parte* at 2-3.

268 AT&T Oct. 17, 2016 *Ex Parte* at 2 (*1999 CPNI Order*, 14 FCC Rcd 14409, para. 42). *See also* NCTA Oct. 20, 2016 *Ex Parte* at 8; ITTA Oct. 21, 2016 *Ex Parte* at 2-3.

269 *See, e.g.*, Cox Communications Inc. October 20, 2016 *Ex Parte* at 2 ("Regulatory authorities and experts recognize first-party marketing is a wide-spread practice and a well understood tool for establishing and maintaining ... customer relationships. Both the FTC and the White House privacy frameworks specifically recognize this commonly accepted practice and permit companies to use customer data to communicate with their customers and personalize their customers' experience based on the customer's implied consent in most instances. Even existing FCC CPNI rules permit carriers to use CPNI to engage in some first-party marketing, without customer approval. Regulating such activities here would be unprecedented and would not reflect customers' current expectations of their broadband providers: to anticipate what they want and when they want it, to provide maximum value, and then tell them about it.") (citations omitted); NCTA Oct. 20, 2016 *Ex Parte* at 7-8 (also noting that broadband providers are new entrants to many products and services offered by large edge providers).

270 Cox Communications Inc. October 20, 2016 *Ex Parte* at 3.

271 Technology Policy Institute Oct. 17, 2016 *Ex Parte* at 1 ("Requiring regulatory approval for new business models is likely to reduce experimentation, and reducing the number of potential methods of paying for service is likely to harm consumers."); Nokia Oct. 14, 2016 *Ex Parte* at 2 (describing the benefits of such offers).

272 Verizon Oct. 21, 2016 *Ex Parte* at 2. *See also* CTIA Comments at 50-55.

273 *See* CTIA Comments at 50 ("Most wrongs suffered by wireless consumers are relatively small and individualized, involving excess charges on a bill, a defective piece of equipment, or the like. These claims are simply too small to justify paying a lawyer to handle the matter and, in any event, most consumers do not have the resources to do so—and a lawyer is needed to navigate the complicated procedures that apply in court. And claims of this sort cannot be brought as class actions because they involve facts specific to an individual consumer's situation .... For this large category of consumer claims, arbitration provides the only realistic option for obtaining a fair resolution of the dispute.").

274 Verizon Oct. 21, 2016 *Ex Parte* at 2 (citing 9 U.S.C. § 2).

275 CTIA Comments at 56 (citing Shearson/Am. Express, Inc. v. McMahon, 482 U.S. 220, 226-227 (1987); CompuCredit Corp. v. Greenwood, 132 S. Ct. 665, 673 (2012)).

276 CTIA Comments at 56.

277 *See, e.g.*, Verizon Comments at 74; CTIA Comments at 56-58.

278 *See, e.g.*, WISPA Comments at 27-28 (seeking a two-year extension for all the Commission rules); ITTA Sept. 30, 2016 *Ex Parte* at 3 (same).

279 *See, e.g.*, Verizon Sept. 23, 2016 *Ex Parte* at 1 ("Once rules are adopted, providers must go through an extensive and complex implementation process. Specifically, providers must perform an assessment of their existing processes and systems to determine what changes must be made; review, update, and negotiate supplier and other contracts; update written requirements documents; research, design, code, and test updates to customer care, self-serve, and back-office applications and systems; train employees and suppliers; draft customer communications; develop notice methods and periods; and set up a system for ensuring ongoing compliance. These actions will take a significant amount of time to complete, requiring approximately 18 months from the date rules are adopted.").

280 Indeed, the Obama Administration itself told the European Union that the FTC framework was strong and that nothing more, from a regulatory perspective, was needed to protect online consumers against predatory practices.

281 Statement of Chairman Tom Wheeler, Hearing before the U.S. House of Representatives Subcommittee on Communications and Technology, "Oversight of the Federal Communications Commission," Preliminary Transcript at 141 (Nov. 17, 2015).

282 *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, 2637 (2016) (Statement of Commissioner Jessica Rosenworcel).

283 Commissioner Jessica Rosenworcel Responses to Questions for the Record Submitted to the House Energy and Commerce Subcommittee on Communications and Technology's Hearing on "Oversight of the Federal Communications Commission" at 3 (July 12, 2016), *available at* http://bit.ly/2eOhvkg.

284 Federal Trade Commission Bureau of Consumer Protection Staff Comments at 8.

285 *Order* at para. 30.

286 EPIC Comments at 15.

287 Anmol Sachdeva, Google quietly updates privacy policy to drop ban on personally identifiable web tracking, *The Tech Portal* (Oct. 21, 2016), *available at* http://bit.ly/2dIvcmY.

288 Robert McMillan & Damian Paletta, Privacy Debate Flares With Report About Yahoo Scanning Emails, *Wall Street Journal* (Oct. 5, 2016), *available at* http://on.wsj.com/2dI7***o***vW.

289 Oscar Raymundo, Apple keeps track of all the phone numbers you contact using iMessage, *MacWorld* (Sept. 28, 2016), *available at* http://bit.ly/2ev8QVi.

290 Patrick Nelson, Twitter location data reveals users' homes, workplaces, *NetworkWorld* (May 18, 2016), *available at* http://bit.ly/1XmHAYf.

291 Dennis Bednarz, Amnesty International rates Microsoft's Skype among worst in privacy, *WinBeta* (Oct. 23, 2016), *available at* http://bit.ly/2f8RnDv.

292 *See, e.g.*, CTIA Comments at 16-23; Comcast Comments at 67.

293 Interestingly, when deciding that the section 222(e) exception for subscriber list information does not apply to broadband subscriber information, the order takes pains to examine the intent of Congress regarding the exception and analyzes the publishing technologies and information sharing practices that were in place at the time of enactment. In deciding that the rest of section 222 applies to broadband, however, the order breezes right past Congressional intent. Accordingly, section 222(e) is focused on "telephone books" or ""direct equivalents" (no "functional equivalents" here) but somehow section 222(c) covers applications.

294 *See, e.g.*, CTIA Comments at 27; AT&T Comments at 105-107; Verizon Comments at 57-58.

295 Verizon Comments at 58-59 (citing Whitman v. American Trucking Ass'ns, Inc., 531 U.S. 457, 468 (2001); Dole Food Co. v. Patrickson, 538 U.S. 468, 476 (2003)).

296 CTIA Comments at 34.

297 47 U.S.C. § 222(h).

298 AT&T Comments at 101.

299 *Id.* at 102.

300 Even under the Commission's erroneous theory, to which I do not subscribe, that section 222(a) provides independent authority, this type of information would have to be excluded because section 222(a) likewise uses the term proprietary. Accordingly, section 222(a) also does not cover PII. Verizon also makes the point that, at most, section 222(a) requires "that carriers 'protect the confidentiality' of information; it does not govern permissible *uses* of information" and, therefore, "is far too thin a reed to authorize the entire regulatory apparatus the Commission proposes to erect for PII that is not CPNI." Verizon Comments at 59.

301 *See, e.g.*, Verizon Comments at 56 ("The fact that the Commission has only now — after 18 years — claimed to discover new authority within Section 222 over all PII held by all telecommunications carriers, rather than only CPNI, belies that novel statutory interpretation. As the Supreme Court has cautioned, '[w]hen an agency claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy, we typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance."D') (citing Utility Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2444 (2014) (citation and internal quotation marks omitted)).

302 For example, the order now claims that a broad definition of protected information is required to better align FCC rules with the FTC approach. Putting aside for a moment the fact that the FCC does not actually line up with the FTC approach in several key respects, the FCC cannot exceed the limits of the authority delegated to it by Congress. As one commenter noted: "The law is clear that an agency cannot 'use its definitional authority to expand its own jurisdiction."D' Comcast Comments at 68 (citing Am. Bankers Ass'n v. SEC, 804 F.2d 739, 754-55 (D.C. Cir. 1986)).

303 Of course, IP addresses do not qualify as CPNI in any event, as commenters have demonstrated. *See, e.g.*, Comcast Comments at 77-81.

304 *See, e.g.*, AT&T Oct. 17, 2016 *Ex Parte* at 4.

305 *Id.*

306 *See also* AT&T Comments at 108-113; CTIA Comments at 59-73.

307 *See, e.g.*, Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech, et al., Working Paper, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* at 24-25 (filed May 27, 2016); EPIC Comments at 16 ("The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company."); Comcast Comments at 26-34; Verizon Comments at 16-24.

308 *See, e.g.*, ITTA Oct. 21, 2016 *Ex Parte* at 2-3 (noting that "Web browsing and app usage history are not considered sensitive by the FTC" that "the FTC's Privacy Report endorsed an opt-out approach towards web browsing data used for behavioral advertising" and that "[a]gainst the backdrop of the longstanding, embedded commercial practice of consumers benefiting from targeted advertising based on web browsing history, consumers do not have the same expectations of privacy in this context as they do with other categories of information.").

309 T-Mobile Oct. 14, 2016 *Ex Parte* at 2. *See also, e.g.*, Comcast Comments at 26-34; Verizon Comments at 17-24.

310 *See, e.g.*, Comcast Comments at 44-52; T-Mobile Oct. 14, 2016 *Ex Parte* at 1-2.

311 *See, e.g.*, Comcast Comments at 43; ITTA Oct. 21, 2016 *Ex Parte* at 3.

312 Comcast Comments at 43.

313 *See, e.g.*, Internet Commerce Coalition Oct. 18, 2016 *Ex Parte* at 2-3 (describing how ISPs and Internet companies use a combination of "white lists" and "black lists" that "isolate and exclude data categorized as sensitive by the FTC"); AT&T Oct. 17 *Ex Parte* at 3 ("Like any other Internet company, a broadband provider can avoid the use of sensitive information by categorizing website and app usage based on standard industry interest categories established by the Interactive Advertising Bureau ('IAB') and other leading industry associations. This process involves correlating non-content web address or app information (e.g., visit to a sports website) with a pre-established "white list" of permissible interest categories (e.g., sports lover) available from the IAB. The list of interest categories can be refined as needed to exclude any sensitive categories."); American Association of Advertising Agencies et. al Oct. 21, 2016 *Ex Parte* at 2 ("[C]ompanies across the Internet, including ISPs, have for decades used a combination of administrative and technical controls to limit the use of sensitive data for marketing and advertising purposes, absent consumer consent. These practices were developed to comply with the FTC's privacy framework and the self-regulatory program administered by the DAA."); Future of Privacy Forum Reply at 8; Google Oct. 3, 2016 *Ex Parte* at 1; NCTA Oct. 20, 2016 *Ex Parte* at 3-5; INCOMPAS Oct. 21, 2016 *Ex Parte* at 3.

314 ITIF Oct. 20, 2016 *Ex Parte* at 2.

315 Comcast Comments at 48; Technology Policy Institute Oct. 17, 2016 *Ex Parte* at 2 ("All available research suggests that opt-in consent dramatically reduces participation. Any data classified under opt-in is less likely to be available to support services, innovation, and competition, as we and others discussed in previous filings.") (citing Tom Lenard and Scott Wallsten, Technology Policy Institute, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking* (May 2016); Avi Goldfarb, Catherine E. Tucker and Liad Wagman, *Comments on Notice of Proposed Rule Making: 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'* (May 20, 2016)).

316 Comcast Comments at 48 (citing Mindi Chahal, *Consumers less likely to "opt in' to marketing than to 'opt out,' Marketing Week* (May 7, 2014), https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/).

317 *Id.* at 52.

318 And even if the Commission "fixed" the definition, it would still be precluded by the statute from placing restrictions on a broadband provider's purchase or use of third-party data. *See, e.g.*, Comcast Comments at 75-76.

319 *See, e.g.*, NCTA Oct. 20, 2016 *Ex Parte* at 8 ("The FCC has recognized that the statute permits carriers to use customer data to market products and services distinct from the underlying telecommunications service from which the data is collected. In interpreting the degree to which Section 222 accommodates first party marketing, the Commission stated that the relevant inquiry should focus on 'the customer's reasonable expectations of privacy in connection with CPNI."D') (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, para. 41 (1999) (*1999 CPNI Order*)).

320 *See* 2012 FTC Privacy Report at 41-42; Internet Commerce Coalition Oct. 18, 2016 *Ex Parte* at 4 (explaining that "first-party marketing of an ISP's other products and services should be permissible based on implied consent, as both the FTC and Administration have previously concluded"); NCTA Oct. 20, 2016 *Ex Parte* at 8 (noting that "both the FTC and White House privacy frameworks afford companies flexibility to use customer data to engage in first-party marketing and advertising of their own services based on implied consent") (citing 2012 FTC Privacy Report at 40 ("[M]ost first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice"); The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 17 (2012) ("[C]ompanies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it.")); ITTA Oct. 21, 2016 *Ex Parte* at 2-3.

321 AT&T Oct. 17, 2016 *Ex Parte* at 2 (*1999 CPNI Order*, 14 FCC Rcd 14409, para. 42). *See also* NCTA Oct. 20, 2016 *Ex Parte* at 8; ITTA Oct. 21, 2016 *Ex Parte* at 2-3.

322 *See, e.g.*, Cox Communications Inc. October 20, 2016 *Ex Parte* at 2 ("Regulatory authorities and experts recognize first-party marketing is a wide-spread practice and a well understood tool for establishing and maintaining ... customer relationships. Both the FTC and the White House privacy frameworks specifically recognize this commonly accepted practice and permit companies to use customer data to communicate with their customers and personalize their customers' experience based on the customer's implied consent in most instances. Even existing FCC CPNI rules permit carriers to use CPNI to engage in some first-party marketing, without customer approval. Regulating such activities here would be unprecedented and would not reflect customers' current expectations of their broadband providers: to anticipate what they want and when they want it, to provide maximum value, and then tell them about it.") (citations omitted); NCTA Oct. 20, 2016 *Ex Parte* at 7-8 (also noting that broadband providers are new entrants to many products and services offered by large edge providers).

323 Cox Communications Inc. October 20, 2016 *Ex Parte* at 3.

324 Technology Policy Institute Oct. 17, 2016 *Ex Parte* at 1 ("Requiring regulatory approval for new business models is likely to reduce experimentation, and reducing the number of potential methods of paying for service is likely to harm consumers."); Nokia Oct. 14, 2016 *Ex Parte* at 2 (describing the benefits of such offers).

325 Verizon Oct. 21, 2016 *Ex Parte* at 2. *See also* CTIA Comments at 50-55.

326 *See* CTIA Comments at 50 ("Most wrongs suffered by wireless consumers are relatively small and individualized, involving excess charges on a bill, a defective piece of equipment, or the like. These claims are simply too small to justify paying a lawyer to handle the matter and, in any event, most consumers do not have the resources to do so—and a lawyer is needed to navigate the complicated procedures that apply in court. And claims of this sort cannot be brought as class actions because they involve facts specific to an individual consumer's situation .... For this large category of consumer claims, arbitration provides the only realistic option for obtaining a fair resolution of the dispute.").

327 Verizon Oct. 21, 2016 *Ex Parte* at 2 (citing 9 U.S.C. § 2).

328 CTIA Comments at 56 (citing Shearson/Am. Express, Inc. v. McMahon, 482 U.S. 220, 226-227 (1987); CompuCredit Corp. v. Greenwood, 132 S. Ct. 665, 673 (2012)).

329 CTIA Comments at 56.

330 *See, e.g.*, Verizon Comments at 74; CTIA Comments at 56-58.

331 *See, e.g.*, WISPA Comments at 27-28 (seeking a two-year extension for all the Commission rules); ITTA Sept. 30, 2016 *Ex Parte* at 3 (same).

332 *See, e.g.*, Verizon Sept. 23, 2016 *Ex Parte* at 1 ("Once rules are adopted, providers must go through an extensive and complex implementation process. Specifically, providers must perform an assessment of their existing processes and systems to determine what changes must be made; review, update, and negotiate supplier and other contracts; update written requirements documents; research, design, code, and test updates to customer care, self-serve, and back-office applications and systems; train employees and suppliers; draft customer communications; develop notice methods and periods; and set up a system for ensuring ongoing compliance. These actions will take a significant amount of time to complete, requiring approximately 18 months from the date rules are adopted.").

31 FCC Rcd. 13911 (F.C.C.), 31 F.C.C.R. 13911, 65 Communications Reg. (P&F) 1349, 2016 WL 6538282

End of Document

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
AT&T Inc.	)	File No.: EB-TCD-18-00027704
	)	NAL/Acct. No.: 202032170004
	)	FRN: 0005193701

NOTICE OF APPARENT LIABILITY FOR FORFEITURE AND ADMONISHMENT

Adopted: February 28, 2020 **Released: February 28, 2020**

By the Commission: Chairman Pai and Commissioner O'Rielly issuing separate statements; Commissioner Rosenworcel dissenting and issuing a statement; Commissioner Starks approving in part, dissenting in part and issuing a statement.

TABLE OF CONTENTS

I. INTRODUCTION

1. The wireless phone is a universal fixture of modern American life. Ninety-six percent of all adults in the United States own a mobile phone.[1] Of those mobile phones, the majority are smartphones that provide Internet access and apps, which Americans use to read, work, shop, and play. More than almost any other product, consumers "often treat [their phones] like body appendages."[2] The

[1] Pew Research Center, Demographics of Mobile Device Ownership and Adoption in the United States – Mobile Fact Sheet (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[2] Pew Research Center, Americans' Views on Mobile Etiquette, Chapter 1: Always on Connectivity (Aug. 26, 2015), https://www.pewresearch.org/internet/2015/08/26/chapter-1-always-on-connectivity/.

wireless phone goes wherever its owner goes, at all times of the day or night. For most consumers, the phone is always on and always within reach.[3] And every phone must constantly share its (and its owner's) location with its wireless carrier because wherever it goes, the networks must be able to find it to know where to route calls.

2. The American public and federal law consider such information highly personal and sensitive—and justifiably so. As the Supreme Court has observed, location data associated with wireless service "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[4] Section 222 of the Communications Act requires carriers to protect the confidentiality of certain customer data related to the provision of telecommunications service, including location information. The Commission has advised carriers that this duty requires them to take "every reasonable precaution" to safeguard their customers' information.[5] The Commission has also warned carriers that the FCC would "[take] resolute enforcement action to ensure that the goals of section 222 are achieved."[6]

3. Today, we do exactly that. In this Notice of Apparent Liability, we propose a penalty of $57,265,625 against AT&T Inc. (AT&T or Company) for apparently violating section 222 of the Communications Act and the Commission's regulations governing the privacy of customer information. We find that AT&T apparently disclosed its customers' location information, without their consent, to a third party who was not authorized to receive it. In addition, even after highly publicized incidents put the Company on notice that its safeguards for protecting customer location information were inadequate, AT&T apparently continued to sell access to its customers' location information for nearly a year without putting in place reasonable safeguards—leaving its customers' data at unreasonable risk of unauthorized disclosure.

II. BACKGROUND

A. Legal Framework

4. The Act and the Commission's rules govern and limit telecommunications carriers' use and disclosure of certain customer information. Section 222(a) of the Act imposes a general duty on telecommunications carriers to "protect the confidentiality of proprietary information" of "customers."[7] Section 222(c) establishes specific privacy requirements for "customer proprietary network information" or CPNI, namely information relating to the "quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[8] The Commission has issued regulations implementing the privacy requirements of section 222 (CPNI Rules),[9] and has amended those rules over time. Most relevant to this

[3] *Id.*

[4] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (internal quotation marks and citations omitted).

[5] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007) (*2007 CPNI Order*).

[6] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[7] 47 U.S.C. § 222(a).

[8] 47 U.S.C. § 222(c), (h)(1)(A) (emphasis added). "Telecommunications service" is defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(53). The mobile voice services provided by AT&T are "telecommunications services." *See* 47 U.S.C. § 332(c)(1); H.R. Conf. Rep. No. 104-458 at 125 (1996) ("This definition [of 'telecommunications service'] is intended to include commercial mobile service.").

[9] *See* 47 CFR § 64.2001 *et seq.*

proceeding are the rules that the Commission adopted governing customer consent to the use, sharing, or disclosure of CPNI and those relating to a carrier's duty to discover and protect against unauthorized access to CPNI.

5. *Customer Consent to Disclose CPNI.* With limited exceptions, a carrier may only use, disclose, or permit access to CPNI with customer approval.[10] Generally, carriers must obtain the "opt-in approval" of their customers before disclosing CPNI.[11] This means that a carrier must obtain the customer's "affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request . . . ."[12]

6. Prior to 2007, the Commission's rules permitted telecommunications carriers to share customers' CPNI with joint venture partners and independent contractors for certain purposes based on a customer's "opt-out approval." This means that a customer is deemed to have consented to a particular use of, disclosure of, or access to CPNI after being given notice of the use, disclosure, or access and not objecting thereto.[13] However, in response to the problem of data brokers on the web selling call detail and other telephone records procured without customer consent,[14] the Commission amended its rules in the *2007 CPNI Order* to require carriers to obtain opt-in approval from a customer before disclosing that customer's CPNI to a carrier's joint venture partner or independent contractor.[15] The Commission recognized that "once the CPNI is shared with a joint venture partner or independent contractor, the carrier no longer has control over it and thus the potential for loss of this data is heightened."[16] Given that observation, the Commission concluded that sharing of data with partners and contractors "warrants a requirement of express prior customer authorization,"[17] which would allow individual consumers to determine if they want to bear the increased risk associated with sharing CPNI with independent contractors and joint venture partners.[18] The Commission emphasized the importance of obtaining express consent particularly because a carrier cannot simply rectify the harms resulting from a breach by terminating its agreement, "nor can the Commission completely alleviate a customer's concerns about the privacy invasion through an enforcement proceeding."[19] The Commission further concluded that contractual safeguards cannot obviate the need for explicit customer consent, as such safeguards would not change the fact that the risk of unauthorized CPNI disclosures increases when such information is

[10] 47 U.S.C. § 222(c)(1) ("Except as required by law *or with the approval of the customer*, a telecommunications carrier that receives or obtains [CPNI] by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.") (emphasis added).

[11] 47 CFR § 64.2007(b).

[12] *Id.* § 64.2003(k).

[13] *See id.* § 64.2003(l).

[14] *See 2007 CPNI Order*, 22 FCC Rcd at 6928, para. 2.

[15] *Id.* at 6947-53, paras. 37-49.

[16] *Id.* at 6948, para. 39.

[17] *Id.*; *see also id.* at 6949, para. 41 ("Further, we find that an opt-in regime will clarify carriers' information sharing practices because it will force carriers to provide clear and comprehensible notices to their customers in order to gain their express authorization to engage in such activity.").

[18] *2007 CPNI Order*, 22 FCC Rcd at 6950, para. 45.

[19] *Id.* at 6949, para. 42.

provided by a carrier to a joint venture partner or independent contractor.[20] Thus, with limited exceptions, a carrier may only use, disclose, or permit access to CPNI with the customer's opt-in approval.[21]

7. *Reasonable Measures to Safeguard CPNI.* The Commission also recognized in the *2007 CPNI Order* that reliance on the opt-in approval requirement alone is insufficient to protect customers' interest in the privacy of their CPNI, finding that at least some data brokers had obtained access to call detail information because of the ease with which a person could pretend to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records, a practice known as "pretexting."[22] In light of the harms arising from pretexting, the Commission adopted rules requiring carriers to "take reasonable measures to *discover* and *protect* against attempts to gain unauthorized access to CPNI."[23] To provide some direction on how carriers should protect against pretexting schemes, the Commission included in its amended rules customer authentication requirements tailored to whether a customer is seeking in-person, online, or over-the-phone access to CPNI.[24] It also adopted password and account notification requirements.[25]

8. The Commission made clear that the specific customer authentication requirements it adopted were "minimum standards" and emphasized the Commission's commitment "to taking resolute enforcement action to ensure that the goals of section 222 [were] achieved."[26] Where there is evidence of an unauthorized disclosure, the Commission specified that it will infer from that evidence that a carrier's practices were unreasonable unless the carrier offers evidence demonstrating that its practices were reasonable.[27] This burden-shifting approach reflects the Commission's expectation that carriers "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information,"[28] while also heeding industry warnings that adopting prescriptive rules detailing specific security practices could be counterproductive.[29] The Commission chose to "allow carriers to determine what specific measures will best enable them to ensure compliance with" the requirement that they remain vigilant in their protection of CPNI.[30] The Commission expected that carriers would employ

[20] *Id.* at 6952, para. 49.

[21] *See* 47 CFR § 64.2007(b).

[22] *2007 CPNI Order*, 22 FCC Rcd at 6928, para. 1 & n.1.

[23] 47 CFR § 64.2010(a) (emphasis added).

[24] *See id.* § 64.2010(b)-(d).

[25] *See id.* § 64.2010(e)-(f).

[26] *2007 CPNI Order*, 22 FCC Rcd at 6959–60, para. 65.

[27] *See id.*at 6959, para. 63 (noting that where there is evidence of an unauthorized disclosure, the Commission "will infer . . . that the carrier did not sufficiently protect that customer's CPNI" and that "[a] carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue"). This approach, which the Commission articulated in the context of pretexting, is particularly applicable here, where a fundamental issue is whether the Company had reasonable measures to ensure that its customers had in fact consented to the disclosure of their CPNI with third parties. Since at least 2007, it has been foreseeable that entities seeking to gain unauthorized access to CPNI would use false pretenses—of one sort or another—to do so.

[28] *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 (citing 47 CFR § 64.2010(a)).

[29] *See 2007 CPNI Order*, 22 FCC Rcd at 6945-46, paras. 33-36 (citing, *inter alia*, CTIA Comments (May 1, 2006) at 6 (arguing that "prescriptive rules detailing specific security practices that must be followed by all carriers do nothing more than provide a road map to criminals and erect a barrier that prevents carriers from adopting new security measures in response to constantly evolving threats")).

[30] *2007 CPNI Order*, 22 FCC Rcd at 6945-46, para. 34.

effective protections that are best suited to their particular systems.[31] Carriers are not expected to eliminate every vulnerability to the security of CPNI, but they must employ "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[32] They must also take reasonable measures to protect the confidentiality of CPNI—a permanent and ongoing obligation to police disclosures and ensure proper functioning of security measures.[33] A variety of government entities provide guidance and publish best practices that are intended to help companies evaluate the strength of their information security measures.[34]

9. *Section 217.* Finally, the Act makes clear that carriers cannot disclaim their statutory obligations to protect their customers' CPNI by delegating such obligations to third parties. Section 217 of the Act provides that "the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person."[35]

10. *The Scope of the Commission's Authority.* Our authority to bring action for violations of section 222 of the Communications Act and the CPNI Rules is limited to actions against providers of telecommunications services[36] and providers of interconnected Voice over Internet Protocol services.[37] To the extent that other entities act unfairly or deceptively by mishandling or failing to protect wireless customer location information, federal civil enforcement authority rests with the Federal Trade Commission, an agency of general jurisdiction.[38]

---

[31] *Id.* at 6959, para. 64. The Commission explained, for example, that although it declined to impose "audit trail" obligations on carriers at that time, it "expect[ed] carriers through audits or other measures to take reasonable measures to discover and protect against" activity indicative of unauthorized access. *Id.* Similarly, the Commission expected that a carrier would "encrypt its CPNI databases if doing so would provide significant additional protection . . . at a cost that is reasonable given the technology a carrier already has implemented," but the Commission did not specifically impose encryption requirements. *Id.*

[32] 47 CFR § 64.2010(a).

[33] *See 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 ("We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.").

[34] For example, the National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. NIST publishes cybersecurity and privacy frameworks which feature instructive practices and guidelines for organizations to reference. The publications can be useful in determining whether particular cybersecurity or privacy practices are reasonable by comparison. The model practices identified in the NIST and other frameworks, however, are not legally binding rules, and we do not consider them as such here. The Federal Trade Commission (FTC) and the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) also offer guidance related to managing data security risks. *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (NIST Cybersecurity Framework); NIST, The NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 (Jan. 16, 2020), https://www.nist.gov/privacy-framework/privacy-framework; FTC, Start with Security: A Guide for Business, Lessons Learned from FTC Cases (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Communications Security, Reliability and Interoperability Council, CSRIC Best Practices, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.

[35] 47 U.S.C. § 217.

[36] 47 U.S.C. § 222.

[37] *2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras 54-59.

[38] 15 U.S.C. § 45(a)(2) ("The [Federal Trade] Commission is hereby empowered and directed to prevent persons . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.").

B. Factual Background

1. AT&T's Wireless Network Services and Customer Location Information

11. AT&T provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on AT&T's wireless network.[39] The mobile phones of AT&T subscribers, like those of customers of other carriers, periodically register with nearby network signal towers.[40] AT&T uses the information generated from this registration activity to ensure the proper functioning of its network and to provide the services to which its customers subscribe.[41] Because AT&T knows the location of its network signal towers, AT&T is able to calculate the approximate geographic location of the mobile phones communicating with its towers. This type of location information—which is created even when the customer does not have an active established connection, such as a voice call or data usage—may at times be helpful to consumers. For example, in emergencies, the location of a customer's mobile phone can enable first responders and law enforcement to assist. Location information is also used for non-emergency location-based services, such as roadside assistance, delivery tracking, and fraud prevention.[42] Other widely used forms of location-based services include real-time mapping, navigation, and local weather forecasting services, although these generally rely on GPS-based location finding rather than customer location information derived from the provision of wireless service.[43]

2. AT&T's Location-Based Services Business Model

12. Until [redacted] AT&T provided location-based service providers access to its customers' location information through a chain of contract-based business arrangements. AT&T sold access to customer location information to companies known as "location information aggregators," who then resold access to such information to third-party location-based service providers or in some cases to intermediary companies who then resold access to such information to location-based service providers. AT&T had arrangements with two aggregators: LocationSmart and Zumigo (the Aggregators).[44] Each Aggregator, in turn, had arrangements with numerous location-based service providers. The most basic form of these relationships is illustrated in Fig. 1:

---

[39] *See* AT&T Inc., 2018 Annual Report, https://investors.att.com/~/media/Files/A/ATT-IR/financial-reports/annual-reports/2018/complete-2018-annual-report.pdf.

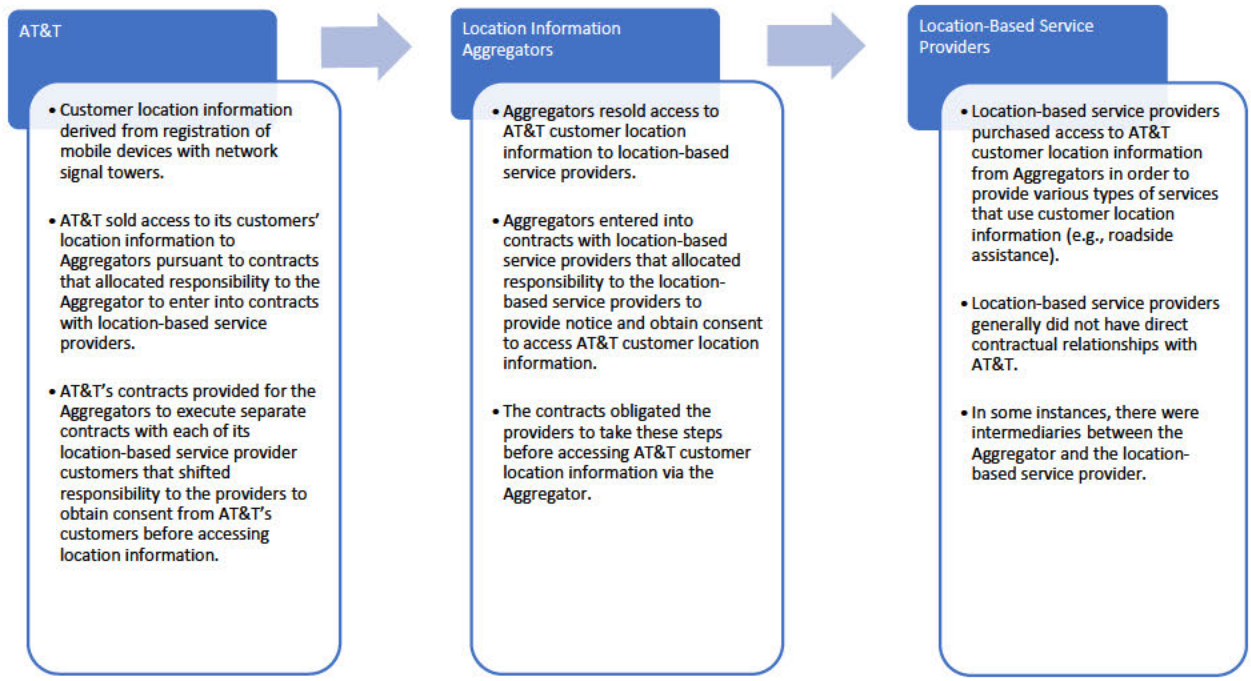
[40] *See* FCC, Wireless Telecommunications Bureau, *Location-Based Services: An Overview of Opportunities and Other Considerations*, at 11-12 (May 2012), https://docs.fcc.gov/public/attachments/DOC-314283A1.pdf (discussing how location information is derived from communications between mobile phones and cellular base stations).

[41] Response to Initial Letter of Inquiry from AT&T, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 11-12, Response to Question 4 (Nov. 14, 2018) (on file in EB-TCD-18-00027704) (LOI Response).

[42] *Id.* at 8-11, Response to Question 3.

[43] Location information derived from the interaction between a subscriber's mobile phone and a carrier's network is distinct from the location information generated by capabilities on a subscriber's phone, which calculates a phone's location by measuring its distance to Global Positioning System (GPS) satellites and through other capabilities. Many popular apps use device-based location functionality to provide consumers with location-based service (including mapping and navigation services) and do not rely on the location information collected by carriers. There are a variety of location positioning methods and protocols in wireless networks that are based on mobile radio signals, and some of these radio signals are configurable and/or controlled by the network operator and not the consumer. *See* Rohde & Schwarz, *LTE Location Based Services Technology Introduction – White Paper*, at 11, Fig. 7 – Supported positioning methods in LTE (Sept. 2013), https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/LTE_LBS_White_Paper.pdf.

[44] AT&T does not contend that its customers consented to these arrangements with the Aggregators.



13. AT&T apparently sold access to its customers' location information, directly or indirectly, to [redacted] third parties, including the two Aggregators. The following [redacted] entities purchased access to AT&T customer location information from LocationSmart [redacted] 3Cinteractive [redacted] SpatialPoint; [redacted] Windstream Communications; [redacted].[45] Three of LocationSmart's customers (3Cinteractive, SpatialPoint, and Windstream Communications) were intermediaries who resold access to AT&T customer location information to, respectively, [redacted].[46] The following [redacted] entities purchased access to AT&T customer location information from Zumigo: [redacted].[47] Finally, AT&T asserts that it sold access to customer location information directly to the following [redacted] location-based

[45] LOI Response at 8-10, Response to Question 3; Response to Letter of Inquiry from AT&T, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, LBS Chart Attachment (Feb. 21, 2020) (on file in EB-TCD-18-00027704) (Further Response).

[46] LOI Response at 10-11, Response to Question 2; Further Response, LBS Chart Attachment.

[47] LOI Response at 10, Response to Question 3; Further Response, LBS Chart Attachment.

service providers [redacted][48]

14. According to AT&T, it structured its location-based service program in accordance with CTIA's "Best Practices and Guidelines for Location Based Services" (CTIA Guidelines)[49] and contractually required the Aggregators and location-based service providers to comply with the CTIA Guidelines.[50]

15. *AT&T's Contract Provisions Governing the Handling of Customer Location Information.* Pursuant to its contracts with the two Aggregators, AT&T provided the Aggregators with access to AT&T customer location information and authorized them to share it with individual location-based service providers after AT&T had reviewed a "Use Case" submitted to AT&T by the location-based service provider.[51] Each Use Case purported to describe the purposes for which the location-based service provider would use the location information, and the process it would use for getting opt-in consent from AT&T's customers to the sharing of that information with the location-based service provider.[52] According to AT&T, it only approved Use Cases for specific purposes and only when the location-based service provider committed to obtaining the affirmative, opt-in consent of the individual whose device was to be located.[53] Pursuant to the terms of AT&T's contracts with the Aggregators, the Aggregators were obligated to have contracts with their location-based service provider customers that prohibited the location-based service providers from retrieving customer location information at their discretion or disclosing it to any third parties that were not known to and approved by the Company.[54] AT&T's contracts required that its Aggregators share consent records with AT&T, and according to AT&T it reviewed such consent records on a daily basis.[55]

16. AT&T's contracts obligated the Aggregators to monitor the practices of the location-based service providers, including compliance with the requirement that location-based service providers notify and collect affirmative customer consent for any use of location information.[56] According to AT&T, it also required the Aggregators and location-based service providers to attest that they were complying with AT&T's contractual requirements.[57] AT&T also asserts that it required the Aggregators to provide evidence daily of each of the consents received by the Aggregators from the location-based service providers.[58] A consent record consisted of an identifier associated with the customer, a date and time stamp of the customer's consent, the version of the notice presented to the customer, and other data purporting to enable AT&T to track the consent.[59] AT&T did not verify the consent before providing

[48] LOI Response at 11, Response to Question 3; Further Response, LBS Chart Attachment.

[49] CTIA, Best Practices and Guidelines for Location Based Services, https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services (last visited Feb. 5, 2020).

[50] LOI Response at 1, Introduction.

[51] *Id.* at 4, Response to Question 1.

[52] *Id.* at 4-5, Response to Question 1.

[53] *Id.*

[54] *Id.* at 6-7, Response to Question 1.

[55] *Id.* at 14, Response to Question 5.

[56] *Id.* at 6, Response to Question 1.

[57] *Id.* at 5, Response to Question 1.

[58] Response to Supplemental Letter of Inquiry from AT&T, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 11, Response to Question 9 (May 24, 2019) (on file in EB-TCD-18-00027704) (Supplemental LOI Response).

[59] Supplemental LOI Response at 11, Response to Question 9.

access to the location data; instead it claimed to verify on a daily basis that each request for information was tied to a consent record.[60] AT&T's contracts with the Aggregators also obligated the Aggregators to comply with various information security requirements, including vulnerability-scanning, encryption, data segregation, access limitation, and other requirements.[61]

17. *AT&T's Right to Suspend or Terminate Access to Location Information.* AT&T had broad authority under its contracts with the Aggregators to quickly terminate access to customer location information. The contracts permitted the Company to suspend the transmission of location information to any location-based service provider that it believed was not complying with its obligations. AT&T also had the right to terminate its relationship with each Aggregator, at its discretion, if among other reasons, the Aggregator engaged in conduct that exposed AT&T to "sanctions, liability, prosecution or other adverse consequences under applicable law," breached the contract in a way that presented an "imminent risk of harm to AT&T [or] AT&T's customers," or otherwise "abuse[d] or misuse[d] AT&T's network or service."[62] Except for the five location-based service providers with whom it contracted directly,[63] AT&T lacked a direct contractual relationship with the location-based service providers to whom it permitted the Aggregators to disclose its customers' location information.

18. *AT&T's Internal Reviews and Auditing*. According to AT&T, between January 2016 and May 2019, it conducted five reviews or audits of its disclosure of customer location information to third parties.[64] The Company claims that three of the five analyses are subject to attorney-client privilege, however, and submitted only the results of the two reviews that AT&T treated as non-privileged.[65] The first non-privileged analysis, conducted from August 2017 to February 2018, involved AT&T's review of its controls over certain disclosures of customer location information for the provision of location-based services. That audit "identified issues with: (i) consistency in the approval processes regarding the provision of subscriber data to third parties; (ii) reporting practices regarding the completeness of subscriber consents; and (iii) record retention practices regarding subscriber consents."[66] AT&T averred that it had remediated all issues identified in the audit by June 6, 2018.[67] The second non-privileged audit was a review of the Aggregators' compliance with AT&T information security requirements for third-party vendors, analyses conducted from July to August 2018 (in the case of LocationSmart) and July to October 2018 (in the case of Zumigo).[68] AT&T found that LocationSmart was not in compliance with

[60] *Id.* at 11, Response to Question 9.

[61] LOI Response at 6-7, Response to Question 1.

[62] LOI Response at ATT-LOI-00013380, Response to Request for Documents No. 3, 2016 Master Agreement between AT&T Corp. and TechnoCom Corporation d/b/a LocationSmart, at Section 8.2 - Termination or Suspension (executed on Feb. 17, 2016 by Mario Proietti, CEO for LocationSmart and Glenn C. Girard, Assoc Dir. Customer Contracts-AT&T Services, Inc.) (AT&T-LocationSmart Agreement); LOI Response at ATT-LOI-00025859, Response to Request for Documents No. 3 2014 Master Agreement between AT&T Corp. and Zumigo, Inc., Section 8.2 – Termination or Suspension (executed on Apr. 25, 2014 by Chira Bakshi, CEO for Zumigo and Ana Castaneda, Contract Specialist for AT&T) (AT&T-Zumigo Agreement). The contracts required the Aggregators to indemnify AT&T for various types of claims, including those arising from privacy violations, but did not provide for any other remedy—such as direct restitution to affected customers—in the event of breach.

[63] *See* LOI Response at 11, Response to Question 3 (explaining that AT&T contracted directly with [redacted]); Further Response, LBS Chart Attachment.

[64] LOI Response at 19-21, Response to Question 11; Supplemental LOI Response at 16, Response to Question 15.

[65] LOI Response at 20-21, Response to Question 11; Supplemental LOI Response at 16, Response to Question 15.

[66] LOI Response at 20, Response to Question 11.

[67] *Id.*

[68] *Id.*

four of the Company's information security requirements (including requirements for password/PIN expiration intervals and encryption of AT&T data in transit).[69] AT&T also found that Zumigo was not in compliance with eight of the Company's information security requirements (including requirements for consistently remediating medium-risk vulnerabilities, having controls to safeguard against unauthorized activities[,]" and requiring privileged users to use multi-factor authentication when accessing AT&T data in the cloud).[70] According to AT&T, LocationSmart and Zumigo adequately remediated all of the identified issues in the second audit.[71]

19. Claiming privilege for the other three audits, AT&T did not share the findings from those reviews with the Enforcement Bureau. Instead, AT&T identified the general topic(s) of and entities that were the subjects of the audits, and with respect to the first audit offered a one sentence description of changes the Company made in response to the audit.[72] The first audit was a privileged compliance review of AT&T's data monitoring practices with respect to the Aggregators and location-based service providers, conducted from February 2017 to April 2018.[73] The second privileged review, begun in May 2018, focused on Securus, LocationSmart, and 3Cinteractive (an intermediary working with Securus and LocationSmart), as well as Aggregators and location-based service providers more generally.[74] The third privileged review, initiated in January 2019, focused on Zumigo and MicroBilt's provision of location-based service.[75] AT&T declined to produce any other information to the Enforcement Bureau concerning those privileged reviews.

3. AT&T's Actions After the Publication of Reports of Unauthorized Access to and Use of Customer Location Information

20. On May 10, 2018, the *New York Times* reported on security breaches involving AT&T's (and other carriers') practice of selling access to customer location information.[76] Specifically, Securus Technologies, Inc. (Securus), a provider of telecommunications services to correctional facilities throughout the United States, also operated a "location-finding service" that enabled law enforcement and corrections officials to access the location of a mobile device belonging to customers of major wireless carriers, including AT&T, *without* the device owner's knowledge or consent.[77] According to the article, Securus required users to certify that they had the authority to perform location searches and to upload an appropriate document, such as a court order or warrant, that provided legal authorization for the location request.[78] Securus did not, however, assess the adequacy of the purported legal authorizations submitted by users of its location-finding service.[79]

---

[69] *Id.* at 19, Response to Question 11.

[70] *Id.* at 20, Response to Question 11.

[71] LOI Response at 19-20, Response to Question 11; Supplemental LOI Response at 9, Response to Question 7.

[72] LOI Response at 21, Response to Question 11; Supplemental LOI Response at 9, Response to Question 7.

[73] LOI Response at 21, Response to Question 11. According to AT&T, as a result of this review, it implemented revisions to the audit and monitoring plan for its identity verification services; revised the provisions of its contracts with the Aggregators and location-based service providers regarding data security, data monitoring, and auditing; and updated its own internal policy documents. *Id.*

[74] *Id.* at 20, Response to Question 11.

[75] Supplemental LOI Response at 8-9, Response to Question 6.

[76] *See* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018), https://www nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.

[77] *Id.*

[78] *Id.*

[79] *Id.*

21. The *New York Times* article described how then-Missouri Sheriff Cory Hutcheson used the Securus service, without legal authorization, to access location information about anyone he pleased.[80] Another newspaper later reported that Hutcheson submitted thousands of unauthorized location requests via the Securus service between 2014 and 2017, in some cases "upload[ing] entirely irrelevant documents including his health insurance policy, his auto insurance policy, and pages selected from Sheriff training manuals" in lieu of genuine legal process.[81] Among those apparently tracked by Hutcheson in this manner were his predecessor as Sheriff, a Missouri Circuit Judge, and at least five highway patrol officers.[82]

22. AT&T does not deny the existence of the Securus location-finding service nor the abuse of that system by Hutcheson. Instead, AT&T asserts that the Securus location-finding service was not an AT&T-authorized Use Case. According to AT&T [redacted][83] As described by AT&T, Securus should only have sought access to AT&T customer information if, in connection with a collect call from a correctional facility, a call recipient was informed, via a prerecorded message, that their location information would be collected, and they had pressed a button to consent to the collection of their location information to proceed with the call.[84] Based [redacted] (which was transmitted from Securus to an intermediary called 3Cinteractive, then from 3Cinteractive to LocationSmart, and finally from LocationSmart to AT&T), AT&T transmitted a customer's location information to Securus, via LocationSmart and 3Cinteractive, and then to [redacted].[85]

23. According to AT&T, [redacted][86] At the same time, AT&T concedes that [redacted][7] Securus continued to make this method of access available to law enforcement from at least 2014 until AT&T terminated Securus's access to AT&T customer location information in [redacted] following the *New York Times* article.[88]

---

[80] *Id.*

[81] *See* Doyle Murphy, *Ex-Missouri Sheriff Cory Hutcheson Sentenced to 6 Months in Prison*, Riverfront Times (Apr. 29, 2019), https://www riverfronttimes.com/newsblog/2019/04/29/ex-missouri-sheriff-cory-hutcheson-sentenced-to-6-months-in-prison.

[82] *See* Complaint, *William T. Cooper et al. vs. Sheriff Cory Hutcheson*, Case: 1:17-cv-00073 (E.D. Mo. May 8, 2017).

[83] LOI Response at 17, Response to Question 8.

[84] *See* Securus Technologies Location-based Services (LBS) White Paper, Feb. 21, 2018 (on file in EB-TCD-18-00027704) at 5; *see also* LOI Response at 17, Response to Question 8.

[85] Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018), https://www nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html; LOI Response at 17, Response to Question 8.

[86] LOI Response at 17, Response to Question 8.

[87] *Id.*

[88] The *New York Times* reported that Hutcheson's misuse of the Securus service began in 2014, and evidence independently obtained by the Enforcement Bureau confirms that fact. *See* Department of Justice Evidence Records (on file in EB-TCD-18-00027704).

24. On May 10, 2018, in response to the *New York Times* report and a May 8, 2018 letter about the Securus program that Senator Ron Wyden sent to AT&T,[89] [redacted].[90] A few days later, on May 16, 2018, AT&T [redacted] 3Cinteractive's [redacted].[91] According to AT&T, [redacted]."[92] As a result, AT&T asserts [redacted]

25. In June 2018, AT&T announced that [redacted].[93] It did not specify how long the process would take. [redacted].[94] In November 2018, AT&T told Enforcement Bureau staff that it planned to implement "enhanced" notice and consent measures for location information-sharing in 2019,[95] but has offered no evidence that it did so.[96]

26. [redacted].[97]

---

[89] *See* Letter from Senator Ron Wyden to Randall L. Stephenson, President and Chief Executive Officer, AT&T Inc. (May 8, 2018), https://www.wyden.senate.gov/imo/media/doc/wyden-securus-location-tracking-letter-to-att.pdf.

[90] LOI Response at 18, Response to Question 8. Senator Wyden's letter was dated May 8, 2018, and AT&T states [redacted] *Id.*

[91] LOI Response at 18, Response to Question 8.

[92] *Id.* at 21, Response to Question 12.

[93] Supplemental LOI Response at 1, Introduction.

[94] Further Response, LBS Chart Attachment. More specifically, AT&T asserts that [redacted] *Id.*

[95] Specifically, AT&T stated that beginning in 2019, it would provide enhanced notice to customers who had given their consent to share location information with location-based service providers by sending them an SMS notice informing them of the sharing and explaining how they can change their consent options. LOI Response at 15, Response to Question 6. AT&T also stated that "[l]ater in 2019," it would provide a "second layer of consent for certain Use Cases" by requiring customers to reply to an SMS message to authorize their sharing of location information. LOI Response at 15, Response to Question 6.

[96] In its Supplemental LOI Response, AT&T does not state whether or when it had implemented the enhanced notice and consent measures described in its LOI Response. *See* Supplemental LOI Response at 15, Response to Question 6.

[97] Supplemental LOI Response at 13, Response to Question 10; Supplemental LOI Response at AT&T-LOI-00025696, Response to Question 10; Response to Request for Documents No. 5.

27. On January 8, 2019, *Motherboard* published an article titled "I Gave a Bounty Hunter $300. Then He Located Our Phone."[98] The article alleged that access to AT&T and other telecommunications carriers' customer location information was sold and resold, with little or no oversight, within the bail bonds industry, and that this led to consumers being tracked without their knowledge or consent.[99] To illustrate the practice, the article described how a "bounty hunter" paid by *Motherboard* used his contacts in the bail bonds industry to access the location of a T-Mobile user's mobile phone.[100] The bounty hunter reportedly received the information from an employee of a bail bonds company that was a customer of MicroBilt.[101] MicroBilt, in turn, was a customer of Zumigo, an Aggregator that received customer location information from AT&T and the other major wireless carriers.[102]

28. AT&T admits [redacted][103] Specifically, although AT&T had [redacted].[105] AT&T agrees that Zumigo and [redacted].[107] Second, Zumigo [redacted][108]

29. On January 10, 2019, AT&T announced that "[i]n light of recent reports about misuse of location services, we decided to eliminate all location aggregator services—even those with clear consumer benefits" and stated that its location-based service program would end in March 2019.[109] According to AT&T, it terminated the access to its customer location information to an additional [redacted][110] AT&T also claims that it sent notices of termination to the two Aggregators

[98] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8. 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-MicroBilt-zumigo-tmobile.

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] Supplemental LOI Response at 13, Response to Question 10.

[104] *Id.* at 4, Response to Question 2.

[105] *Id.* at 13, Response to Question 10.

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *See* Alfred Ng, *AT&T is Cutting Off All Location-Data Sharing Ties in March*, CNET (Jan. 11, 2019), https://www.cnet.com/news/at-t-is-cutting-off-all-location-data-sharing-ties-by-march/.

[110] More specifically, AT&T asserts that it terminated such access for the following entities on the following dates: [redacted]

on [redacted],[111] [redacted].[112] In other words, the Company did not finally terminate its location-based service program until [redacted],[113] or [redacted] days from when the *New York Times* first reported on the Securus location-finding service, as well as the abuse of that service by Hutcheson.

30. *Commission Investigation*. The Enforcement Bureau launched an investigation in May 2018, immediately following the *New York Times* report of unauthorized location tracking involving Securus. The Bureau issued a Letter of Inquiry to AT&T seeking information and documents regarding, among other things, its practices and procedures involving customer location information, its relationships with location information aggregators and location-based service providers, the specific allegations of unauthorized access to location information involving Securus that were detailed by the *New York Times*, and any other identified instances of unauthorized access to location information dating back to 2016.[114] The Bureau requested additional information and documents from AT&T in 2019.[115] AT&T submitted responses to the Bureau's initial and supplemental LOIs, as well as approximately 28,000 pages of responsive documents concerning its sale of access to its customer location information to third parties.[116]

III. DISCUSSION

31. We find that AT&T apparently willfully and repeatedly violated section 222 of the Act and the accompanying CPNI Rules by improperly disclosing customer location information to Hutcheson without customer approval. The customer location information at issue constitutes CPNI, and it may be used only as permitted by section 222 and our CPNI Rules.

32. We also find that the Company apparently violated section 222 of the Act and section 64.2010(a) of the CPNI Rules by failing to protect the confidentiality of its customers' CPNI and by failing to employ "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[117] In particular, we find that for almost a year after AT&T became aware of Securus's

---

[redacted] Further Response, LBS Chart Attachment.

[111] Supplemental LOI Response at 2, Response to Question 1. Also, in January 2019, AT&T sent notices terminating the provision of location information to [redacted] *Id.*

[112] Supplemental LOI Response at 2, Response to Question 1; Further Response, LBS Chart Attachment. More specifically, AT&T asserts that it [redacted] *Id.*

[113] Supplemental LOI Response at 1-2, Introduction.

[114] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Jeanine Poltronieri, Assistant Vice President, External Affairs, AT&T Services, Inc. (Sept. 13, 2018) (on file in EB-TCD-18-00027704) (LOI).

[115] Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Jeanine Poltronieri, Assistant Vice President, External Affairs, AT&T Services, Inc. (Apr. 8, 2019) (on file in EB-TCD-18-00027704) (Supplemental LOI).

[116] *See* LOI Response; *see also* Supplemental LOI Response.

[117] 47 CFR § 64.2010(a).

unapproved location-finding service—and thereby had notice that the "consent records" it received through indirect arrangements with location-based service providers were not reliable indicia of customer consent—the Company's continued reliance on such attenuated consent mechanisms and ineffective monitoring tools apparently did not meet the reasonableness requirement of section 64.2010(a).

A. Customer Location Information Constitutes CPNI

33. We start with a preliminary point: Federal law protects the privacy of the customer location information at issue here. In other words, customer location information is CPNI under the Act and our rules.

34. The customer location information at issue falls squarely within section 222's definition of CPNI. Section 222 defines CPNI as information relating to the "quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[118] To qualify as location-related CPNI, then, section 222 requires that information meet only two criteria: It must (1) "relate[]" to the "location . . . of a telecommunications service," and (2) it must be "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[119]

35. The customer location information at issue here meets these two criteria. *First*, it relates to the location of a telecommunications service, i.e., AT&T's commercial mobile service.[120] The location data was derived from the wireless mobile devices of AT&T's customers communicating with nearby network signal towers to signal the location of those devices. A wireless mobile device undergoes an authentication and attachment process to the carrier's network, via the closest towers. After a mobile device is authenticated and logically attached to a wireless network, it may be (1) connected (sending/receiving data/voice) or (2) idle. In either state, the carrier must be aware of and use the device's location in order for it to enable customers to send and receive calls. AT&T is therefore providing telecommunications service to these customers whenever it is enabling the customer's device to send and receive calls—regardless of whether the device is actively in use for a call. This view finds ample support in Commission precedent, including the *2013 CPNI Declaratory Ruling*, which indicates that the policy considerations remain the same throughout a consumer's use of a mobile device, including the entire process through which the device stands ready to make or receive a call.[121]

36. *Second*, AT&T's wireless customers made this information available to AT&T because of the carrier-customer relationship embodied in their service agreements. AT&T provides wireless telephony services to the affected customers because they have chosen AT&T to be their provider of telecommunications service—in other words, they have a carrier-customer relationship. The customer location information to which AT&T sold access was generated by the service that AT&T provided to those customers. In short, AT&T's customers provided their wireless location data to AT&T because of

[118] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

[119] 47 U.S.C. § 222(h)(1)(A) (defining "customer proprietary network information").

[120] *See* 47 U.S.C. § 332(c)(1) (providing that "a person engaged in the provision of a service that is a commercial mobile service shall, insofar as such person is so engaged, be treated as a common carrier for purposes of this chapter"), (d)(1) (defining "commercial mobile service").

[121] *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609, 9616, para. 22 (2013) (*2013 CPNI Declaratory Ruling*) (discussing "telephone numbers of calls dialed and received and the location of the device at the time of the calls" and "the location of a customer's use of a telecommunications service"); *id.* at 9617, para. 25 (concluding that even locations of failed calls fall within the definition of CPNI).

their customer-carrier relationship with AT&T, so that AT&T could use that location information to provide them with a telecommunications service. That makes the location information CPNI.

37. Resisting this straightforward conclusion, AT&T denies that the location information was collected by the carrier "solely by virtue of the carrier-customer relationship"[122] on the ground that wireless customers receive both telecommunications services and non-common-carrier data services—and that the latter constitute the bulk of its network traffic.[123] We disagree. The definition of CPNI does not depend on the amount of telecommunications services relative to a carrier's other service offerings. Although AT&T might also provide non-common-carrier services to the same customer, it has that relationship with the customer because the customer has chosen AT&T to be its provider of telecommunications service—that is, by virtue of the carrier-customer relationship. We reject AT&T's overly narrow reading of this common-sense meaning of the statute, which would have the perverse effect of eliminating the statutory protections of the most sensitive types of CPNI contrary to the clear intent of Congress.

38. We remain likewise unpersuaded that location information generated and collected by carriers while a phone is in standby mode (i.e., while a phone is on, but not actively in use during a call) is materially different than any other customer location information generated or collected by the Company. The definition of CPNI does not distinguish between the location information collected by carriers from a mobile device during a telephone call and the location information generated when the device is turned on and available for calls but not engaged in transmitting a voice conversation. In both cases, the location "relates" to the carrier's provision of telecommunications service to the customer, and the customer's location is available to the carrier solely by virtue of its carrier-customer relationship.

39. Nor does the use of the term "call location information" elsewhere in section 222 imply that every use of the term "location" in section 222 refers only to the location of the device when actively in use during a call. Arguably, the provision allowing sharing of "call location information" with public safety, family members, and others in emergency situations appears to contemplate allowing the sharing of a device's location outside the context of individual calls, suggesting that even that more specific term includes all location information.[124] But even if the term "call location information" elsewhere in section 222 is limited to information about the location of voice telephone calls, there is no reason to conclude the same about the broader term "location." Given the plain meaning of "location" and the obvious sensitivity of information that a carrier has about the location of its customers, we see no reason to interpret the statute as excluding the location of customer devices when they are not engaged in calls.

40. AT&T nevertheless asserts that it derived location information for aggregators and location-based service providers "through means that are independent of its provision of telecommunications services," and that when it delivers telecommunications services to mobile devices, it "generates location information via a separate process for the purpose of delivering telecommunications services."[125] In making this assertion, AT&T fails to refute the central point that the Company necessarily obtains location information by virtue of its provision of the telecommunications service when it enables the connection of a customer's device to its network for the purpose of sending and receiving calls, and the customer has no choice but to reveal that location to the carrier. We find AT&T's

[122] That said, AT&T emphasized that it nevertheless collected and attempted to protect and treat location information in an essentially equivalent manner to CPNI. The Company asserts that it obeyed the core requirements of section 222 and the CPNI Rules by (1) disclosing the information to third parties only with their customers' informed consent, and (2) protecting the data through extensive safeguards. LOI Response at 11-12, Response to Question 4; Supplemental LOI Response at 5-6, Response to Question 3.

[123] Supplemental LOI Response at 3-4, Response to Question 2.

[124] *See* 47 U.S.C. § 222(d)(4)(A)-(C).

[125] LOI Response at 11-12, Response to Question 4.

arguments regarding the classification of location information unpersuasive, particularly in light of the more straightforward reading of the statutory text.

41. Having concluded that the customer location information at issue is CPNI under section 222 of the Act, we likewise conclude that the rules governing consent to the use, disclosure, and sharing of CPNI and protection of CPNI, which incorporate the statutory definition by reference,[126] also apply to that customer location information.

B. AT&T Apparently Violated Section 222 and the CPNI Rules by Disclosing CPNI to a Missouri Sheriff Without Authorization

42. AT&T apparently violated section 222(c)(1) of the Act and section 64.2007 of the Commission's rules when it disclosed customer location information to Hutcheson. Section 222(c)(1) states that carriers shall only use, disclose, or permit access to individually identifiable CPNI with the approval of the customer.[127] Section 64.2007 of the Commission's rules states that a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.[128]

43. The evidence reflects that Hutcheson used the Securus service to obtain the location information of AT&T customers. AT&T shared the information with LocationSmart, which then shared it with 3Cinteractive, which then shared it with Securus,[129] which then disclosed it to Hutcheson—despite the absence of AT&T customer consent for the disclosures. The evidence shows that between 2014 and 2017, at least 147 AT&T customers' location information was disclosed to Hutcheson, via Securus, without the customers' consent.[130] Notwithstanding the misconduct of Hutcheson, each such disclosure constitutes a violation of section 222(c)(1) of the Act and section 64.2007 of the Commission's rules for which AT&T is responsible.

44. AT&T does not dispute that it disclosed its customers' location information to Hutcheson without the customers' consent and in the absence of an exception that would make the consent requirement inapplicable. Instead, AT&T argues that [redacted].[131] AT&T explains that notwithstanding the contractual customer notice and authorization provisions it imposed on LocationSmart, and that LocationSmart then imposed on 3Cinteractive and Securus, [redacted][132]

45. We find these arguments unavailing. AT&T is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred. Rather, sections 222 and 217 of the Act make clear that ultimate responsibility for these unauthorized disclosures rests with the carrier—in this case, AT&T. The restrictions on the use and disclosure of CPNI in section 222 of the Act expressly apply to "telecommunications carriers."[133] Section

[126] 47 CFR § 64.2003(g).

[127] 47 U.S.C. § 222(c)(1). There are exceptions in circumstances not relevant here.

[128] 47 CFR § 64.2007(b). There are exceptions in circumstances not relevant here.

[129] LOI Response at 17; Response to Question 8.

[130] *See* Department of Justice Evidence Records (on file in EB-TCD-18-00027704).

[131] LOI Response at 16-18, Response to Question 8.

[132] *Id.*

[133] The Commission extended the applicability of its CPNI Rules to interconnected Voice over Internet Protocol providers in 2007. *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59. Congress acknowledged this

222 broadly prohibits telecommunications carriers from using CPNI collected in connection with providing telecommunications service for any purpose other than providing such service or other services "necessary to, or used in" providing such service (for example, publishing directories).[134] Apart from a few exceptions not relevant here,[135] section 222 allows a telecommunications carrier to use CPNI for other purposes only where "required by law or with the approval of the customer."[136] In short, the obligation to protect CPNI falls on *telecommunications carriers*; the carrier must obtain customer approval to use, disclose, or permit someone else to access the CPNI for any purpose not strictly related to the purpose for which it was provided to the carrier.

46. To allow a telecommunications carrier to share CPNI with an entity that is not subject to section 222 without imposing sufficient controls could deprive its customers of the statutory protections of section 222.[137] The Commission recognized this problem in 2007, responding to the reality at that time that individuals' calling records were available for sale on numerous websites.[138] As a result, the Commission determined that it was necessary to further limit the sharing of CPNI with others outside a customer's carrier by requiring carriers to obtain opt-in approval from a customer even before disclosing that customer's CPNI to a carrier's joint-venture partner or independent contractor. "Opt-in approval" is defined as a method that "requires that *the carrier* obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of *the carrier's* request."[139] This was necessary in part "because a carrier is no longer in a position to personally protect the CPNI once it is shared."[140]

47. We recognize that carriers have long relied on third parties—aggregators and/or location-based service providers—to act on their behalf to obtain their customers' consent to the sharing of their CPNI.[141] But such reliance has never meant absolution for carriers. Instead, section 217 of the Act provides that "the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier."[142] In other words, a carrier cannot avoid its statutory obligations by assigning them to a third party.

48. So it is unsurprising that the Commission has consistently held that carriers are responsible for the conduct of third parties acting on the carrier's behalf.[143] Just as the Commission

---

extension in its 2008 amendments to section 222. *See* Pub. L. No. 110-283, § 301, 122 Stat. 2620, 2625-26, *codified at* 47 U.S.C. § 222(d)(4), (f)(1), (g).

[134] *See* 47 U.S.C. § 222(c)(1).

[135] *See* 47 U.S.C. § 222(d) (specifying four exceptions).

[136] 47 U.S.C. § 222(c)(1).

[137] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14881, paras. 46-47 (2002).

[138] *2007 CPNI Order*, 22 FCC Rcd at 6928-29, para. 2.

[139] 47 CFR § 64.2003(k) (defining "opt-in approval") (emphases added).

[140] *2007 CPNI Order*, 22 FCC Rcd at 6948, para. 39.

[141] To the extent that the third parties were *not* acting on behalf of the carrier, the carrier itself would have provided those third parties with access to its customers' CPNI without obtaining for themselves the approval required by section 222(c)(1)—thus violating federal law. AT&T does not appear to argue that situation is present here.

[142] 47 U.S.C. § 217.

[143] *See, e.g.*, *Long Distance Consol. Billing Co.*, Forfeiture Order, 34 FCC Rcd 1871, 1874-75, para. 10 (2019); *Eure Family Ltd. Partnership*, Memorandum Opinion and Order, 17 FCC Rcd 21861, 21863-64, para. 7 (2002); *Long Distance Direct, Inc.*, Memorandum Opinion and Order, 15 FCC Rcd 3297, 3300, para. 9 (2000); *Vista Services*

recently held that a carrier was "not relieved of liability [for slamming] simply because it provided its telemarketers with a policy manual and sales script and directed its telemarketers to market its service 'through lawful means,'"[144] a carrier is not relieved of its section 222 obligations simply because it contracts with third parties and relies on them to obtain the statutorily required approval—even if it imposed similar obligations by contract. Similarly, in 2012, the Commission found it unnecessary to impose on Lifeline providers an explicit obligation that they, rather than their agents or representatives, review all documentation of eligibility.[145] That was because the carriers themselves would be legally responsible for the acts and omissions of those agents: "[Carriers] may permit agents or representatives to review documentation of consumer program eligibility for Lifeline. However, the [carrier] remains liable for ensuring the agent or representative's compliance with the Lifeline program rules."[146]

49. At bottom, AT&T may not have it both ways. If AT&T was relying on third parties to satisfy its obligations to obtain consent, then it is liable for those third parties' failures as it would be if they had been the failures of AT&T itself. If not, then AT&T effectively granted those third parties the capability to access the CPNI of its customers without customer approval.

50. In sum, we find that AT&T apparently violated section 222(c)(1) of the Act and section 64.2007(b) of our rules in connection with its unauthorized disclosures of CPNI to Hutcheson.[147]

C. AT&T Apparently Failed to Take Reasonable Measures to Protect CPNI

51. AT&T apparently violated section 222 of the Act and section 64.2010 of our rules by failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information.[148] The May 10, 2018 *New York Times* report on the Securus and Hutcheson breaches exposed serious inadequacies with the safeguards on which AT&T relied to protect its customers' location information. Our investigation shows that AT&T failed to promptly address those inadequacies. We therefore conclude that AT&T apparently failed to take reasonable measures in a timely fashion to protect its customers' CPNI following that report.

52. In plain terms, our rules recognize that companies cannot prevent all data breaches, but require carriers to take reasonable steps to safeguard their customers' CPNI and to discover attempts to gain access to their customers' CPNI. In the absence of an unauthorized disclosure, the Commission bears the burden of demonstrating that the methods employed by a carrier to safeguard CPNI were unreasonable. But where an unauthorized disclosure *has* occurred—as here—this burden shifts to the carrier. In that case, the Commission treats the unauthorized access to a subscriber's CPNI as *prima facie* evidence that a carrier failed to sufficiently protect the information.[149] The responsible carrier then

Corp., Order of Forfeiture, 15 FCC Rcd 20646, 20650, para. 9 (2000); *American Paging, Inc. (of Virginia)*, Memorandum Opinion and Order, 12 FCC Rcd 10417, 10420, para. 11 (1997); *Triad Broadcasting Co., Inc.*, Memorandum Opinion and Order, 96 FCC 2d 1235, 1244, para. 21 (1984); *see also Silv Communication Inc.*, Notice of Apparent Liability for Forfeiture, 25 FCC Rcd 5178, 5180, para. 5 n.18 (2010).

[144] *Long Distance Consol. Billing Co.*, 34 FCC Rcd at 1875, para. 10.

[145] *Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6708-09, para. 110 (2012).

[146] *Id.* at 6709, para. 110.

[147] 47 U.S.C. § 222(c)(1); 47 CFR § 64.2007(b).

[148] 47 CFR § 64.2010(a); *see also 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 ("We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.").

[149] *2007 CPNI Order*, 22 FCC Rcd at 6959–60, para. 65.

shoulders the burden of proving the reasonableness of its measures to (1) detect unauthorized attempts to access CPNI and (2) protect CPNI from such attempts.[150]

53. AT&T thus bears the burden of demonstrating that the measures it took to safeguard CPNI were reasonable both before and after the Securus and Hutcheson breaches. To meet this burden, AT&T offers three general categories of safeguards that it claims collectively amounted to a reasonable attempt to protect customer location information. In general, AT&T relied on the same safeguards both before and after the May 10, 2018 report of the Securus and Hutcheson breaches.

54. *First*, AT&T asserts that it vetted and approved each Aggregator, location-based service provider, and Use Case in which location information was shared.[151] Through its contractual requirement that customer location information be used only for approved Use Cases, AT&T attempted to limit how the location data to which it sold access would be used by the companies that purchased it and how those companies would obtain the consent to receive such data.[152] In addition to requiring that any data it shared be used only in accordance with an approved Use Case, AT&T annually reviewed its approved Use Cases and required Aggregators and location-based service providers to attest that they were complying with AT&T's contractual requirements.[153] Yet the Securus and Hutcheson breaches demonstrate that this contractual safeguard alone was insufficient to prevent the misuse of the customer location information to which AT&T sold access. Notwithstanding AT&T's contract with LocationSmart, LocationSmart's contract with 3Cinteractive, and 3Cinteractive's contract with Securus [redacted], Securus was able to set up a separate program to access and disclose customer location information and operate it *for at least four years* in a manner inconsistent with its [redacted].

55. *Second*, AT&T required Aggregators and location-based service providers to supply notice to and obtain the consent of customers prior to sharing any location information.[154] In so doing, AT&T emphasizes that it structured its location-based service program in accordance with the CTIA Guidelines and required the Aggregators and location-based service providers to comply with the CTIA Guidelines, which call on location-based service providers to receive notice and consent to use and sharing of location information.[155] Those guidelines focus on best practices for notice and consent by location-based service providers. But they do not include best practices recommendations for carriers that sell access to their customers' location information to location-based service providers. For example, they do not offer guidance to carriers on how to assure that location-based service providers comply with a contractual obligation to access location information only after furnishing proper notice and receiving customer consent.

56. Aggregators and location-based service providers, in turn, were required to send a record of the consent they received to AT&T.[156] AT&T explains that "[o]n a daily basis, AT&T conduct[ed] a review to determine that each request for location information is tied to a consent record indicating that the customer consented to the disclosure of location information."[157] However, this safeguard relied

[150] *Id.*

[151] LOI Response at 3-4, Response to Question 1.

[152] *Id.* at 4, Response to Question 1.

[153] *Id.* at 5, Response to Question 1.

[154] *Id.*

[155] LOI Response at 1, Introduction; *see also* CTIA, Best Practices and Guidelines for Location Based Services, https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services.

[156] *Id.*

[157] LOI Response at 14, Response to Question 5.

almost entirely on the unverified assertions of the Aggregators and location-based service providers to whom AT&T sold access to customer location information. Notwithstanding the contractual requirements that AT&T imposed on the Aggregators (and that the Aggregators were required to impose on the location-based service providers), AT&T did not submit evidence from its own audits or other sources to show that the Aggregators actually held location-based service providers to these obligations. And whatever the value of such review on paper, it clearly failed in practice as AT&T's "daily" practice of reviewing consent records allowed the Securus and Hutcheson breaches to continue *for at least four years* without AT&T's knowledge.

57. *Third and finally*, AT&T imposed a variety of information security requirements on the Aggregators to whom it sold access to customer location information—for example, that they have a published privacy policy, industry-standard security controls, and that they monitor and audit compliance with their agreement with AT&T.[158] But, as AT&T explains, AT&T generally had a direct contractual relationship only with Aggregators, who in turn were required to impose these terms on location-based service providers.[159] In other words, these contractual requirements were largely passed down to the entities responsible for obtaining consent and that used the location information of AT&T's customers through an attenuated chain of downstream contracts.

58. To enforce the requirements, AT&T would have needed to take steps to determine whether they were actually being followed. AT&T has not shown that it did so. While AT&T apparently conducted limited reviews of its policies and practices related to disclosing location information to third parties, it has largely declined to provide the results of those assessments to the Enforcement Bureau.[160] And those that it did provide to the Bureau found vulnerabilities with both the consent mechanisms and with Aggregators' compliance with AT&T's contractual requirements.[161] These included but were not limited to "issues with: (i) consistency in the approval processes regarding the provision of subscriber data to third parties; (ii) reporting practices regarding the completeness of subscriber consents; and (iii) record retention practices regarding subscriber consents."[162]

59. In sum, the safeguards implemented by AT&T to protect customer location information against unauthorized use relied almost entirely on contractual agreements, passed on to location-based service providers through an attenuated chain of downstream contracts. AT&T's efforts to ensure compliance with these agreements apparently consisted almost entirely of reviewing unverified vendor-created consent records. What limited power AT&T had to verify these records or otherwise demand compliance, it did not seem to meaningfully exercise. And it had almost no other visibility or apparent awareness into how the location data it sold was used or protected. While business relationships often rely on trusting a counterparty to honor its contractual obligations, it is hard to conclude that such trust alone was a reasonable safeguard here—even in the absence of an unauthorized disclosure. This is particularly so in light of the industry's experience with pretexting, which should have apprised AT&T of the high risk that bad actors would attempt to gain unauthorized access to AT&T's customers' CPNI, particularly by trying to find ways around any systems AT&T put in place to authenticate that its customers were actually providing consent to third parties' access to their location information.

60. Setting aside the inadequacy of AT&T's safeguards before disclosure of the Securus and Hutcheson breaches, AT&T was on clear notice that its safeguards were inadequate after the disclosure, and so we focus on the actions that AT&T took, or failed to take, after discovery of that breach. We find that AT&T has apparently failed to demonstrate that its safeguards were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018. The Securus incident laid

[158] *Id.* at 6-7, Response to Question 1.

[159] LOI Response at 3, Response to Question 1.

[160] *Id.* at 19-21, Response to Question 11.

[161] *Id.*

[162] *Id.* at 20, Response to Question 11.

bare the fundamental weaknesses of AT&T's safeguards with respect to the third parties to which it entrusted its customers' location information. Nevertheless, for [redacted] days after that incident came to light, AT&T continued to sell access to its customers' location information under the same system that had allowed (1) Securus to provide location information in a manner inconsistent with its [redacted] and (2) Hutcheson to easily and improperly access AT&T customer location information. Relying on demonstrably faulty safeguards in the wake of this incident does not appear to have been reasonable.

61. There are several commonsense measures that AT&T could have taken following the May 2018 *New York Times* article. One obvious measure would have been to identify the companies involved in the Securus breach and terminate their access until it could verify that these companies had properly safeguarded its customers' location data. AT&T did so only in part. [redacted] But it did not suspend the access of LocationSmart, the Aggregator that had the contractual obligations to monitor Securus and 3Cinteractive's access to AT&T's customer data, for another [redacted] days ([redacted]).

62. Another measure would have been to promptly ascertain the full scope and extent of the Securus breach. AT&T notes that it did conduct an "internal review of Securus, LocationSmart, and 3Cinteractive, and more generally of Location Aggregators and LBS Providers" following the May 2018 *New York Times* article.[163] But because AT&T has declined to provide the details of this audit to the Commission's Enforcement Bureau, it is impossible for us to conclude that (1) the scope of the investigation was reasonable or (2) that AT&T took reasonable steps in light of its audit findings, which AT&T has likewise refused to provide to the Bureau. Again, it is *AT&T* that bears the burden of demonstrating the reasonableness of its practices in the wake of an unauthorized disclosure.[164]

63. What is more, the full impact of Securus's unauthorized access to CPNI apparently remains unknown to AT&T even to this day. That's because AT&T claims that [redacted][165] Rather than shielding AT&T from liability, that admission shows the inherent weakness of AT&T's arguments that its contract-based model provided reasonable protection of CPNI. If AT&T cannot compel Securus to cooperate with AT&T's investigation into unauthorized access to its customers' location information, it cannot say that the same contract-based system actually protects customer location information from unauthorized access by other entities. Whatever Securus's justification for denying AT&T's request, its refusal is further evidence of the fact that AT&T disclosed CPNI to a third party over which it had little or no control or authority.

64. Another measure AT&T could have taken was to determine whether the Securus incident was an isolated occurrence or whether it was indicative of a broader vulnerability with AT&T's program. This would mean examining not only the companies involved in the Securus incident, but also taking broader efforts to audit similarly situated companies' compliance with AT&T's contractual safeguards. Yet AT&T has offered nothing more than a broad assertion to suggest that it took steps after the publication of the *New York Times* article to identify and remedy the broader security deficiencies exposed by revelations about Securus's location-finding service. AT&T has provided no evidence that it sought to determine whether there were other unauthorized programs being operated that allowed access to AT&T customer location information in ways that contravened AT&T's contracts with its Aggregators. Nor has AT&T provided evidence that it sought to determine whether there were abuses of unauthorized or authorized programs that were giving users unauthorized access to AT&T customer location information. Nor has AT&T demonstrated that the weaknesses in its oversight of access to customer

[163] LOI Response at 20, Response to Question 11.

[164] *2007 CPNI Order*, 22 FCC Rcd at 6959–60, para. 65.

[165] LOI Response at 21, Response to Question 12.

location information by LocationSmart, 3Cinteractive, and Securus were not present for the other [redacted] entities to whom AT&T sold access.

65. Unfortunately, the apparent failure of AT&T to impose reasonable safeguards on its program to sell access to customer location information after the *New York Times* article is not merely a matter of theory. On January 8, 2019, *Motherboard* reported on its success purchasing access to customer location information that was disclosed to MicroBilt.[166] Although not the carrier that was the subject of the article, AT&T [redacted][167] Specifically, although AT&T had [redacted][168] MicroBilt apparently disclosed location information to its own corporate customers, which included members of the bail bonds industry. And, as the *Motherboard* article demonstrated, purchasing access to customer location information provided by a carrier to MicroBilt was not a difficult thing to do—nor did it appear to be difficult for *Motherboard* to unearth the vulnerability.

66. Stepping back, this means that the safeguards that AT&T had in place for the [redacted] days after the *New York Times* article apparently failed to discover yet another case of unauthorized access to customer location information, by a whole separate set of entities than were involved in the Securus breach. Or to put it differently, after the Securus incident had demonstrated serious systematic flaws in AT&T's safeguards to protect CPNI, AT&T continued to rely on those same safeguards so that it could continue to sell access to more than [redacted] separate entities—so it is no surprise that those safeguards were subject to an almost identical security vulnerability, reflecting the Company's failure to respond appropriately to the data breaches involving Hutcheson.[169] And AT&T apparently recognized as much on January 10, 2019, when it announced that "[i]n light of recent reports about misuse of location services, we decided to eliminate all location aggregator services."[170] But even then, AT&T did not fully terminate its sale of access to customer location information until [redacted]—a full [redacted] days after the *Motherboard* article.[171]

67. Yet another measure that AT&T could have taken was to enhance the measures it used to verify customer consent—for example, by directly confirming with customers that they have actually consented to the use of their location information. After the Securus and Hutcheson breaches came to light, AT&T had good reason to doubt the accuracy of the consent records it received from any location-based service provider. As AT&T itself explains, [redacted]

---

[166] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8. 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-MicroBilt-zumigo-tmobile.

[167] Supplemental LOI Response at 13, Response to Question 10.

[168] *Id.*

[169] A category of the NIST Cybersecurity Framework's "Recover" Core Function is to improve based on past experience. *See* NIST Cybersecurity Framework at 43 (improvements mean that "response activities are improved by incorporating lessons learned from current and previous detection/response activities"). *See also* NIST, Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, at vi (Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf (discussing "information security continuous monitoring," which involves "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions," as a critical component of an organization's cyber risk management framework).

[170] *See* Alfred Ng, *AT&T is cutting off all location-data sharing ties in March*, CNET (Jan. 11, 2019), https://www.cnet.com/news/at-t-is-cutting-off-all-location-data-sharing-ties-by-march/.

[171] Supplemental LOI Response at 1-2, Introduction.

[redacted][172] Thus, the Securus and Hutcheson breaches made clear that instead of developing a consent mechanism that would allow AT&T to confirm that its customers had actually consented to the sharing of their location information, it created a system that required it to rely on the unverified representations of third-party location-based service providers that had financial incentives to access that information.

68. Again, AT&T apparently recognized as much when it told staff in November 2018 that, beginning in 2019, it would provide enhanced notice to customers who had given their consent to share location information with location-based service providers by sending them an SMS notice informing them of the sharing and explaining how they can change their consent options.[173] AT&T also said that "[l]ater in 2019," it would provide a "second layer of consent for certain Use Cases" by requiring customers to reply to an SMS message to authorize their sharing of location information.[174] But there is no evidence that AT&T ever implemented any of these modifications to its consent verification process. Instead, it left in place a consent verification system that it knew to be flawed for as many as [redacted] days for [redacted] separate entities to access customer location information, thereby increasing the risk of further unauthorized access.

69. Finally, the surest safeguard to protect its customers' CPNI would have been for AT&T to expeditiously terminate its location-based service program. If AT&T could not reasonably safeguard the customer location information that it sold access to, then it should have ceased to sell access to that information. Yet it was only after the *Motherboard* article was published—[redacted] days after the Securus incident was disclosed—that AT&T finally accelerated shutting down its flawed location-based service program.[175] AT&T terminated access to customer location information for [redacted] location-based service providers or intermediaries over the course of eight months between May and the end of December 2018.[176] In contrast, AT&T terminated the access of [redacted] and the remaining [redacted] entities to whom it sold access to customer location information over the course of 3 months in early 2019.[177] AT&T admits that [redacted] which AT&T fully terminated on [redacted]—or [redacted] days after the May 2018 *New York Times* report.[178] AT&T's contracts with the Aggregators included a provision giving AT&T the right to terminate the agreements at any time upon written notice.[179] The time for AT&T to have exercised this provision was far earlier—shortly after the Company learned that Securus had been operating a secret location-finding service without AT&T's authorization and despite AT&T's existing safeguards. AT&T fails to explain its inaction in the face of an obvious risk to its customers' privacy.

70. AT&T apparently did not take any of these reasonable steps. Nor has it presented evidence that it took other reasonable measures that might have cured the flaws exposed by the Securus

[172] LOI Response at 3, Introduction.

[173] *Id.* at 15, Response to Question 6.

[174] *Id.*

[175] *See* Alfred Ng, *AT&T is cutting off all location-data sharing ties in March,* CNET (Jan. 11, 2019), https://www.cnet.com/news/at-t-is-cutting-off-all-location-data-sharing-ties-by-march/; Further Response, LBS Chart Attachment.

[176] Further Response, LBS Chart Attachment.

[177] *Id.*, LBS Chart Attachment.

[178] Supplemental LOI Response at 1-2, Introduction.

[179] AT&T-LocationSmart Agreement, Section 8.2; AT&T-Zumigo Agreement, Section 8.2.

and MicroBilt breaches. The ease with which Hutcheson accessed location information about any individual of his choosing should have alerted AT&T to its lack of visibility into how the location-based service providers were making use of the location information that it was entrusting to the Aggregators and that it needed to change its practices or terminate its location-based service program. After learning of Hutcheson's practices, AT&T placed its customers' location information at continuing risk of unauthorized access through its failure to terminate its program or impose reasonable safeguards to protect its customers' location information. For these reasons, we conclude that AT&T apparently failed in its obligation under section 222 and our rules to have reasonable measures in place to discover and protect against attempts to gain unauthorized access to its customers' CPNI.[180]

D. Proposed Forfeiture

71. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against any entity that "willfully or repeatedly fail[s] to comply with any of the provisions of [the Act] or of any rule, regulation, or order issued by the Commission . . . ."[181] Here, section 503(b)(2)(B) of the Act authorizes us to assess a forfeiture against AT&T of up to $204,892 for each day of a continuing violation, up to a statutory maximum of $2,048,915 for a single act or failure to act.[182] In exercising our forfeiture authority, we must consider the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[183] In addition, the Commission has established forfeiture guidelines; they establish base penalties for certain violations and identify criteria that we consider when determining the appropriate penalty in any given case.[184] Under these guidelines, we may adjust a forfeiture upward for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator.[185]

72. The Commission's forfeiture guidelines in section 1.80(b) of the Commission's rules do not establish a base forfeiture for violations of section 222(c) or the accompanying CPNI Rules.[186] Nor has the Commission calculated forfeitures for the unauthorized disclosure of CPNI previously. Thus, we look to the base forfeitures established or issued in analogous cases for guidance. In 2011 and 2012, the Bureau issued Forfeiture Orders for failure to timely file the annual CPNI compliance certifications required by section 64.2009(e) of the Commission's rules (*CPNI Cases*).[187] Similar to this case, the

[180] 47 CFR § 64.2010(a); *see also 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 (stating that the Commission expects carriers to "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information").

[181] 47 U.S.C. § 503(b).

[182] *See* 47 U.S.C. § 503(b)(2)(B); 47 CFR § 1.80(b)(2). These amounts reflect inflation adjustments to the forfeitures specified in section 503(b)(2)(B) ($100,000 per violation or per day of a continuing violation and $1,000,000 per any single act or failure to act). The Federal Civil Penalties Inflation Adjustment Act of 1990, Pub. L. No. 101-410, 104 Stat. 890, as amended by the Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, Sec. 31001, 110 Stat. 1321, requires the Commission to adjust its forfeiture penalties periodically for inflation. *See* 28 U.S.C. § 2461 note (4). The Enforcement Bureau announced the Commission's inflation-adjusted penalty amounts for 2020 on December 27, 2019. *See Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 19-1325 (EB 2019).

[183] 47 U.S.C. § 503(b)(2)(E).

[184] 47 CFR § 1.80(b)(8), Note to paragraph (b)(8).

[185] *Id*.

[186] 47 CFR § 1.80(b).

[187] *See, e.g., Jahan Telecommunication, LLC*, Order of Forfeiture, 27 FCC Rcd 6230 (EB-TCD 2012); *Nationwide Telecom, Inc*., Order of Forfeiture, 26 FCC Rcd 2440 (EB-TCD 2011); *Diamond Phone, Inc*., Order of Forfeiture, 26 FCC Rcd 2451 (EB-TCD 2011); *USA Teleport, Inc*., Order of Forfeiture, 26 FCC Rcd 2456 (EB-TCD 2011); *88*

driving purpose behind the Commission's actions in the *CPNI Cases* was enforcing the protections that Congress established in section 222(c) for consumers' proprietary information. In the *CPNI Cases*, the base forfeiture was between $20,000 and $29,000 for failure to file or failure to respond to a Bureau order to file certain information regarding the carriers' CPNI filings. In 2014, the Commission issued a Notice of Apparent Liability against TerraCom, Inc. and YourTel America, Inc., for apparently violating section 222(a) of the Act.[188] In *TerraCom*, the carriers' failure to secure their computer systems revealed detailed personal information belonging to individual Lifeline program applicants; the Commission proposed a penalty of $8,500,000 in that case.[189]

73. Neither the *CPNI Cases* nor *TerraCom* are directly on point with the conduct in this case, but nevertheless are helpful in context. We find that AT&T's failures to protect CPNI were much more egregious and fundamental than the failures of the carriers in the *CPNI Cases*, which involved the failure to file compliance certifications required by Commission rules. The potential harm that flowed from failure to establish reasonable safeguards to protect customer location information from unauthorized access was significantly greater than the harm posed by a carrier's failure to file CPNI certifications in a timely manner. Consumers carry their smartphones or wireless phones on their person or within easy reach at all times of the day or night. The precise physical location of a wireless device is an effective proxy for the precise physical location of the person to whom that phone belongs at that moment in time. Exposure of this kind of deeply personal information puts those individuals at significant risk of harm—physical, economic, or psychological. For consumers who have job responsibilities in our country's military, government, or intelligence services, exposure of this kind of information can have serious national security implications.

74. In contrast to the *CPNI Cases*, *TerraCom* addressed a situation of similarly serious threats to privacy—albeit in the context of a different part of section 222. *TerraCom* dealt with exposure of personal information—not CPNI—and the Commission proposed penalties based on language in section 222(a) that had never been examined or codified in a Commission rulemaking. Here, in contrast, the Commission has examined section 222(c) in multiple rulemaking and other proceedings and has promulgated rules necessary to interpret and enforce the statute. That said, the proposed penalty in *TerraCom* was significant in light of the scope of the apparent harm.

75. Apparent Violations of Section 222 of the Act and Section 64.2010 of the Commission's Rules. The violations in this case were continuing in nature, extending each day that the Company's location-based services operated in the apparent absence of reasonable measures to protect CPNI. We propose a base forfeiture of $40,000 for the first day of such a violation and a $2,500 forfeiture for the second day and each successive day that the violation continued. In other contexts involving consumer protections under the Act and the Commission's rules, the Commission has applied a base forfeiture of $40,000 for a single act.[190] We find that the base forfeiture we propose is appropriate (1) to provide a meaningful distinction between the violations in this case and those of other cases involving less egregious facts; and (2) to provide consistency with other consumer protection cases involving serious harms to consumers. We find this base forfeiture appropriately deters wrongful conduct and reflects the increased risk consumers face when their information is not secured in a timely manner.

76. We recognize that AT&T took one reasonable step towards improving its safeguards by terminating Securus and 3Cinteractive's [redacted]

Telecom Corporation, Order of Forfeiture, 26 FCC Rcd 7913 (EB-TCD 2011); *DigitGlobal Communications, Inc.*, Order of Forfeiture, 26 FCC Rcd 8400 (EB-TCD 2011).

[188] *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd. 13325 (2014) (*TerraCom*).

[189] *TerraCom*, 29 FCC Rcd at 13343, para. 52.

[190] *See, e.g., Advantage Telecommunications Corp.*, Forfeiture Order, 32 FCC Rcd 3723 (2017); *Preferred Long Distance, Inc.*, Forfeiture Order, 30 FCC Rcd 13711 (2015).

[redacted] days, respectively, after the *New York Times* report. But that step did not protect customer location information at all from the other [redacted] entities that had access to it. These included location-based service providers, the two Aggregators, and two intermediary aggregators—and constitute [redacted] separate continuing violations. We find that AT&T apparently did not take reasonable steps to safeguard that CPNI until it terminated the access of each of these [redacted] entities to AT&T customer location information. AT&T did so on the dates listed below, including [redacted],—a full [redacted] days after the *New York Times* report—for [redacted], and [redacted]—a full [redacted] days after the *New York Times* report—for the two Aggregators and [redacted] other entities. Even though no carrier can be expected to fully investigate and take remedial actions on the same day it learns that its safeguards are inadequate, AT&T's failure to take reasonable steps to safeguard that information in the 30 days after discovering the breach constitutes a continuing violation of our rules. We therefore calculate each continuing violation from June 9, 2018, or 30 days after publication of the *New York Times* report, and apply a base forfeiture of $40,000 for the first day of such violation and a $2,500 forfeiture for the second day and each successive day the violation continued. These calculations are set forth in Table 1 below:

	Table 1: Calculation of Base Forfeiture Penalty			
	Number of Entities	Date AT&T Terminated Access	Days of Continuing Violation (from June 9, 2018)	Base
	[redacted]	[redacted]	[redacted]	$750,000
	[redacted]	[redacted]	[redacted]	$440,000
	[redacted]	[redacted]	[redacted]	$277,500
	[redacted]	[redacted]	[redacted]	$660,000
	[redacted]	[redacted]	[redacted]	$6,417,500
	[redacted]	[redacted]	[redacted]	$1,950,000
	[redacted]	[redacted]	[redacted]	$517,500
	[redacted]	[redacted]	[redacted]	$560,000
	[redacted]	[redacted]	[redacted]	$570,000
	[redacted]	[redacted]	[redacted]	$6,100,000
	[redacted]	[redacted]	[redacted]	$10,667,500
	[redacted]	[redacted]	[redacted]	$645,000
	[redacted]	[redacted]	[redacted]	$1,365,000
	[redacted]	[redacted]	[redacted]	$4,882,500
	[redacted]	[redacted]	[redacted]	$10,010,000
Total:	[redacted]			**$45,812,500**

Accordingly, we find that AT&T is apparently liable for a base forfeiture in the amount of $45,812,500 for its apparent violations of section 222 of the Act and section 64.2010 of our rules.

77. Apparent Violations of Section 222(c)(1) of the Act and Section 64.2007(b) of the Commission's Rules. Although we find that AT&T apparently violated the Act and our rules for its unauthorized disclosures of CPNI to Hutcheson, the one-year statute of limitations bars any forfeiture for

those violations.[191] We thus instead exercise our discretion to admonish AT&T for its unauthorized disclosures of CPNI to Hutcheson.[192]

78. Unlike other federal agencies,[193] the Commission's authority to propose a monetary forfeiture for violations by a common carrier such as AT&T is statutorily limited to the one-year period before issuance of the associated notice of apparent liability.[194] In this case, Hutcheson's unauthorized access to customer location information ceased by April 2017, when he was arrested by the FBI and state law enforcement authorities. Thus, the statute of limitations on these violations ran out in April 2018, one month before the unauthorized disclosures even came to light in the May 2018 *New York Times* report. As the Act states and courts have affirmed, the countdown clock on the Commission's statutory deadline for action begins when a violation *occurs*, rather than when it is discovered.[195] Accordingly, we are prohibited by statute from imposing a forfeiture penalty when the underlying violation occurred years ago, as was the case with AT&T's unauthorized disclosures to Hutcheson.

79. Upward Adjustment. Given the totality of the circumstances, and consistent with the Commission's *Forfeiture Policy Statement*,[196] we also conclude that a significant upward adjustment is warranted. The responsibility for safeguarding the location information of its customers rested squarely on the Company, making it highly culpable. The violations at issued occurred over an extended period of time and placed consumers at significant risk of harm. Moreover, the harm included the potential for malicious persons to identify the exact locations of AT&T subscribers who belong to law enforcement, military, government, or other highly sensitive positions—thereby threatening national security and public safety. In this case, the risk was not merely theoretical; Hutcheson did in fact obtain the precise location of multiple Missouri State Highway Patrol officers on numerous occasions.

[191] *See* 47 U.S.C. § 503(b)(6)(B).

[192] *See, e.g., WDT World Discount Telecommunications Co., Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 31 FCC Rcd 12571 (EB 2016); *Life on the Way Communications, Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 28 FCC Rcd 1346 (EB-SED 2013); *Locus Telecommunications, Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 26 FCC Rcd 17073 (EB 2011).

[193] In contrast to the one-year limitation on Commission investigation and action, many other federal agencies—including but not limited to the Federal Trade Commission—enjoy a five-year statute of limitations period within which to investigate and pursue civil penalties. *See* 28 U.S.C. § 2462 (providing, in part, "Except as otherwise provided by Act of Congress, an action, suit or proceeding for the enforcement of any civil fine, penalty, or forfeiture, pecuniary or otherwise, shall not be entertained unless commenced within five years from the date when the claim first accrued. . .").

[194] *See* 47 U.S.C. § 503(b)(6)(B). Notwithstanding the one-year statute of limitations, the Enforcement Bureau can and frequently does enter into agreements with the targets of investigations in order to pause the statute of limitations while an investigation is underway. These agreements are commonly referred to as "tolling agreements." In this investigation, the Enforcement Bureau entered into a tolling agreement with AT&T so that we may assess penalties for conduct going as far back as May 3, 2018.

[195] *See* 47 U.S.C. § 503(b)(6)(B); *see also Gabelli v. SEC*, 568 U.S. 442, 450 (2013) (holding that "discovery rule" for delaying commencement of statute of limitations is inapplicable to civil enforcement action by Securities and Exchange Commission, and observing that "[t]here are good reasons why the fraud discovery rule has not been extended to Government enforcement actions for civil penalties").

[196] *Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, Report and Order, 12 FCC Rcd 17087 (1997) (*Forfeiture Policy Statement*), *recons. denied*, Memorandum Opinion and Order, 15 FCC Rcd 303 (1999).

80. We find that an upward adjustment of 25% above the $45,812,500 base forfeiture, or the amount of $11,453,125, is justified in these circumstances, will protect the interests of consumers, and deter entities from violating the Commission's rules in the future.[197]

81. Therefore, after applying the *Forfeiture Policy Statement*, section 1.80 of the Commission's rules, and the statutory factors, we propose a total forfeiture of $57,265,625 for AT&T's apparent willful and repeated violations of section 222 of the Act[198] as well as section 64.2010 of the Commission's rules.[199]

IV. REQUESTS FOR CONFIDENTIALITY

82. AT&T has requested that some of the materials it submitted to the Commission in this matter be withheld from public inspection, pursuant to section 0.459 of our rules.[200] With respect to the particular information set forth in this Notice of Apparent Liability, we conclude that there is a significant public interest in revealing this information to the public by publicly releasing an unredacted version of this Notice. We further conclude that this interest outweighs whatever competitive harms to AT&T and others might result from the disclosure of this information, and therefore partially deny AT&T's request.

83. The Commission may publicly reveal even otherwise confidential business information if, after balancing the public and private interests at stake, it finds that it would be in the public interest to do so.[201] At the outset, we find a strong public interest in the public knowing AT&T's practices with respect to the location-based services and customer location information at issue, including to whom the carrier provided access to such information; the steps the carrier took or failed to take to safeguard this information; and the extent to which any such information was improperly disclosed or otherwise put at risk. This conclusion is further supported by both the sensitivity of the location data involved, the large number of customers potentially affected, and the fact that the extent of any additional improper disclosure remains unknown. The public therefore has a strong interest in understanding the facts supporting this Notice, so that they can understand the risks, if any, that AT&T's practices posed to their location data. We further find that the benefits of revealing the information contained in this Notice greatly outweigh whatever competitive harms to AT&T might result from its competitors or business partners knowing its policies and the actions it took regarding the disclosure of its customers' location

[197] *See, e.g.*, *Forfeiture Policy Statement*, 12 FCC Rcd at 17098, para. 20 (recognizing the relevance of creating the appropriate deterrent effect in choosing a forfeiture); *see also* 47 CFR § 1.80(b)(8), Note to paragraph (b)(8) (identifying upward adjustment criteria for section 503 forfeitures).

[198] 47 U.S.C. § 222.

[199] 47 CFR § 64.2010.

[200] AT&T has requested confidential treatment of its responses to the Letters of Inquiry sent to it by the Bureau, except with regard to (1) how location-based services work; (2) the names of the Aggregators and intermediary providers used by AT&T in the transmission of location-based services data and a categorical descriptions of location-based service providers with which AT&T shared location data via those entities (as listed below); (3) contract information (but not including financial information); (4) legal arguments as to whether the information allegedly provided without authorization is CPNI; (5) the fact that AT&T performed audits, including privileged audits, and descriptions of the audit findings as provided in its LOI responses; and (6) information concerning the second layer of consent AT&T developed in 2018. Further Response.

[201] *See Establishing the Digital Opportunity Data Collection, Modernizing the FCC Form 477 Data Program*, Report and Order and Second Further Notice of Proposed Rulemaking, 34 FCC Rcd 7505, 7522-23, para. 40 & n.100 (2019) (noting long-established authority to release even otherwise confidential information after a balancing of the public and private interests at stake); *American Broadband & Telecommunications Company and Jeffrey S. Ansted*, Notice of Apparent Liability for Forfeiture and Order, 33 FCC Rcd 10308, 10366, para. 184 (2018); *Chrysler v. Brown*, 441 U.S. 281, 292-94 (1979); *Schreiber v. FCC*, 381 U.S. 279, 291-92 (1965); 47 U.S.C. § 154(j) ("The Commission may conduct its proceedings in such manner as will best conduce to the proper dispatch of business and the ends of justice."); 47 CFR § 0.461(f)(4).

data. We likewise find that the public interest greatly outweighs any private interest AT&T may have in keeping confidential the entities with whom it shared customer location data. This is all the more true given that AT&T argues that it required these entities to obtain affirmative consent from AT&T's customers for the sharing of their location data.[202] Thus, the identity of these entities should already be widely known and was required by AT&T to be divulged to its affected customers. And to the extent that AT&T's customers did not provide their consent, we find that it is contrary to the public interest to allow the location-based service providers, the intermediaries, or AT&T to keep these identities hidden from, among others, the very customers whose private location information was shared for the commercial benefit of these entities.

84. Because AT&T's requests are being ruled on by the Commission, and not the Bureau, in the first instance, we will not release the unredacted version of this Notice for 10 business days to allow AT&T or a relevant third party to file a petition for reconsideration;[203] if any avail themselves of this opportunity, we will continue to withhold the information from public inspection until we have ruled on the petition(s).[204] If, after 10 business days, AT&T or a relevant third party has not filed a petition for reconsideration or sought a judicial stay with regard to this partial denial of AT&T's confidentiality request, the material will be made publicly available.[205]

V. ORDERING CLAUSES

85. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act[206] and section 1.80 of the Commission's rules,[207] AT&T Inc. is hereby **NOTIFIED** of this **APPARENT LIABILITY FOR A FORFEITURE** in the amount of fifty-seven million, two hundred and sixty-five thousand, six hundred and twenty-five dollars ($57,265,625) for willful and repeated violations of section 222 of the Act[208] and section 64.2010 of the Commission's rules.[209]

86. **IT IS FURTHER ORDERED** that AT&T Inc. is hereby **ADMONISHED** for its apparent violations of section 222(c) of the Act[210] and section 64.2007 of the Commission's rules.[211]

87. **IT IS FURTHER ORDERED** that, pursuant to section 1.80 of the Commission's rules,[212] within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, AT&T Inc. **SHALL PAY** the full amount of the proposed forfeiture or **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture consistent with paragraphs 90-91below.

88. AT&T Inc. shall send electronic notification of payment to Michael Epshteyn and Rosemary Cabral, Enforcement Bureau, Federal Communications Commission, at

---

[202] LOI Response, Response to Question 1.

[203] The Aggregators, intermediaries, and location-based service providers, to the extent that they are third-party owners of some of the information for which AT&T has requested confidential treatment, may file a petition for reconsideration with respect to their own information.

[204] *Cf.* 47 CFR § 0.459(g).

[205] *See* 47 CFR § 0.455(g).

[206] 47 U.S.C. § 503(b).

[207] 47 CFR § 1.80.

[208] 47 U.S.C. § 222.

[209] 47 CFR § 64.2010.

[210] 47 U.S.C. § 222(c).

[211] 47 CFR § 64.2007.

[212] 47 CFR § 1.80.

michael.epshteyn@fcc.gov and rosemary.cabral@fcc.gov on the date said payment is made. Payment of the forfeiture must be made by credit card, ACH (Automated Clearing House) debit from a bank account using the Commission's Fee Filer (the Commission's online payment system),[213] or by wire transfer. The Commission no longer accepts forfeiture payments by check or money order. Below are instructions that payors should follow based on the form of payment selected:[214]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. A completed Form 159 must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 may result in payment not being recognized as having been received. When completing FCC Form 159, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[215] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using the Commission's Fee Filer website at https://apps.fcc.gov/FeeFiler/login.cfm. To pay by credit card, log-in using the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Pay bills" on the Fee Filer Menu, and select the bill number associated with the NAL Account – the bill number is the NAL Account number with the first two digits excluded – and then choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using the Commission's Fee Filer website at https://apps.fcc.gov/FeeFiler/login.cfm. To pay by ACH, log in using the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Pay bills" on the Fee Filer Menu and then select the bill number associated to the NAL Account – the bill number is the NAL Account number with the first two digits excluded – and choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

89. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer—Financial Operations, Federal Communications Commission, 445 12th Street, SW, Room 1-A625, Washington, DC 20554.[216] Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

90. The written statement seeking reduction or cancellation of the proposed forfeiture, if any, must include a detailed factual statement supported by appropriate documentation and affidavits pursuant to sections 1.16 and 1.80(f)(3) of the Commission's rules.[217] The written statement must be mailed to the Office of the Secretary, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554, ATTN: Enforcement Bureau – Telecommunications Consumers Division, and must include the

[213] Payments made using the Commission's Fee Filer system do not require the submission of an FCC Form 159.

[214] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6), or by e-mail at ARINQUIRIES@fcc.gov.

[215] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

[216] *See* 47 CFR § 1.1914.

[217] 47 CFR §§ 1.16, 1.80(f)(3).

NAL/Account Number referenced in the caption. The statement must also be e-mailed to Michael Epshteyn at michael.epshteyn@fcc.gov and Rosemary Cabral at rosemary.cabral@fcc.gov.

91. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits: (1) federal tax returns for the most recent three-year period; (2) financial statements prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status. Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation.

92. **IT IS FURTHER ORDERED**, pursuant to section 0.459(g) of the Commission's rules,[218] that the Requests for Confidential Treatment filed by AT&T Services, Inc. in this proceeding **ARE DENIED IN PART**, to the extent specified herein.

93. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture shall be sent by first class mail and certified mail, return receipt requested, to David R. McAtee II, Senior Executive Vice President and General Counsel, AT&T Inc., c/o Jeanine Poltronieri, Asst. Vice President – Federal Regulatory, AT&T Services, Inc., 1120 20th St. NW, Washington, DC 20036.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[218] 47 CFR § 0.459(g).

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *AT&T Inc.*, File No.: EB-TCD-18-00027704.

For most Americans, their wireless phone goes wherever they go. And every phone must constantly share its—and its owner's—location with a wireless carrier in order to enable the carrier to know where to route calls. Information about a customer's location is highly personal and sensitive. As the U.S. Supreme Court has observed, this type of information "provides an intimate window into a person's life."[1] This makes it critical that all telecommunications carriers protect the confidentiality of their customers' location information. Congress has made this requirement clear in the Communications Act. And the Commission has made this requirement clear in its implementing rules.

Today, we also make clear that we will not hesitate to vigorously enforce these statutory provisions and regulations. After a thorough investigation, we find that all of our nation's major wireless carriers apparently failed to comply with these vitally important requirements. In brief, long after these companies were on notice that their customers' location data had been breached, they continued to sell access to that data for many months without taking reasonable measures to protect it from unauthorized disclosure. This FCC will not tolerate any telecommunications carrier putting American consumers' privacy at risk. We therefore propose fines against these four carriers totaling more than $200 million.

For their diligent work on this item, I'd like to thank Rosemary Cabral, Rebecca Carino, Michael Epshteyn, Rosemary Harold, Jermaine Haynes, Erica McMahon, Ann Morgan, Shannon Lipp, Tanishia Proctor, Nakasha Ramsey, Phil Rosario, Mika Savir, Daniel Stepanicich, David Strickland, Raphael Sznajder, Kristi Thompson, David Valdez, and Shana Yates of the Enforcement Bureau; Justin Faulb, Lisa Hone, Melissa Kirkel, Kris Monteith, and Zach Ross of the Wireline Competition Bureau; Martin Doczkat, Aspasia Paroutsas, and Robert Pavlak of the Office of Engineering and Technology; Michael Carlson, Douglas Klein, Marcus Maher, Linda Oliver, Joel Rabinovitz, and Bill Richardson of the Office of General Counsel; and Virginia Metallo of the Office of Economics and Analytics. Our Enforcement Bureau staff reviewed more than 50,000 pages of documents during the course of this complex investigation, and their painstaking efforts to uncover the details of what happened enabled us to take this strong enforcement action. While this nitty-gritty investigative work is not glamorous and can take longer than some in the peanut gallery might like, it is indispensable to building a case that will stand up in a court of law rather than only garnering some headlines.

[1] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

Re: *AT&T Inc.*, File No.: EB-TCD-18-00027704.

The pocket-sized technology that nearly everyone carries today is capable of amazing functionality, including the ability to pinpoint exact locations, which has recognizable benefits. Yet, this technology can be used for nefarious purposes as well. The privacy breaches that were reported in the press related to these notices of apparent liability (NALs) are serious and warrant further investigation to determine exactly what happened, whether the parties violated current law, and if so, how such events can be prevented in the future. There is enough evidence contained within these four documents to warrant NALs, and as such I will vote to approve. However, it should be noted that I do so with serious reservations. I would have expected more well-reasoned items than what is presented here, especially given the yearlong plus investigation. Significant revisions and a more in-depth discussion of what occurred will be necessary before I will consider supporting any forfeiture.

Specifically, I am concerned that we do not have all the relevant facts before us, and that we either haven't heard or sufficiently considered counter arguments from AT&T, Sprint, T-Mobile, and Verizon. Not only was additional information filed just days ago, but when the parties discussed these cases with my office, it was readily apparent that the record was incomplete. It is also unclear as to whether the Commission has a firm grasp of the services that were actually being offered to consumers, when these services were offered and/or terminated, and whether many of the location-based offerings included to justify the substantial proposed fines were involved in any actual violations. It also would have been preferable to engage the parties in conversation prior to issuing the NALs, to establish a more solid foundation from which to consider appropriate penalties. The parties appear to have had barely any chance to discuss the potential violations and the legal basis behind the NALs with the Enforcement Bureau's investigators, which undermined their opportunity to explain their underlying practices and ultimately shed more light on the whole situation.

Equally important, I am not convinced that the location information in question was obtained as the result of a "call" or as part of a "telecommunications service," raising questions about the application of our section 222 authority. The item seems to rely on the argument that these companies obtain location information solely to connect the device to the network for the purpose of sending and receiving voice calls. That seems to be a major stretch, because the same connection is needed in order to send data, which is not a telecommunications service under the Commission's sound decision to declare it a Title I service. Beyond the important jurisdictional concern relating to the breadth of our legal authority, more facts are needed to contemplate all of the various applications at issue and how the location information is obtained.

In the end, I am hopeful that these issues can be sorted out, especially when AT&T, Sprint, T-Mobile, and Verizon reply to these NALs. I look forward to developing a fulsome record and discussing these alleged violations with the parties. I want to be clear that I remain open minded on this entire matter.

STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL
DISSENTING

Re: *AT&T Inc.*, File No.: EB-TCD-18-00027704.

This investigation is a day late and a dollar short. Our real-time location information is some of the most sensitive data there is about us, and it deserves the highest level of privacy protection. It did not get that here—not from our nationwide wireless carriers and not from the Federal Communications Commission. For this reason, I dissent.

Everywhere we go our smartphones follow. They power the connections that we count on for so much of modern life. But because they are always in our palms and pockets, they are collecting gobs of data about everything we are doing—and where we are doing it.

That means our phones know our location at any given moment. This geolocation data is especially sensitive. It's a record of where we've been and by extension, who we are. If it winds up in the wrong hands, it could provide criminals and stalkers with the ability to locate any one of us with pinpoint accuracy. It could be sold to domestic abusers or anyone else who wishes to do us harm. Its collection and distribution or sale without our permission or without reasonable safeguards in place is a violation of our most basic privacy norms. It's also a violation of the law.

But what we've learned is that it happened anyway. In May 2018, The New York Times reported that our wireless carriers were selling our real-time location information to data aggregators. Then in January 2019 Motherboard revealed that bounty hunters and other shady businesses had access to this highly sensitive data. Further reporting by Vice pieced together just how this sensitive data wound up in the hands of hundreds of bounty hunters who were willing to sell it to anyone for just a few hundred dollars. It turns out wireless carriers sold access to individual real-time location information to data aggregators, who then sold it to a skip-tracing firm, who then sold it to a bail-bond company, who then sold it to individual bounty hunters.

If that sounds like a tortured chain of data possession, it is. And if you don't remember giving this kind of permission or signing up for the sale of your geolocation data on a black market, you're not alone. Comb through your wireless contract, it's a good bet there is nothing in there that discloses your carrier could monetize your real-time location in this way.

It should have been simple for the FCC to take action to stop this practice under Section 222 of the Communications Act. But that didn't happen. Instead, for months this agency said nothing except that it was investigating. It did not provide the public with any details, despite the ongoing risk to the security of every one of us with a smartphone. As a result, the sale of our most sensitive location information continued for far too long under the watch of this agency.

All told, taking nearly two years to address these troubling revelations is a stain on this agency's public safety record. It's a testament to how little it makes privacy a priority.

That's why starting last year I took on this issue on my own. I took to television and spoke on cable and broadcast news about how a black market was developing where anyone could buy information about where we are and what we are doing based on location data from our wireless devices. I wrote every nationwide wireless carrier and asked them to state whether they had ended their arrangements to sell location data and what steps they were taking to secure any data that had already been shared. I made these letters public. I also made public the responses. In the course of doing so, I am pleased to report

that I was able to secure the first public statements from inside this agency about what carriers were doing with our location information.

I am also pleased that at my request the FCC is taking the necessary steps to remove redactions in the text of this long-awaited enforcement action that would have covered up exactly what happened with our location data. We should care more about protecting the privacy of consumers than the privacy of companies' business practices—especially when they violate the law.

However, in the end I find this enforcement action inadequate. There are more than 270 million smartphones in service in the United States and this practice put everyone using them at a safety risk. The FCC heavily discounts the fines the carriers could owe under the law and disregards the scope of the problem.

Here's why. At the outset, the FCC states that this impermissible practice should be the subject of a fine for every day that it was ongoing. But right at the outset the agency gives each carrier a thirty-day pass from this calculation. This thirty day "get-out-of-jail-free" card is plucked from thin air. You'll find it in no FCC enforcement precedent. And if you compare it to every data security law in the country, this stands as an outlier. In fact, state privacy laws generally require companies to act on discovered breaches on a much faster timetable—in some cases, less than a week. Real-time location data is some of the most sensitive information available about all of us and it deserves the highest level of privacy protection. Permitting companies to turn a blind eye for thirty days after discovering this data is at risk falls short of any reasonable standard.

Next, the FCC engages in some seriously bureaucratic math to discount the violations of our privacy laws. The agency proposes a $40,000 fine for the violation of our rules—but only on the first day. For every day after that, it imposes only a $2,500 fine for the same violation. But it offers no acceptable justification for reducing the fine in this way. Plus, given the facts here—the sheer volume of those who could have had their privacy violated—I don't think this discount is warranted.

In sum, it took too long to get here and we impose fines that are too small relative to the law and the population put at risk. But this effort is far from over. Because when the FCC releases a Notice of Apparent Liability, it is just early days. The fines are not final until after the carriers that are the subject of this action get a chance to respond. That means there is still work to do—and this agency cannot afford to wait another year to do it. If past practice is any guide, we all have reason to be concerned.

STATEMENT OF COMMISSIONER GEOFFREY STARKS
APPROVING IN PART AND DISSENTING IN PART

Re: *AT&T Inc.*, File No.: EB-TCD-18-00027704.

Taking control of our personal information is one of the defining civil rights issues of our generation. Practically every day, we learn about new data harms: algorithmic and facial recognition bias; companies failing to protect our most sensitive information from hackers and thieves; and "pay to track" schemes that sell location information to third parties. These practices put all Americans at risk, and they are especially insidious because they replicate and deepen existing inequalities in our society.

In recent months, consumers have become increasingly aware of how much private information trails behind them as they go about their days. In December 2019, the New York Times opinion series *One Nation, Tracked* brought renewed focus to the issue of smartphone tracking.[1] Their stories illustrated, sometimes in frightening detail, how much can be learned about a person from the location of their smartphone. Using supposedly anonymous location data, the Times was able to follow the movements of identifiable Americans, from a singer who performed at President Trump's inauguration to President Trump himself.

The findings by journalists at the New York Times, Motherboard, and many other outlets unsettle us for good reason. Your location at any time goes to the heart of personhood—where you live, who you see, where you go, and where you worship. And tracking over time can build a picture of a life in intimate detail. Disclosure of those coordinates and patterns isn't just creepy; it can leave us vulnerable to safety threats and intrusions never before possible on such a comprehensive scale. And because people of color rely more heavily on smartphones for internet access than other Americans, they bear these harms disproportionately.

For those "freaked out" by their reporting, the Times offered a number of steps consumers can take to limit access to the location data, including blocking location sharing and disabling mobile advertising IDs. Those can be good steps, but they are no defense against your wireless carrier. Your carrier needs to know where you are to complete your calls. Because it is simply impossible to use a mobile phone—an important part of participation in our modern economy—without giving location data to one of the carriers, our rules about how that they can use customer location data must be strict and strictly enforced.

For that reason, I am pleased that the Notices of Apparent Liability we vote on today confirm that misuse of customer location data by AT&T, Verizon, Sprint, and T-Mobile violate the Commission's rules. These serious violations damaged Americans' faith in our telephone system, and I am pleased that we have reached bipartisan agreement that enforcement is appropriate here. I cannot fully approve these Notices, however, because in conducting these investigations and determining the appropriate penalty, we lost track of the most important part of our case—the very consumers we are charged with protecting. Because I strongly believe we should have determined the number of customers impacted by the abuses and based our forfeiture calculations on that data—calculations that would have been possible if we had investigated more aggressively—I must dissent in all remaining parts of the item.

[1] Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," New York Times (Dec. 19, 2019).

Enforcement Authority

Congress has clearly directed carriers to protect our location information, and these Notices confirm that this protection exists even when no call is in progress. Going forward, there should be no dispute about this basic legal conclusion.

This is a responsibility that can't be delegated away. Carriers are responsible for the actions of their agents and sub-contractors. This is a well-established principle, and it recognizes the special nature of the customer-carrier relationship. We trust our wireless carrier to provide high-quality service, and we don't expect that our carrier is going to monetize that relationship.

None of these carriers should be surprised that we take the protection of customer data so seriously. In 2007, the Commission addressed the problem of "pretexting," where data brokers would impersonate customers to fool carriers into disclosing confidential customer information. We revamped our rules and, for the first time, required that carriers obtain "opt-in" consent to the disclosure of customer information, rather than presenting it as an "opt-out."

Regrettably, these investigations show that carriers did not heed that warning. Despite the clear message from the FCC, these carriers did not treat the protection of their customers' data as a key responsibility. Instead, they delegated responsibility for protecting this sensitive information to aggregators and third-party location service providers. They subjected these arrangements to varying degrees of oversight, but all were ineffective and failed to prevent the problem. Significant penalties are more than justified.[2]

Delays

Today's action has been too long delayed. As the Notices point out, the Commission has been investigating these matters for nearly two years. And the investigations show that, even after the problems with their location data sharing programs became readily apparent, the carriers took months to shut them down. Indeed, nearly one year ago, I published an op-ed in the NY Times about the slow pace of this investigation, and the need for the FCC to "act swiftly and decisively to stop illegal and dangerous pay-to-track practices."[3] I had no idea it would be another 11 months before we finally acted.

From the beginning, it has been difficult to get the facts straight. The carriers repeatedly told the public that they were stopping their location sharing program while hiding behind evasive language and contractual terms. For example, on June 15, 2018, Verizon told Senator Ron Wyden, "[w]e are initiating a process to terminate our existing agreements for the location aggregator program."[4] But Verizon didn't terminate its aggregator agreements until November 2018, and didn't end all of its location data sharing

[2] In fact, just a few years ago, the Enforcement Bureau entered into multi-million-dollar consent decrees with these same carriers involving a similar problem— the unauthorized billing of customers by third-party vendors where the carriers sought to delegate their consumer protection responsibility via contract. As in the cases at issue here, the carriers claimed that they weren't responsible for unlawful billing because their contracts had requirements placing any responsibility on the downstream companies. The carriers we find liable today did a fundamental disservice to their customers when they simply "passed the buck" to these location data aggregators and service providers. Failure to supervise their agents is no defense. *See Cellco Partnership d/b/a Verizon Wireless,* Order and Consent Decree, 30 FCC Rcd 4590 (Enf. Bur. 2015) (requiring $90 million in payments and restitution to consumers to settle allegations that Verizon charged consumers for third-party products and services that the consumers did not authorize; *Sprint Corp.*, Order and Consent Decree, 30 FCC Rcd 4575 (Enf. Bur. 2015) ($68 million); *AT&T Mobility LLC,* Order and Consent Decree, 29 FCC Rcd 11803 (Enf. Bur. 2014) (($105 million); *T-Mobile USA, Inc.*, Order and Consent Decree, 29 FCC Rcd 15111 (Enf. Bur. 2014) ($90 million).

[3] Geoffrey Starks, "Why It's So Easy for a Bounty Hunter to Find You," New York Times (April 19, 2019).

[4] Letter from Karen Zacharia, Chief Privacy Officer, Verizon, to Senator Ron Wyden, dated June 15, 2018.

programs until April 2019. With respect to the other carriers, on June 19, 2018, the Washington Post reported:

> AT&T then said in a statement Tuesday that it also will be ending its relationship with location data aggregators "as soon as practical" while ensuring that location-based services that depend on data sharing, such as emergency roadside assistance, can continue to function. Sprint said in a statement that it cut ties with LocationSmart on May 25, and has begun cutting ties with the data brokers who received its customers' location data.
>
> T-Mobile chief executive John Legere tweeted: "I've personally evaluated this issue & have pledged that @tmobile will not sell customer location data to shady middlemen."[5]

Despite these statements, each of these carriers continued to sell their customers' location data for *months* afterwards. Americans deserve better.

For its part, the FCC also failed to act with sufficient urgency. As a former enforcement official, I recognize the challenges of reviewing the tens of thousands of pages of documents produced in these investigations, but we have conducted similarly extensive investigations much faster. Indeed, we took less time to resolve the highly complex merger between T-Mobile and Sprint, which involved mountains of pages of materials. Given the seriousness of the violations here, the Commission should have invested the resources necessary to get a draft to the Commission faster. By allowing this investigation to drag on when we knew that important public safety and public policy issues were at stake, we failed to meet our responsibilities to the American people.

Consumer Harms

I am concerned that the penalties proposed today are not properly proportioned to the consumer harms suffered because we did not conduct an adequate investigation of those harms. The Notices make clear that, after all these months of investigation, the Commission still has no idea how many consumers' data was mishandled by each of the carriers. I recognize that uncovering this data would have required gathering information from the third parties on which the carriers' relied. But we should have done that via subpoenas if necessary. We had the power—and, given the length of this investigation, the time—to compel disclosures that would help us understand the true scope of the harm done to consumers. Instead, the Notices calculate the forfeiture based on the number of contracts between the carriers and location aggregators, as well as the number of contracts between those aggregators and third-party location-based service providers. That is a poor and unnecessary proxy for the privacy harm caused by each carrier, each of which has tens of millions of customers that likely had their personal data abused. Under the approach adopted today, a carrier with millions more customers, but fewer operative contracts, would get an unfairly and disproportionately lessened penalty. That is inconsistent with our approach in other consumer protection matters and cannot stand.[6] More importantly, basing our forfeiture on a carrier's

[5] Brian Fung, "Verizon, AT&T, T-Mobile and Sprint Suspended Selling of Customer Location Data After Prison Officials Were Caught Misusing It," Washington Post (June 19, 2018).

[6] *See, e.g., Scott Rhodes A.K.A. Scott David Rhodes, Scott D. Rhodes, Scott Platek, Scott P. Platek*, Notice of Apparent Liability for Forfeiture, FCC 20-9, 2020 WL 553616 (rel. Jan. 31, 2020) (spoofed robocall violations; calculates the proposed forfeiture of $12,910,000 by assessing a base forfeiture of $1,000 per each of 6,455 verified unlawful spoofed robocalls with a 100% upward adjustment); *Kenneth Moser dba Marketing Support Systems*, Notice of Apparent Liability for Forfeiture, FCC 19-135, 2019 WL 6837865 (rel. Dec. 13, 2019) (spoofed robocall violations; calculates the proposed forfeiture of $9,997,750 by assessing a base forfeiture of $1,000 per each of 5,713 analyzed/verified calls with a 75% upward adjustment); *Long Distance Consolidated Billing Company*, Notice of Apparent Liability for Forfeiture, 30 FCC Rcd 8664 (2015) (slamming and cramming violations; calculates $2.3 million forfeiture by assessing a $40,000 forfeiture for each unlawful bill plus an upward adjustment for misrepresentation) (subsequent history omitted); *Neon Phone Service*, Notice of Apparent Liability for Forfeiture, 32 FCC Rcd 7964 (2017) (slamming and cramming violations; proposing a $3.9 million forfeiture by assessing a base forfeiture of $40,000 for each unlawful bill plus an upward adjustment for egregiousness). *See also TerraCom*,

number of aggregator contracts cannot be squared with our core mission today – to vindicate harmed consumers first and foremost.

Make no mistake – there are real victims who've had their privacy and security placed in harm's way. Each of them has a story. As discussed in the Notices, in May 2018, the *New York Times* reported that then-Missouri Sheriff Cory Hutcheson had used Securus technologies, a vendor that all of these wireless carriers allowed to access their customer location data, to conduct thousands of unauthorized location requests, accessing the locations of multiple individuals, including his predecessor as Sheriff, a Missouri Circuit Judge, and at least five highway patrol officers.[7] But I've personally spoken at length with one of those officers, retired Missouri State Highway Patrol Master Sergeant William "Bud" Cooper.

MSgt. Cooper told me that, while leading a homicide unit with the State Highway Patrol, he would investigate cases in the Missouri county where Cory Hutcheson was Sheriff. As they worked together on investigations, M.Sgt. Cooper noticed Hutcheson following up on leads and locating witnesses and suspects very quickly. M.Sgt. Cooper initially thought Hutcheson just had a particularly effective network of informants, but then grew suspicious and asked Hutcheson about his methods. Hutcheson eventually told him that he was using a Securus program to "ping" phone numbers from the investigations to uncover people's locations.

M.Sgt. Cooper suspected "something dirty" was going on. M.Sgt. Cooper began to wonder, based on Hutcheson's behavior towards him and his state trooper colleagues, if Hutcheson was targeting their phones too.

When M.Sgt. Cooper's worst fears were confirmed—that he had been targeted, along with his colleagues and a narcotics investigator—he was "shocked and angry." "I felt violated." This was personal information, akin to "going into someone's home." M.Sgt. Cooper found it "appalling" when it turned out that Hutcheson was obtaining this information based solely on woefully insufficient supporting documentation, including parts of an instruction manual, his vehicle maintenance records, and even an insurance policy. Hutcheson had personally "pinged" phones without authorization "over 2,000 times, and nobody checked."

M.Sgt. Cooper related that the revelations of Hutcheson's spying have threatened the safety of officers in the community and their informants. He reported that it has become harder to convince witnesses to trust police and talk to them, particularly in communities where witnesses fear retaliation. He has devoted his career to upholding the honor and integrity of law enforcement, but with the Hutcheson scandal "we all took a black eye."

M.Sgt. Cooper's story is but one single account of the harm done by the carriers; but we know there are many—perhaps millions—of additional victims, each with their own harms. Unfortunately, based on the investigation the FCC conducted, we don't even know how many there were, and the penalties we propose today do not reflect that impact.

This ignorance not only highlights a problem with today's decisions but a gap in our policymaking. The Commission needs to consider policy changes to protect the rights of consumers. Specifically, we should initiate a rulemaking to require carriers to inform consumers when there has been a breach of their confidential data, so that individual can take steps to protect themselves.

Even setting aside my concerns that our forfeitures are not pegged to the number of consumers harmed, I would still object to the amount of the proposed forfeiture to T-Mobile. It should be higher. As discussed in the Notice, T-Mobile had clear notice back in July 2017 that its contractual protections were failing to prevent location-based service providers from misusing customer location information. T-

Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) (in proposing a forfeiture for Section 222 violations, citing the number of personal data records exposed by a carrier as the key factor, ultimately resulting in a penalty figure of $8.5 million) (subsequent history omitted).

[7] *See, e.g., T-Mobile NAL* at para. 28; *AT&T NAL* at para. 21; *Verizon NAL* at para. 26; *Sprint NAL* at para. 21.

Mobile knew that one of these service providers was taking customer information and selling it to "bail bonding and similar companies"—aka, bounty hunters. Despite T-Mobile's knowledge of the problem, it took *two months* for the carrier to contact the aggregator company about this issue, and even then, T-Mobile only inquired of the aggregator and reminded it of its contractual obligations. It was the *aggregator* that terminated the service provider's access to T-Mobile customer information soon after hearing from T-Mobile. I believe that T-Mobile was on notice about the problems with its location data protections back in July 2017 and that the proposed forfeiture amount should reflect that fact – the punishment should fit the crime. Unfortunately, although their legal justification for doing so remains a mystery, a majority of my colleagues disagreed.

Transparency

Our slow response has also impacted our ability to discuss the facts of this case and the Commission's credibility for future investigations. Like other federal agencies, the Commission has a process that allows parties to protect the confidentiality of certain materials submitted to the agency. In their responses to the Bureau's investigation, however, the four carriers named in today's decisions bent that process so far that it is broken. Each of them adopted such an overbroad interpretation of our confidentiality protections that the Enforcement Bureau initially circulated heavily redacted draft decisions that would have made it impossible for the public to understand the key facts in each case.

Sadly, this is not a new phenomenon. The Enforcement Bureau has long struggled with parties asserting overbroad designations of confidentiality. Some parties, including some in these cases, have claimed confidential treatment for nearly the entirety of their responses to the Bureau's Letters of Inquiry, including legal arguments, publicly available facts, and even references to Commission's rules. Both as a former Enforcement Bureau official and as a Commissioner, I have seen such tactics hamstring our ability to vindicate the public interest and deter wrongdoing.

We should have rejected these confidentiality requests—some of which are frankly laughable—as soon as the Bureau reviewed the documents. Instead, many of those assertions were taken at face value, and the original drafts had heavy redactions. It is critical that Americans, particularly the hundreds of millions who use the services of these carriers, understand what happened here. If we let unreasonable and self-serving confidentiality assertions stand, those customers will never have the full picture.

Only after Commissioner Rosenworcel and I objected did the Bureau go back to the parties to challenge the confidentiality requests and negotiate the disclosure of more information. While I am glad that some of the parties reduced their requests, much of this information still remains confidential for now. Some even designated as confidential the number of agreements they had entered with aggregators and location-based service providers. That is frivolous.

The Commission does not have not to tolerate this. Section 0.459 of the Commission's rules establishes a process for resolving confidentiality requests. That process takes time, so we must begin resolving such requests immediately upon receipt. Here, despite the extraordinary length of our investigation, we let this problem fester for too long. Now, because we waited until the orders were before the Commission and then rushed to negotiate with the parties, there is insufficient time for the Section 0.459 process to play out. Even with the reduced redactions, Americans who read these Notices and the news coverage of them today will not have all the facts to which they are entitled. So while I am glad that we are ordering the parties to explain why we should not deny their requests completely, I worry that the carriers will have succeeded in hiding key facts until the spotlight has moved on. The FCC must do better.

* * *

Finally, while today's actions underscore and confirm the power of Section 222, they also highlight the need for additional actions. For example, our action today is limited to the major wireless carriers. But we know from this investigation that they are not the only wrongdoers. Securus, for one example, behaved outrageously. Though Securus holds multiple FCC authorizations, I recognize that

there may be legal limitations on the Commission's ability to take enforcement against the company for its misuse of customer location data. But that is no excuse for failing to conduct a comprehensive investigation—including issuing subpoenas to Securus—of the events in question here. That information would have enriched our investigation and could have been provided to other agencies for investigation and enforcement.

Going forward, Americans must be able to place trust in their wireless carriers. I understand that operating businesses at the enormous scale of these companies means relying on third parties for certain services. But these carriers know that the services they offer create risks for users: unauthorized location tracking, SIM hijacking, and billing scams to name just few. Carriers must take responsibility for those people they allow into their operations.

I thank the staff of the Enforcement Bureau for their hard work on these important investigations.

No. 23-55375

IN THE UNITED STATES COURT OF APPEAL

FOR THE NINTH CIRCUIT

MICHAEL TERPIN, *Plaintiff-Appellant*,

v.

AT&T MOBILITY LLC, *Defendant-Appellee*.

On Appeal from the United States District Court
for the Central District of California
Case No. 2:18-cv-06975-ODW-KS

APPELLANT'S ADDENDUM OF AUTHORITIES

VOLUME 3

Pierce O'Donnell
Timothy J. Toohey
Emily Avazian
GREENBERG GLUSKER FIELDS
CLAMAN & MACHTINGER LLP
2049 Century Park East,
Suite 2600
Los Angeles, California 90067
Telephone: (310) 553-3610
Email: POdonnell@ggfirm.com
TToohey@ggfirm.com
EAvazian@ggfirm.com

Attorneys for Plaintiff-Appellant
MICHAEL TERPIN

INDEX

ADDENDUM OF STATUTES, REGULATIONS AND UNPUBLISHED OPINIONS ("ADD")

STATUTES

REGULATORY MATERIALS: FEDERAL COMMMUNICATOINS COMMISSION (FCC)

Document	Description	ADD Nos.
	and Other Customer Information (June 27, 2013)	
29 FCC Rcd 13325, 29 F.C.C.R. 13325, 2014 WL 5439575	*In the Matter of Terracom, Inc. and Yourtel America, Inc. Apparent Liability for Forfeiture* (October 24, 2014)	ADD-180 – ADD-211
30 FCC Rcd. 2808, 30 F.C.C.R. 2808, 2015 WL 1577197	*In the Matter of AT&T Services, Inc.* (April 8, 2015)	ADD-212 – ADD-225
30 FCC Rcd. 7075, 30 F.C.C.R. 7075, 2015 WL 4159266	*In the Matter of Terracom, Inc., and Yourtel America, Inc.* (July 9, 2015)	ADD-226 – ADD-244
30 FCC Rcd. 12302, 30 F.C.C.R. 12302, 2015 WL 6779864	*In the Matter of Cox Communications, Inc.* (November 5, 2015)	ADD-245 – ADD-260
31 FCC Rcd. 13911, 31 F.C.C.R. 13911, 2016 WL 6538282	*In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (November 2, 2016), superseded by Rule *In the Matter of Restoring Internet Freedom*, January 4, 2018	ADD-266 – ADD-493
FCC 20-26, File No.: EB-TCD-18-00027704	*In the Matter of AT&T Inc.: Notice of Apparent Liability for Forfeiture and Admonishment* (February 28, 2020)	ADD-494 – ADD-535
36 FCC Rcd 14120, 36 F.C.C.R. 14120, 2021 WL 4735472	*In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud* (September 30, 2021)	ADD-541 – ADD-587

UNPUBLISHED DECISIONS

Document	ADD Nos.
Fraser v. Mint Mobile, LLC, No. C 22-00138 WHA, 2022 WL 1240864 (N.D. Cal. Apr. 27, 2022)	ADD-588 – ADD-595
Gatton v. T-Mobile USA, Inc., No. SACV 03-130 DOC, 2003 WL 21530185 (C.D. Cal. Apr. 18, 2003)	ADD-596 – ADD-606
Warren v. PNC Bank National Association, --- F. Supp. 3d --- (2023), No. 22-cv-07875-WHO, 2023 WL 3182952 (N.D. Cal. Apr. 30, 2023)	ADD-607 – ADD-621

36 FCC Rcd. 14120 (F.C.C.), 36 F.C.C.R. 14120, 2021 WL 4735472

Federal Communications Commission (F.C.C.)
Notice of Proposed Rulemaking

IN THE MATTER OF PROTECTING CONSUMERS FROM SIM SWAP AND PORT-OUT FRAUD

WC Docket No.
21
-
341
FCC 21-102
Released: September 30, 2021
Adopted: September 30, 2021
Comment Date: [30] days after publication in the Federal Register
Reply Comment Date: [60] days after publication in the Federal Register

****1 *14120** By the Commission: Acting Chairwoman Rosenworcel and Commissioner Starks issuing separate statements.

TABLE OF CONTENTS

I. INTRODUCTION

1. Cell phones are an essential part of everyday life for most Americans. We use them not just to make phone calls but to conduct much of our daily activities through their broadband connections and by using applications we have installed on our devices. We keep in touch with friends and family through voice calls, text messages, messaging applications, and social media. We manage our financial lives by accessing our bank and brokerage accounts and make payments using a wide array of financial services applications. We apply for jobs and for government benefits. We also use them to monitor and record health information. And, when we sign into certain websites or applications, or need to reset a password, we often receive a one-time passcode sent in a text message to our cell phone that we then input into the website or application to authenticate

our identity. As a result, if a bad actor can intercept our text messages, he or she can steal our identities and our money and take control of our digital lives.

2. Today, we focus on putting an end to two methods used by bad actors to take control of consumers' cell phone accounts and wreak havoc on people's financial and digital lives without ever gaining physical control of a consumer's phone. In the first type of scam, known as "subscriber identity module swapping" or "SIM swapping,"[1] a bad actor convinces a victim's wireless carrier[2] to transfer the ***14121** victim's service from the victim's cell phone to a cell phone in the bad actor's possession. This scam is known as "SIM swapping" because it involves an account being fraudulently transferred (or swapped) from a device associated with one SIM to a device associated with a different SIM. In the second method, known as "port-out fraud," the bad actor, posing as the victim, opens an account with a carrier other than the victim's current carrier. The bad actor then arranges for the victim's phone number to be transferred to (or "ported out") to the account with the new carrier controlled by the bad actor.

****2** 3. We have received numerous complaints from consumers who have suffered significant distress, inconvenience, and financial harm as a result of SIM swapping and port-out fraud. In addition, we note that recently disclosed data breaches have exposed customer information that could potentially make it easier to pull off these kinds of attacks.[3] Today, we take aim at these scams, with the goal of foreclosing the opportunistic ways in which bad actors take over consumers' cell phone accounts and proactively addressing the risk of follow-on attacks using stolen data, so as to mitigate the risk of additional consumer harm from recent data breaches. Section 222 of the Communications Act of 1934, as amended (the Act), and our Customer Proprietary Network Information (CPNI) rules, which govern the use, disclosure, and protection of sensitive customer information to which a telecommunications carrier has access, require carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to customers' private information. Our Local Number Portability (LNP) rules govern the porting of telephone numbers from one carrier to another. Yet, it appears that neither our CPNI rules nor our LNP rules are adequately protecting consumers against SIM swapping and port-out fraud. We, therefore, propose to amend our CPNI and LNP rules to require carriers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or carrier. We also propose to require providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts, and we seek comment on other ways to protect consumers from SIM swapping and port-out fraud.

II. BACKGROUND

4. *SIM Swapping and Port-Out Fraud*. Cell phone numbers are frequently used as a means of authenticating a user for various types of accounts, including accounts with telecommunications carriers, e-mail and social media providers, financial institutions, and retail websites. For example, a consumer logging in to an e-mail account from a new computer might be asked not only to provide her username and password, but also to input a one-time code sent via text message to her cell phone. Similarly, a consumer who has forgotten her password for a social media website may be prompted to enter a one-time code sent via text message to her cell phone before being allowed to reset her password. Because so many consumers have their cell phones with them at all times, text message-based two-factor authentication can be incredibly convenient. Text message-based authentication relies upon a customer's control of her device and her phone number, which is typically achieved through the SIM. Phone calls and text messages are routed to the device that has the SIM associated with the relevant phone number.

***14122** 5. When a cell phone owner loses, breaks, or upgrades her cell phone, she can sometimes take the SIM card out of her previous cell phone and insert it into her new phone. Often, however, she needs to contact her wireless carrier, explain that she is changing cell phones, and request that her wireless carrier reassign her account information to the SIM in her new device. When a bad actor successfully impersonates the customer of a wireless carrier and convinces the carrier to redirect the real customer's cell phone service to a new SIM in a device that the bad actor controls, the bad actor gains access to all of the information associated with the customer's account, including CPNI, and gains control over the customer's phone number and receives both text messages and phone calls intended for the victim.

****3** 6. When a wireless service customer decides to switch wireless carriers, the customer provides certain identifying information (telephone number, current account number, ZIP code, and any customer-assigned passcode) to the new wireless carrier to request that the customer's existing number be ported to the new service provider. The new service provider then sends a request with this information through the numbering administrator to the current service provider to port the

customer's number. Once the current service provider verifies this information (thus "validating the port"), the two service providers coordinate through the numbering administrator to port the customer's number to the new service provider. As in SIM swapping fraud, when a bad actor successfully impersonates the customer of a wireless carrier and convinces the carrier to port the real customer's telephone number to a new service provider and a device that the bad actor controls, the bad actor gains control over the customer's phone number and can intercept both text messages and phone calls intended for the victim.

7. Once a fraudulent SIM swap or port-out request has been completed, the bad actor has acquired the means to take over many more of the victim's accounts. Such account takeover tactics can cause substantial consumer injury. Because text messages are often used by banks, businesses, and payment services to verify a customer's identity when a customer requests updates to accounts, intercepting a text message used to authenticate a customer can allow a bad actor to reset a customer's password and take over the customer's financial, social media, and other accounts. Having taken over these accounts, the bad actor can then change login credentials, drain bank accounts, and, increasingly, steal cryptocurrency and sell or try to ransom social media accounts.[4] Loss of service on a customer's device—the phone going dark or only allowing 911 calls—is typically the first sign of a SIM swapping or port-out scam. There are also media reports that, in some instances, a hacker was able to perpetrate a ***14123** "partial porting fraud" by changing the carrier for delivery of SMS messages without changing the primary carrier for purposes of voice, data, and accounting.[5]

8. The Commission and our sister agency, the Federal Trade Commission (FTC), have received hundreds of consumer complaints about SIM swapping and port-out fraud.[6] Some of the complaints describe wireless carrier customer service representatives and store employees who do not know how to address instances of fraudulent SIM swaps or port-outs, resulting in customers spending many hours on the phone and at retail stores trying to get resolution. Other consumers complain that their wireless carriers have refused to provide them with documentation related to the fraudulent SIM swaps, making it difficult for them to pursue claims with their financial institutions or law enforcement. Several consumer complaints filed with the Commission allege that the wireless carrier's store employees are involved in the fraud, or that carriers completed SIM swaps despite the customer having previously set a PIN or password on the account.

****4** 9. A study published last year by a group of Princeton University researchers examined the types of authentication mechanisms in place at five major wireless carriers, AT&T Mobility, LLC (AT&T), T-Mobile US, Inc. (T-Mobile), Tracfone, US Mobile, and Verizon Wireless (Verizon), to identify the weaknesses that allow for SIM swapping.[7] The researchers opened 50 prepaid accounts (10 with each carrier) and called to request a SIM swap on each account. The researchers found that all five carriers "used insecure authentication challenges that could easily be subverted by attackers."[8] They also found that "in general, callers only needed to successfully respond to one challenge in order to authenticate, even if they had failed numerous prior challenges in the call."[9] In nine instances involving two different carriers, "customer service representatives (CSRs) either did not authenticate the caller or leaked account information prior to authentication."[10]

10. The researchers identified six types of information used by the carriers to authenticate their customers: (1) Personal Information: including street address, e-mail address, date of birth; (2) Account Information: last 4 digits of payment card number, activation date, last payment date and amount; (3) Device Information: IMEI (device serial number), ICCID (SIM serial number); (4) Usage Information: recent phone numbers called; (5) Knowledge: PIN or password, answers to security questions; and (6) Possession: one-time passcode sent via text message or e-mail.[11]

***14124** 11. The researchers found that all of these methods of authentication were or could be vulnerable to abuse. For example, authenticating customers through recent payment information was easily exploitable. According to the researchers, three of the wireless carriers were using payment systems that did not require authentication when using a refill card.[12] An attacker could purchase a refill card at a retail store, submit a re?ll on the victim's account, then request a SIM swap using the known re?ll as authentication.[13] The researchers also found that "using information about recent calls for authentication is exploitable."[14] A bad actor could bait his victim into placing calls to specific phone numbers, and then provide those phone numbers when the customer service representative requested information about outgoing calls.[15] It appeared to the researchers that the customer service representatives also had the discretion to allow authentication with incoming call information.[16] The researchers also found that some of the wireless carriers authenticated their customers through the use of account information or personal information that would have been readily available to bad actors. For example, four of the five carriers authenticated their customers using device information that could be obtained by bad actors.[17] One carrier used preset "security" answers to authenticate its customers. As the authors explained, "[r]ecent research has demonstrated that security questions are an insecure means of authentication, because answers that are memorable are also frequently guessable by an

attacker.""[18] Finally, the research team found that three of the five wireless carriers disclosed personal customer information without authentication, including information that could be used to authenticate a customer.[19]

**5 12. The researchers also "evaluated the authentication policies of over 140 online services that offer phone-based authentication to determine how they stand up to an attacker who has compromised a user's phone number via a SIM swap."[20] They found that 17 websites across different industries have implemented authentication policies with logic ?aws that would allow an attacker to fully compromise an account with just a SIM swap.[21]

13. *Privacy of Telecommunications Customer Information*. Section 222 of the Act obligates telecommunications carriers to protect the privacy and security of information about their customers to which they have access as a result of their unique position as network operators.[22] Section 222(a) requires carriers to protect the confidentiality of proprietary information of and relating to their customers.[23] Section 222(b) provides that a carrier that receives or obtains proprietary information from other carriers ***14125** in order to provide a telecommunications service may only use such information for that purpose and may not use that information for its own marketing efforts.[24] Section 222(c)(1) provides that a carrier may only use, disclose, or permit access to CPNI that it has received by virtue of its provision of a telecommunications service: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[25] CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[26] The Commission has not provided an exhaustive list of what constitutes CPNI, but has explained that CPNI includes (but is not limited to) information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.[27]

14. Beginning in 1998, the Commission promulgated rules implementing the express statutory obligations of section 222.[28] In addition to adopting restrictions on the use and disclosure of CPNI, the Commission adopted a set of rules designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI.[29] Among other things, the Commission required telecommunications carriers to train their personnel as to when they are and are not authorized to use CPNI, and required carriers to have an express disciplinary process in place.[30] In addition, the Commission required each carrier to annually certify its compliance with the CPNI requirements and to make this certification publicly available.[31]

6 ***14126 15. In 2007, the Commission amended its CPNI rules to address "pretexting," the practice of pretending to be a particular customer or other authorized person to obtain access to that customer's call detail or other private communications records.[32] The Commission concluded that "pretexters have been successful at gaining unauthorized access to CPNI"[33] and that "carriers' record on protecting CPNI demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI."[34] To prevent fraudsters from impersonating a telephone company's customer, the Commission amended its CPNI rules to restrict the release of call detail information[35] based on customer-initiated telephone contact, impose password requirements for customer account access, and require carriers to appropriately authenticate both new and existing customers seeking access to CPNI online.[36] The Commission also required carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI[37] and to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed.[38] To protect customers from malicious account changes, these carrier notifications cannot reveal the changed account information, nor can they be sent to any updated account information associated with the change.[39] In addition, the Commission modified its CPNI rules to require carriers to notify law enforcement and customers of security breaches involving CPNI.[40] The Commission has made clear that carriers are free to bolster their security measures through additional measures to meet their section 222 obligations to protect the privacy of CPNI, and that carriers have a fundamental duty to remain vigilant in their protection of CPNI.[41] Finally, the Commission also extended the application of its CPNI rules to providers of interconnected VoIP service, finding that it is "reasonable for American consumers to expect that their telephone calls are private irrespective of whether the call is made using the services of a wireline carrier, a wireless carrier, or an interconnected VoIP provider, given that these services, from the perspective of a customer making an ordinary telephone call, are virtually indistinguishable."[42] Also in 2007, Congress adopted criminal prohibitions both on obtaining CPNI from a telecommunications carrier and on the sale,

transfer, purchase, or receipt of fraudulently obtained CPNI.[43]

****7** 16. *Local Number Portability*. The LNP process gives consumers the ability to retain their phone numbers when switching telecommunications service providers and enhances competition by ***14127** enabling consumers to choose a provider that best suits their needs. Section 251(b)(2) of the Act requires local exchange carriers (LECs) to "provide, to the extent technically feasible, number portability in accordance with requirements prescribed by the Commission."[44] The Act and the Commission's rules define number portability as "the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another."[45] Section 251(e)(1) of the Act gives the Commission exclusive jurisdiction over the North American Numbering Plan and related telephone numbering matters in the United States.[46] Although the Act excludes CMRS providers from the statutory definition of "local exchange carrier," the Commission extended the LNP obligations to CMRS providers pursuant to its independent authority in sections 1, 2, 4(i) and 332 of the Act.[47]

17. Since 2002, wireless carriers have been required to provide wireless number portability, but the Commission has not codified customer validation requirements for porting phone numbers between wireless carriers in our rules.[48] In 2003, the Commission offered guidance on wireless number portability.[49] Among other things, the Commission found that, absent an agreement setting additional terms, wireless carriers need only share basic contact and technical information with each other sufficient to validate and execute the port.[50] The Commission also found that it did not "see a present need to propose formally incorporating the industry standard [two-and-one-half-hour porting interval] in our rules," but "view[ed] this industry standard as feasible and []encourage[d] carriers to complete wireless-wireless ports within this timeframe."[51]

18. In 2007, the Commission clarified that a porting-out provider may not require more than a "minimal but reasonable" amount of information from the porting-in provider to validate the port request and accomplish the port.[52] The Commission observed that the wireless industry had reached an ***14128** agreement to require only three fields of information to validate a simple port request—the customer telephone number, account number, and password (if applicable).[53] The Commission concluded that for simple[54] WIRELINE-TO-wireline, wireless-to-wireless, and intermodal ports, lnp validation should be based on no more than four fields: (1) 10-digit telephone number; (2) customer account number; (3) 5-digit zip code; and (4) passcode (if applicable).[55] The Commission found that use of these four fields "will sufficiently protect consumers from slamming," the switching of a consumer's traditional wireline telephone company for a local, local toll, or long distance service without permission, and explained that data in the record suggested that "complaints about unauthorized ports occur much less frequently for wireless-to-wireless ports, where only three validation fields are used, than for intermodal ports."[56]

****8** 19. To ensure that consumers were able to port their telephone numbers efficiently and to enhance competition for all communications services, in 2009 the Commission adopted the *Porting Interval Order*, which reduced the porting interval for simple wireline and simple intermodal port requests to one business day.[57] The Commission reasoned that delays in porting cost consumers time and money and limit consumer choice and competition because consumers would abandon efforts to switch providers when they got frustrated with slow porting.[58]

20. In 2010, to ensure that customers could easily port numbers between carriers, the Commission adopted an Order standardizing the data exchanged between carriers when service providers execute a wireline or intermodal simple port subject to the one-business day porting interval.[59] The Commission concluded that 14 information fields are necessary to accomplish a simple wireline or intermodal port, and thus mandated that service providers use those 14 fields—and only those fields—to accomplish such ports.[60] The Commission maintained the same three customer-provided information ***14129** fields from the *2007 LNP Four Fields Declaratory Ruling*—the ported telephone number, the customer's account number, and customer's zip code—to help protect against fraudulent ports. To further help protect against fraudulent ports, the rules also permit customers to request that a user-created passcode be put on their account, which the consumer must then provide before a port can be accomplished.[61] The Commission at the time found that the exchange of these fields struck the appropriate balance between streamlining the porting process and ensuring accurate ports, and also reasonably balanced consumer concerns about unauthorized ports with competitors' interest in ensuring that porting obligations may not be used in an anticompetitive manner to inhibit consumer choice.[62] Wireless-to-wireless ports continued to be governed by the *2007 LNP Four Fields Declaratory Ruling* for customer-provided fields of information and their own industry agreement regarding technical fields.

21. The members of the non-governmental, multi-stakeholder Number Portability Industry Forum (NPIF) have created "Best Practices" for porting between and within telephony carriers.[63] These Best Practices are voluntary and not mandated by the Commission, but reflect the consensus of the NPIF or its predecessor organization regarding the preferred processes for porting. Best Practice 73 (Unauthorized Port Flow) specifically addresses unauthorized ports, including fraudulent ports.[64] Among other things, Best Practice 73 encourages carriers to review "incident and/or police report details if provided (official document showing case number or other verification that the matter was reported or attempted to be reported to law enforcement by reporting end user is acceptable)" and places priority on resolving unauthorized ports that have a heightened severity of impact, including "FCC/PUC/Attorney General complaint; court order; military institution; medical facility; business lines (i.e. national organization, main published line); emergency services; medical support services; or otherwise documented as properly reported to law enforcement."[65]

***14130 III. DISCUSSION**

****9** 22. We believe that our CPNI and number porting rules are ripe for updates that could help prevent SIM swapping and port-out fraud.[66] In this Notice, we propose to prohibit wireless carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer. We also propose to amend our CPNI rules to require wireless carriers to develop procedures for responding to failed authentication attempts and to notify customers immediately of any requests for SIM changes. We also seek comment on whether we should impose customer service, training, and transparency requirements specifically focused on preventing SIM swap fraud. We likewise propose to amend our number porting rules to combat port-out fraud while continuing to encourage robust competition through efficient number porting. Finally, we consider whether we should adopt any other changes to our rules to address SIM swap and port-out fraud, including the difficulties encountered by victims of these schemes. We seek comment on our proposals and invite input from stakeholders on how to best tailor the rules to combat this growing, pernicious fraudulent activity.

A. Strengthening the Commission's CPNI Rules to Protect Consumers

23. *Customer Authentication Requirements for SIM Change Requests*. To reduce the incidence of SIM swap fraud, we propose to prohibit carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer, and to define "SIM" for purposes of these rules as a physical or virtual card contained with a device that stores unique information that can be identified to a specific mobile network.[67] We seek comment on these proposals. Consistent with the recommendations made last year by the Princeton Research team that studied SIM swapping, we propose that use of a pre-established password;[68] a one-time passcode sent via text message to the account phone number or a pre-registered backup number; a one-time passcode sent via e-mail to the e-mail address associated with the account; or a passcode sent using a voice call to the account phone number or a preregistered back-up telephone number would each constitute a secure method of authenticating a customer prior to a SIM change.[69] We seek comment on this proposal and whether it will serve as an effective deterrent to SIM swapping fraud.

24. Are each of these authentication methods secure? Since 2016, the National Institute of Standards and Technology (NIST) has recognized known risks associated with SMS-based authentication, distinguishing "SMS-based authentication from other out-of-band authentications methods due to heightened security risks including 'SIM change."D'[70] In addition, recent media reports call into question the security of using text messages for authentication purposes. For example, a recent investigation found that SMS-based text messages could be easily intercepted and re-routed using a low-cost, online marketing service that helps businesses do SMS marketing and mass messaging.[71] As with ***14131** SIM swap fraud, once the hacker was able to re-route a target's text messages, the hacker was also able to access other accounts associated with that phone number. Wireless carriers reportedly have mitigated the security vulnerability uncovered in this investigation.[72] Has this vulnerability has been fixed so that it is no longer a threat to customers of any carrier? What rules could we adopt to ensure that authentication using text messages is secure and effective to protect consumers from SIM swap fraud? Or alternatively, should we prohibit carriers from using text messaging, or specifically SMS text messaging, to authenticate customers requesting SIM swaps? What steps could we take to prevent a customer's text messages from being forwarded without authorization? Should we, for example, require companies offering the text forwarding services to call the customer whose texts will be forwarded to confirm consent prior to forwarding? If so, what authority may we rely upon to adopt such a rule? Are such methods effective? What other steps should we take to help secure customers' accounts and text messages?

****10** 25. All of the methods of authentication that we propose to include in the requirement to authenticate a wireless

customer before allowing for a SIM swap are familiar ones, already used by consumers and companies in various other circumstances. Based on stakeholder experience with these methods of authentication, how burdensome would our proposed authentication requirement be on customers making legitimate SIM change requests? Would they pose particular challenges to customers whose phone associated with their account has been lost, stolen, or destroyed, or customers who are not comfortable with technology, or to customers with disabilities? Should customers be able to opt-in or opt-out of certain methods of authentication?

26. We also invite comment on whether there are other secure methods of authentication that we should allow carriers to use to authenticate their customers in advance of effectuating a SIM change. What practices and safeguards do carriers currently employ to authenticate customers when SIM change requests are made? Have carriers implemented any processes and protections to address SIM swap fraud specifically? If so, have those practices been effective? Do carriers use multi-factor authentication and has it been effective in preventing SIM swap fraud? If so, should we adopt a multi-factor authentication requirement to prevent SIM swap fraud? If we do require multi-factor authentication, is texting sufficiently secure to permit it as an authentication method for use in multi-factor authentication? Are there emerging technologies or authentication methods in development that could potentially be implemented to protect customers from SIM swap fraud? Are there other security measures incorporated into handsets or operating systems that can be used to authenticate or otherwise prevent SIM swap fraud? Could blockchain technologies that store data in a decentralized manner offer additional security when authenticating customers requesting SIM changes? Are there limitations in these technologies, such as security, storage, scalability, and cost that could place a burden on providers and manufacturers of SIMs? What privacy risks are associated with any of these methods or others suggested by commenters? How effective would any of these methods be at deterring SIM swap fraud? As with the methods we have proposed, what challenges do other secure methods of authentication pose to customers and how burdensome would they be on customers making legitimate SIM change requests, particularly those customers who are no longer in possession of their cell phone because it was lost, stolen, or destroyed, or customers who are not comfortable with technology, or customers with disabilities? What are the costs to carriers for any alternative secure authentication methods?

27. If we adopt a specific set of authentication practices that carriers must employ before effectuating a SIM change, how can we account for changes in technology, recognizing that some of these methods may become hackable over time, while additional secure methods of authentication will likely be ***14132** developed over time? We seek comment on whether instead of requiring specific methods of authentication, we should adopt a flexible standard requiring heightened authentication measures for SIM swap requests. The Commission has previously found that "techniques for fraud vary and tend to become more sophisticated over time" and that carriers "need leeway to engage emergingthreats."[73] The Commission has allowed carriers to determine which specific measures will best enable them to ensure compliance with the requirement that carriers take reasonable measures to discover and protect against fraudulent activity.[74] We observe that to the extent carriers have already implemented or are considering implementing additional protections against SIM swap fraud, we want to ensure that any rules we adopt do not inhibit carriers from using and developing creative and technical solutions to prevent SIM swap fraud or impose unnecessary costs. Would codifying a limited set of methods for authenticating customers in advance of approving SIM swapping requests reduce carriers' flexibility to design effective measures and, in effect, reduce their ability to take aggressive actions to detect and prevent fraudulent practices as they evolve? Could requiring specific methods of authentication provide a "roadmap" to bad actors? What costs would such requirements impose on carriers, particularly smaller carriers?

****11** 28. To that end, we seek comment whether we should instead require carriers to comply with the NIST Digital Identity Guidelines, which are updated in response to changes in technology, in lieu of other proposals.[75] The NIST Digital Identity Guidelines are a set of guidelines that provide technical requirements for federal agencies "implementing digital identity services," focusing on authentication.[76] Would requiring carriers to adopt and comply with these guidelines "future proof" authentication methods? Would these guidelines effectively protect consumers in the context of SIM swap fraud? Are these guidelines generally applicable in the telecommunications context, and do the guidelines provide sufficient flexibility to carriers? Would requiring carriers to comply with the guidelines pose any difficulties for smaller providers, and would the authentication methods recommended in the guidelines pose any particular challenges to customers? We also seek comment on whether there are other definitive government sources that we could consider adopting as appropriate authentication methods.

29. We also seek comment on what would be an appropriate implementation period for wireless carriers to implement any

changes to their customer authentication processes. Because of the serious harms associated with SIM swap fraud, we believe that a speedy implementation is appropriate. Are there any barriers to a short implementation timeline and, if so, what are they? What could we do to eliminate or reduce potential obstacles? Will smaller wireless carriers need additional time to implement the requirements we propose?

30. Are there other ways we can strengthen the Commission's customer authentication rules to better protect customers from SIM swap fraud? For example, for online access to CPNI, our rules require a carrier to authenticate a customer "without the use of readily available biographical information[] or account information."[77] Given evidence of the ease with which bad actors can create recent payment or call detail information,[78] we propose to make clear that carriers cannot rely on such information to authenticate customers for online access to CPNI. We invite comment on that proposal.

***14133** 31. We also seek comment on whether there are other methods of authentication that carriers should be allowed to implement to prevent SIM fraud that originates in retail locations. Our rules currently allow carriers to disclose CPNI to a customer at a carrier's retail location if the customer presents a valid photo ID.[79] We seek comment on whether a government-issued ID alone is sufficient for in-person authentication. How prevalent is in-person fraud using fake IDs as a source of SIM swap fraud? What role can, and should, retail stores play in authentication, particularly in situations where customers do not have access to technology or are not tech savvy? Should customer authentication requirements be the same for SIM changes initiated by telephone, online, or in store?

****12** 32. We also invite comment on whether we should amend our rule on passwords and back-up authentication methods for lost or forgotten passwords.[80] Our rules require a carrier to authenticate the customer without the use of readily available biographical information or account information to establish the password.[81] We permit carriers to create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information or account information.[82] Should we make changes to this requirement? If so, what changes are needed? Do the existing rules create vulnerabilities that should be addressed? Should these requirements be updated to reflect any changes in technology? How would they enhance the protections already provided to consumer passwords?

33. *Response to Failed Authentication Attempts*. We propose to require wireless carriers to develop procedures for responding to failed authentication attempts, and we seek comment on this proposal. We seek comment on what processes carriers can implement to prevent bad actors from attempting multiple authentication methods while at the same time ensuring that protections do not negatively impact legitimate customer requests. For example, would a requirement that SIM swaps be delayed for 24 hours in the case of multiple failed authentication attempts while notifying the customer via text message and/or e-mail, be effective at protecting customers from fraudulent SIM swaps? If we adopt such a rule, should we specify the number of attempts, and if so, how many attempts should trigger the 24-hour delay? How burdensome would this be for customers, and what costs would this impose on carriers? How long would it take carriers to develop and implement procedures for responding to failed authentication attempts? Would such a requirement have anti-competitive effects?

34. *Customer Notification of SIM Change Requests*. As part of our effort to protect consumers from fraudulent SIM swapping, we propose to require wireless providers to notify customers immediately of any requests for SIM changes. We seek comment on this proposal. Is it unnecessary if we adopt specific heightened authentication requirements prior to providing a SIM swap? Or will it provide a worthwhile second line of protection against fraudulent SIM swaps?

35. Our CPNI rules currently require carriers to notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.[83] This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.[84] As the Commission found with respect to these other types of account changes, we believe that notification of SIM change requests could be an important tool for customers to monitor their account's security, and ***14134** could help protect customers from bad actors "that might otherwise manage to circumvent []authentication protections" and enable customers "to take appropriate action in the event" of fraudulent activity.[85] Do commenters agree?

****13** 36. We also seek comment on how this notification should be provided to customers. We believe that the verification methods provided in our rules for other types of account changes may be insufficient to protect customers from SIM swap

fraud because in these situations, the bad actor has taken control of the customer's account and any verification communications sent after the transfer by voicemail or text may be directed to the bad actor rather than to the victim. Moreover, mail to the address of record will likely be too slow to stop the ongoing fraud that may involve financial accounts, social media profiles, and other services. We therefore propose to amend our rules to include notification requirements that would more effectively alert customers to SIM fraud on their accounts and seek comment on what types of notification would be most effective in alerting customers to SIM swap fraud in progress. Would e-mail notification be more effective? Should we retain the option to send such notifications by mail even though this method involves significant delay? Should carriers be required to give customers the option of listing a personal contact (e.g., a spouse or family member) and then inform that contact that the customer is requesting a SIM swap? What other methods of communication could be used to get timely notification to customers, particularly those customers who are no longer in possession of their device because it has been lost or stolen?

37. In addition to immediate customer notification of requests for SIM swaps, we seek comment on requiring up to a 24-hour delay (or other period of time) for SIM swap requests while notifying the customer via text message, e-mail, through the carrier's app, or other push notification[86] and requesting verification of the request. Once a customer verifies the SIM change request either via text, the carrier's app (if the device is in the customer's possession), an e-mail response, or the customer's online account, the carrier would be free to process the SIM change. If we adopt heightened authentication requirements, is a temporary delay in transferring the account to a new SIM necessary to ensure sufficient time for a customer to receive the notification of activity on the account and take action if the customer has not initiated the changes? Would this requirement be effective in preventing SIM swap fraud? How burdensome would such a delay be for customers? Are there safety implications for customers who legitimately need a new SIM? Could such a delay prevent the customer from completing 911 calls during the waiting period? What costs would this requirement impose on carriers, and how long would it take carriers to develop, test, and implement such a process? Would such a requirement be anti-competitive? Should we consider other approaches to customer notifications of SIM transfers?

38. *Customer Service, Training, and Transparency*. Additionally, we seek comment on whether we should impose customer service, training, and/or transparency requirements specifically focused on preventing SIM swap fraud. For example, should we require carriers to modify customer record systems so that customer service representatives are unable to access CPNI until after the customer has been properly authenticated? Would this approach be effective in preventing customer service representatives from assisting with authentication through the use of leading questions or other more nefarious employee involvement in SIM swap fraud? Would a requirement for record-keeping of the authentication method used for each customer deter employee involvement in SIM swapping fraud? Are there ways to avoid employee malfeasance, such as requiring two employees to sign off on every SIM change? What burdens would be associated with these possible requirements? Anecdotal evidence suggests that, in some cases, customer service representatives are not trained on procedures to deal with customers who have been victims of SIM swap fraud, and as a result, customers who are already victims ***14135** have difficulty getting help from their carriers. To address this concern, we seek comment on whether we should impose training requirements for customer service representatives to address SIM swap fraud attempts, complaints, and remediation. What costs would these measures impose on carriers? Is there a way to reduce the burdens of these proposals while still achieving the policy aims? Would these proposals reduce SIM swap fraud or otherwise impact the customer experience? How long would it take wireless carriers to implement any new training requirements? Are there alternative approaches that might be more effective or efficient?

****14** 39. We also seek comment on whether we should require wireless providers to offer customers the option to disable SIM changes requested by telephone and/or online access (i.e., account freezes or locks).[87] We believe that offering these protections would impose minimal burdens on carriers while offering significant protection to customers. Do commenters agree? Whether or not we require wireless providers to offer such services, we also seek comment on whether we should require carriers to provide a transparent, easy-to-understand, yearly notice to customers of the availability of any account protection mechanisms the carrier offers (e.g., SIM transfer freeze, port request freezes, PINs, etc.). What costs would such notification requirements impose on carriers? We believe that any customer notifications should be brief, use easy-to-understand language, and be delivered in a manner that is least burdensome to customers. We seek comment on what form such notifications could take and how they could be delivered to customers to provide meaningful notice of such services while imposing minimal burden on carriers. Do we need to prescribe a method or methods for customers to unfreeze or unlock their accounts? What methods would be sufficiently secure? Would an unfreeze or unlock be immediate or should there be a waiting period before an unlocked account can be transferred?

40. *Accounts with Multiple Lines*. We seek comment on how these proposed CPNI rule changes impact wireless accounts with multiple lines, such as shared or family accounts. If we require the customer to provide a one-time passcode for the carrier to execute a SIM change, should each line on the shared or family account have its own passcode? If the account owner elects to freeze the account to protect against unauthorized changes, how can we ensure that another member of the shared or family account remains able to port-out his or her number? Should the freeze option apply only to individual lines and not to entire accounts? Do our proposed rules impact these types of accounts with multiple lines in any other ways?

41. *Remediation of SIM Swap Fraud*. We seek comment on how we can enable timely resolution of SIM swap fraud to minimize financial and other damage to customers who are victims of SIM swap fraud. How can we encourage and/or ensure that carriers quickly resolve complaints in cases of SIM swap fraud? Should we require carriers to respond to customers and offer redress within a certain time frame? What would be the costs to carriers, and what are the costs to customers if we do not do so? We seek comment on the methods wireless carriers have established to help victims of SIM swap fraud halt an unauthorized SIM swap request or to recover their phone numbers from bad actors.[88]

42. *Carriers' Duty to Protect CPNI*. We also seek comment on codifying the Commission's expectation that carriers must take affirmative measures to discover and protect against fraudulent activity beyond the measures specifically dictated by our rules and that additional measures (e.g., self-monitoring) are required to comply with section 222's mandate to protect the confidentiality of customer information. In the *2007 CPNI Order*, the Commission codified the requirement that carriers take reasonable measures to discover and protect against unauthorized access to CPNI,[89] and specified that adoption of the rules in ***14136** that *Order* does not relieve carriers of their fundamental statutory duty to remain vigilant in their protection of CPNI,[90] nor does it insulate them from enforcement action for unauthorized disclosure of CPNI. The Commission allowed carriers flexibility in how they would satisfy their statutory obligations but expressed an expectation that carriers would take affirmative measures to discover and protect against fraudulent activities beyond what is expressly required by the Commission's rules.[91] We seek comment on whether codifying a requirement to take affirmative measures to discover and protect against fraudulent activities would lead to more effective measures to detect and prevent SIM swap fraud. Has the expectation expressed in 2007 been effective?[92] Would the additional threat of enforcement of a codified rule create additional incentives for carriers to take more aggressive action to detect and prevent fraudulent access to CPNI? We seek comment on whether there are additional requirements needed to ensure that carriers comply with their legal obligations under section 222 to detect and prevent SIM swap fraud.

****15** 43. *Tracking the Effectiveness of Authentication Measures*. We seek comment on what data carriers collect about SIM swap fraud, and whether we should require that carriers track data regarding SIM swap complaints to measure the effectiveness of their customer authentication and account protection measures. What would be the burdens of requiring wireless carriers to internally track customer SIM swap complaints? Do wireless carriers already report this information to the U.S. Secret Service and Federal Bureau of Investigation (FBI) pursuant to the Commission's rules?[93] We also seek comment on whether we should modify our breach reporting rules to require wireless carriers to report SIM swap and port-out fraud to the Commission, and what the costs would be to carriers of doing so, including the timeframe for implementing such a requirement. Should we require carriers to inform the Commission of the authentication measures that they have in place and when those measures change? Would requiring carriers to update the Commission about changes to authentication measures, along with the frequency of customer SIM swap complaints, be sufficient to enable the Commission to evaluate the efficacy of a carrier's authentication measures, or should the Commission require carriers to provide additional information? We also seek comment on how we should ensure carrier compliance with any proposed obligations that we adopt. For example, should we specifically direct the Commission's Enforcement Bureau, or another Bureau or Office, to conduct compliance audits? Are there other audits or models that we should use as guidelines to ensure compliance? We seek comment on the best method to enforce our proposals.

44. *Applicability of Customer Authentication Measures*. We seek comment on whether any new or revised customer authentication measures we adopt should apply only to wireless carriers and only with respect to SIM swap requests, or whether such expanded authentication requirements would offer benefits for all purposes and with respect to all providers covered by our CPNI rules. Is there anything unique about VoLTE service or the upcoming Voice over New Radio (VoNR) that we need to ***14137** consider?[94] Further, as the nation's networks migrate from 2G and 3G to 4G and 5G, are there particular technical features that should be taken into consideration regarding authentication requirements? Is the type of phone number takeover that occurs through SIM swap fraud only relevant to mobile phone numbers (due to SIM swaps and

text message-based text authentication)? Are there also concerns with respect to account takeovers of interconnected Voice over Internet Protocol (VoIP) services,[95] one-way VoIP services, and landline telephone services? Even if the same concerns are not present (or as strongly present), should we apply any stronger authentication requirements to all providers to protect customers' privacy and to provide uniform rules across all providers? If so, under what legal authority could we extend the proposed authentication requirements to services other than wireless? Is there value to uniformity with other categories of providers? Would costs imposed on these carriers outweigh the limited benefit of these requirements related to non-wireless carriers? Are there any other rules that would need to be aligned for consistency if we make changes to the CPNI rules to address SIM swap fraud? In addition, if limited to wireless providers only, we believe that any new rules we adopt should apply to all providers of wireless services, including resellers. Do commenters agree?

**16 45. We also seek comment on whether any new rules should apply only to certain wireless services, such as pre-paid services. Is SIM swap fraud limited to, or more prevalent with, pre-paid or post-paid wireless accounts? Do wireless resellers (many of which offer pre-paid services) encounter this type of fraud more or less often than facilities-based carriers? We invite comment on whether some or all changes discussed here should apply to all mobile accounts or whether certain changes should be limited to pre-paid or post-paid accounts only. We note that pre-paid plans generally do not require credit checks and therefore subscribers to prepaid plans may be more low-income and economically vulnerable individuals. Would such requirements impose disproportionate burdens on these customers?

46. We also seek comment on the scope of any changes that we may make to the CPNI rules to address SIM swap fraud. Specifically, should any new rules be narrowly tailored to deal only with SIM swap fraud, or should they be broader to ensure that they cover the evolving state of fraud on wireless customers?[96] Outside of the account takeover context, are there benefits to providing expanded authentication requirements before providing access to CPNI to someone claiming to be a carrier's customer? We seek comment on whether any heightened authentication measures required (or prohibited) should apply for access to all CPNI, or only in cases where SIM change requests are being made.

47. In addition, we seek comment on the impact that our proposed rules could have on smaller carriers. Would the proposed requirements impose additional burdens on smaller carriers? Would they face different costs than larger carriers in implementing the new requirements, if adopted? Would smaller carriers need more time to comply with new authentication rules? Do they face other obstacles that we have not considered here?

48. We believe that we have authority to adopt the proposed rules discussed in this section pursuant to our authority under sections 4, 201, 222, 303, and 332 of the Act,[97] and we seek comment on *14138 this conclusion. Do we have additional sources of authority on which we may rely here?[98] To the extent that we have not already done so, we also solicit input on the relative costs and benefits of our proposals to amend the CPNI rules to address SIM swap fraud. How many legitimate SIM swap requests do carriers receive yearly, and what are customers' most common reasons for requesting a legitimate SIM swap? Is there any evidence concerning the degree to which authentication measures limit legitimate SIM swaps, or the degree to which they successfully prevent fraud? We ask commenters for input on how any of these proposals could positively or negatively affect the customer experience and whether they foresee any unintended consequences from the changes we propose here.

B. Strengthening the Commission's Number Porting Rules to Protect Consumers

**17 49. We next seek comment on proposals to strengthen our number porting rules to protect customers from unauthorized ports and port-out fraud. One reason that number porting can be used to subvert two-factor authentication may be the relative ease with which carriers fulfill port order requests from other carriers.[99] The Commission has, in the past, been concerned that adding "additional steps for the customer would also add a layer of frustration and complexity to the number porting process, with anticompetitive effects."[100] While the Commission remains committed to "facilitat[ing] greater competition among telephony providers by allowing customers to respond to price and service changes ...,"[101] we seek comment below on what additional measures we can adopt to protect customers from port-out fraud.

50. *Notification of Wireless Port Requests and Customer Authentication Processes*. We propose to require wireless carriers to provide notification to customers through text message or other push notification to the customer's device whenever a port-out request is made to ensure that customers may take action in the event of an unauthorized port request, and seek comment on our proposal. For example, Verizon sends its customers a text message letting the customer know that a port-out

request has been initiated.[102] When the request is completed, Verizon will send the customer an e-mail stating that the port to the new service was successful.[103] AT&T may also "send customers a text message to help protect them from illegal porting. This notification will not prevent or delay the customer's request. It just adds ***14139** a simple step to better protect against fraud."[104] We believe that requiring customer notice of port requests could be a minimally intrusive protective measure that could be automated to minimize delays while providing significant protections for customers. Do commenters agree? Do other carriers currently notify their customers of port-out requests? What would be the costs for carriers to implement such a requirement, particularly for smaller carriers? How much time would carriers need to implement such a requirement? Would requiring notification of port requests to customers harm competition? Is there a particular method of notification that is most effective? For this and other potential rules that may require text messages and/or push notifications, should we define the scope of permissible text messages or other push notifications and, if so, what definition or definitions should we use?[105]

51. We also seek comment on whether a port request notification requirement is sufficient to protect customers from port-out fraud, or whether we should also require customer verification or acknowledgement of the text message or push notification through a simple Yes/No response mechanism. Would a customer port verification requirement unreasonably hinder the porting process, and could it be used anticompetitively by carriers? Should we require that customers respond within a certain amount of time before the carrier can execute the port? We recognize that some customers may not frequently check their text messages or push notifications, which could lead to a delay if we require the customer to verify the port. Should we require carriers to send follow-up messages to the customer via e-mail or a phone call? What other processes have wireless carriers adopted to protect customers from port-out fraud, and have they been effective in reducing port-out fraud?

****18** 52. As discussed above, the National Institute of Standards and Technology and recent media reports call into question the security of using text messages for authentication purposes.[106] Is notification and/or verification of a port request via text message a secure means of authenticating the validity of a customer's wireless port request? Should we instead require an automated notification call and verification response through a voice call or other method, such as e-mail or carrier app? What methods would ensure that customers who have voice-and-text-only service, or whose devices are incapable of accessing a carrier's app or website, are not hindered in their porting choices? Are there any barriers for smaller carriers implementing any of these changes to protect customers' accounts from port-out fraud?

53. We seek comment whether we should require customers' existing wireless carriers to authenticate a customer's wireless port request through means other than the fields used to validate simple port requests. Are the benefits of potentially protecting customers from port-out fraud outweighed by the potential harms to competition from delaying or impeding customers' valid wireless number port requests? We seek comment on the processes that wireless carriers, including MVNO providers, resellers, and smaller carriers, currently use to authenticate customer port-out requests, and whether those methods are effective in preventing port-out fraud. According to CTIA, "[w]ireless providers are constantly improving internal processes to stay ahead of ... bad actors, while protecting the rights of legitimate customers to transfer their phone number to a new device or wireless provider," including "[s]ending one-time passcodes via text message or e-mail to the account phone number or the e-mail associated with the account when changes are requested ...."[107] Verizon will not allow its customers to transfer their number to a different carrier unless that customer first requests a Number Transfer Pin.[108] ***14140** When a Verizon customer requests a port from its new service provider, the customer must present the Verizon account number and Number Transfer Pin in order to authenticate the request.[109] AT&T customers can create a unique passcode that in most cases the customer is required to provide "before any significant changes can be made including porting through another carrier,"[110] and starting September 30, 2021, will require customers to request a Number Transfer PIN to transfer their number to another service provider, which will replace the account passcode customers currently use.[111] T-Mobile assigns each of its customer accounts a 6-15 digit PIN that must be provided whenever an individual requests to port-out the phone number associated with that account.[112] Have such port-out PINs been effective at protecting customers from port-out fraud? Have carriers noticed any effect from adopting port-out PINs or other additional security measures on their customers' likelihood of switching carriers? Is there any evidence indicating how security measures affect porting frequency? Should we require wireless carriers to authenticate customers for wireless port requests under the same standard as we require carriers to authenticate customers for SIM change requests, recognizing that in the porting context, the Act sets forth competing goals of protecting customer information and promoting competition through local number porting? What would be the benefits and costs of doing so?

****19** 54. We seek comment on any other technical or innovative solutions for customer authentication for port requests that carriers could implement to reduce port-out fraud. For example, are there technologies developed out of the Mobile

Authentication task force, a collaboration among the three major U.S. wireless carriers, that could be easily implemented into the port authentication process? ZenKey, which was developed under the auspices of the Mobile Authentication task force, "collects and shares device and account data with your wireless carrier ... [to] easily and more securely authenticate, sign up, and sign in,"[113] and "uses multi-factor authentication, including unique network signals, to not only verify a user's device but also allow verification that the user is who they say they are."[114] Could carriers use similar technology to authenticate wireless customer port requests? What would be the costs of doing so and what are the challenges to implementation, including customer privacy and consent implications? What other technologies exist that carriers could use to quickly and effectively authenticate wireless port requests to reduce port-out fraud? As the nation's networks migrate from 2G and 3G to 4G and 5G, are there particular technical features that should be taken into consideration for protecting customers from port-out fraud?

55. We seek comment on whether we should require all carriers to implement any of the additional authentication processes for wireless port requests some providers have already developed and implemented. Is there value in uniformity? Would it reduce consumer confusion if we mandate the same authentication requirements on all wireless port-out requests regardless of the providers involved? Would that potential reduction in consumer confusion outweigh the benefits of enabling carriers to create innovative procedures to protect against port-out fraud attempts as they evolve? Would requiring specific additional customer authentication procedures, as opposed to simply making it clear that carriers are responsible for preventing port-out fraud, provide a roadmap to bad actors? Should we instead require ***14141** carriers to develop heightened customer authentication procedures like those already initiated by the three nationwide wireless carriers, but provide flexibility to the individual carriers to create and employ what works best for their service? Should we require different authentication procedures for pre-paid wireless account port-out requests than we do for post-paid wireless account port-out requests? We also seek comment on what implementation period the wireless industry would need to implement any additional validation requirements and processes we adopt.

56. We seek comment on how additional port authentication requirements would affect the timing of simple wireless-to-wireless ports. Would allowing additional authentication procedures cause unreasonable delay to the wireless porting process or cause harm to competition? In adopting any additional customer authentication requirements, we want to ensure that we leave carriers in a position to innovate and address new problems as they arise. Relatedly, we seek comment on whether it is necessary to codify a simple wireless-to-wireless porting interval to ensure that any new port authentication requirements do not lead to delay in the current porting process. The wireless industry has voluntarily established an industry standard of two and one-half hours for simple wireless-to-wireless ports.[115] Should we codify this interval in our rules?

****20** 57. *Port-Freeze Offerings*. We propose to require all wireless providers, including resellers, to offer customers the option to place a "port-freeze" on their accounts at no cost to the customer to help deter port-out fraud. We observe that our rules currently permit local exchange carriers (LECs) to offer their customers the ability to "prevent[] a change in a subscriber's preferred carrier selection unless the subscriber gives the carrier from whom the freeze was requested his or her express consent."[116] Should we require wireless providers to offer a similar option, and would making this option available to wireless customers deter wireless port-out fraud? Verizon offers customers the option to lock their number, blocking all port-out requests unless the account owner turns off the Number Lock feature through the Verizon mobile app, on Verizon's website, or by calling customer service.[117] Do other wireless carriers currently offer a similar feature? Has this feature, and others like it, been successful at deterring port-out fraud? What costs would offering this feature impose on carriers? How can we make sure that customers are easily notified of this feature? Would a one-time notice for existing customers, and notice at the time service is started, be effective at notifying customers? How often should carriers provide this notice to customers? What method would be least burdensome on carriers while also notifying all customers, including those that do not access their accounts through online services or carrier apps, of the availability of this feature? Local exchange carriers who offer their customers the "preferred carrier freeze" option must follow specific requirements regarding the solicitation and imposition of this option.[118] Should we extend similar requirements to wireless carriers? If we impose these requirements, would the benefits gained by deterring port-out fraud outweigh the costs of this measure?[119] What happens when a customer ***14142** locks his or her account but is unable to recall the information necessary to unlock their account? Should there be a back-up authentication method available? Are there other methods wireless carriers use to prevent unauthorized port requests that we should consider requiring?

58. *Wireless Port Validation Fields*. We also propose to codify the types of information carriers must use to validate simple wireless-to-wireless port requests. Pursuant to the Commission's *2007 LNP Four Fields Declaratory Ruling*, the wireless industry agreed to use three fields of customer-provided information—telephone number, account number, and ZIP

code—plus a passcode field (if customer-initiated) to validate requests for simple wireless-to-wireless ports. We propose to codify this requirement in our rules for simple wireless-to-wireless ports, just as we have codified field requirements for simple wireline and intermodal ports.[120] We preliminarily believe that standardizing the fields necessary to complete a simple wireless-to-wireless port will allow for quicker and more efficient porting,[121] and we seek comment on this view. We propose adopting the existing fields because we are cognizant that imposing new or different customer-required information fields could complicate the porting process, from both the carrier and customer perspectives, and we seek comment on this view. We seek comment whether codifying the existing fields used for validating simple wireless ports, in combination with immediate customer notification of port-requests and the offering and advertisement of port-freeze options as we propose, would help to protect customers from port-out fraud. Do such measures appropriately balance the competitive benefits of rapid porting with protecting customers' accounts from fraud?

**21 59. Are there additional fields of customer-provided information we should require for validation of wireless-to-wireless ports to minimize port-out fraud, while ensuring the continued rapid execution of valid port-out requests? If we require additional fields of customer-provided information for only wireless-to-wireless simple ports, will that cause unnecessary complications for the telecommunications industry as a whole? Will it impose additional costs on wireless carriers that would reduce competition in the telecommunications marketplace? We seek comment on whether requiring carriers to implement changes to the wireless port validation requirements would significantly impair the customer's ability to perform a legitimate port-out request. Would requiring carriers to implement additional customer-provided fields for wireless port requests stifle the ability of customers to switch carriers while retaining their phone number or keep customers locked into contracts with their current service providers? Would customers still be able to respond to price and service changes in a quick and efficient manner? Finally, we propose to make clear that any customer validation requirements apply to both facilities-based wireless carriers and resellers of wireless service and we seek comment on that proposal.

60. We seek comment on whether we should require carriers to implement a customer-initiated passcode field for all wireless number port requests, or whether it should remain optional. While AT&T, Verizon, and T-Mobile offer this option, it is unclear if all customers are required to participate. What would be the burden on customers and carriers, particularly smaller carriers, were we to mandate passcode fields for wireless number port requests? Could it harm competition and cause customer frustration if a customer has either not set up a passcode or does not know how to set up a passcode? Should we require carriers to make a customer-initiated passcode optional on an opt-out rather than opt-in basis? What steps could carriers take to make it least burdensome on customers to establish an account passcode for wireless number porting purposes? We also seek comment on how we can ensure that a customer can make a legitimate port request if he forgets his passcode.

61. *Remediating Port-Out Fraud*. We seek comment on how we can ensure timely resolution of unauthorized port-out requests to minimize financial and other damage to customers who are victims of such fraud. What information do wireless carriers currently collect about port-out fraud? Are wireless *14143 carriers already tracking instances of customer complaints regarding this issue? Should we require that carriers use this information to measure the effectiveness of their customer authentication and account protection measures? How can we encourage and/or ensure that carriers coordinate and work together to quickly resolve complaints in cases of port-out fraud? Should we require carriers to respond to customers who allege they are victims of port-out fraud and to offer redress to such customers within a certain time frame? What would be the costs to carriers, and what are the costs to customers if we do not do so? We seek comment on the methods wireless carriers have established to help victims of port-out fraud stop an unauthorized port-out request or to recover their phone numbers from bad actors.

**22 62. *Accounts with Multiple Lines*. We seek comment on how the proposed changes to our LNP rules impact wireless accounts with multiple lines, such as shared or family accounts. If we require the customer to provide a one-time passcode for the carrier to execute the port, should each line on the shared or family account have its own passcode? If the account owner elects to freeze the account to protect against unauthorized changes, how can we ensure that another member of the shared or family account remains able to port-out their number? Should the port-freeze option apply only to individual lines and not to entire accounts? Do our proposed rules impact these types of accounts with multiple lines in any other ways?

63. *Role of Administrator*. We also seek comment on whether the Local Number Portability Administrator (LNPA) can play a role in thwarting port-out fraud by serving as an authorized neutral third-party to verify customer identification prior to authorizing a port-out request. The LNPA operates the Number Portability Administration Center (NPAC), which "is the

system that supports the implementation of LNP and is used to facilitate number porting in the United States.[122] The LNPA, through the NPAC, currently works with a customer's new service provider to create a number port and sends a notification to the old service provider, once the existing service provider validates and confirms the subscriber's information.[123] What information regarding port requests does the NPAC retain? Is there additional information regarding port requests the NPAC should retain to help prevent port-out fraud? What records could be helpful if provided to customers who have been victims of unauthorized port-out fraud? Through what means and under what conditions, if any, should wireless providers permit their customers to access NPAC data regarding port requests that pertain to the customer's telephone number? Are there additional obligations that we should direct or encourage North American Portability Management, LLC, which oversees the LNPA contract, to impose on the LNPA to safeguard against port-out fraud?

64. As discussed above, the Number Portability Industry Forum has created "Best Practices" for porting between and within telephony carriers.[124] Best Practice 73 (Unauthorized Port Flow) specifically addresses carrier processes for responding to unauthorized ports, including fraudulent ports, which are ports "which occurred as the result of an intentional act of fraud, theft, and/or misrepresentation."[125] We seek comment on the extent to which wireless providers have adopted Best Practice 73. If wireless carriers have adopted Best Practice 73, is it effective in addressing port-out fraud? Are there changes we can make to the process flow to better protect customers? If wireless carriers have not implemented Best Practice 73, we seek comment on other methods they use to investigate potentially fraudulent ports and how they restore service to the customer. Should we require mobile carriers to adopt Best Practice 73 to help speed resolution of fraudulent port complaints? We also seek comment on what ***14144** role the North American Numbering Council (NANC) can play in establishing updated best practices to protect customers from port-out fraud and in reaching industry consensus.

****23** 65. *Partial Porting Fraud*. We seek comment on whether the proposals on which we seek comment above would also be effective against partial porting fraud, where the bad actor changes the consumer's carrier for delivery of SMS messages without changing their primary carrier. Would our proposed customer notification and authentication rule prevent routing of SMS messages through an alternate provider without customer notification? Would a port freeze prevent changing the delivery provider and destination of SMS messages? If not, what changes to the proposed rules would be required to ensure they also apply to partial porting fraud? What additional measures would be necessary to prevent partial porting fraud in addition to the fraud that may occur when a wireless provider completely ports a consumer's mobile service?

66. *Impact on Smaller Carriers*. We seek comment on the impact the LNP rule changes that we discuss above could have on smaller carriers. Would these new requirements impose undue burdens on smaller carriers? Would smaller carriers face different costs from larger carriers in implementing the new requirements, if adopted? Would smaller carriers need more time to comply with revised number porting rules? Do they face other obstacles that we have not considered here?

67. *Legal Authority*. Finally, we seek comment on our legal authority to adopt the possible rules discussed in this section. We propose to rely on authority derived from sections 4, 201, 251(b)(2), 251(e), 303, and 332 of the Act to implement the proposed changes to our number porting rules to address port-out fraud, and seek comment on our proposal.[126] Are there additional sources of authority on which the Commission can rely to implement these proposals? Should we extend any of the LNP rules on which we seek comment to any entities other than wireless carriers, such as landline carriers or VoIP providers? If so, we propose concluding that we have authority to do so pursuant to section 251(e), and we seek comment on this view.[127] We also seek comment on whether we should update the references to "CMRS" in the Commission's number porting rules to reflect evolving technology. Finally, we solicit input on the relative costs and benefits of our proposals to amend the LNP rules to address port-out fraud.

C. Additional Consumer Protection Measures

68. Finally, we seek comment on any additional rules that would help protect customers from SIM swap or port-out fraud or assist them with resolving problems resulting from such incidents. We are aware that customers sometimes need documentation of the fraud incident to provide to law enforcement, financial institutions, or others to resolve financial fraud or other harms of the incident. A SIM swap or port-out fraud victim may have difficulty obtaining such documentation from the carrier because the carrier may not have processes in place to produce such documentation. To provide support for customers who have become victims, we seek comment on requiring wireless carriers to provide to customers (upon request) documentation of SIM swap or port-out fraud on accounts that the customer may then provide to law enforcement, financial institutions, or others. We seek comment on what information should be included in the documentation provided by carriers.

We also seek comment on the potential benefits and projected costs of this proposal, including on smaller providers. Further, we invite input on how the proposed rule would affect the customer experience, either positively or negatively.

**24 69. Next, we seek comment on other measures we can adopt to ensure that customers have easy access to information they need to report SIM swap, port-out, or other fraud. As discussed above, *14145 we believe that customer service representatives should be trained on how to assist customers who have been victims of SIM swap or port-out fraud, and carriers should have procedures in place for a response. Identity theft, including SIM swap fraud, can cause intense anxiety for victims and must be addressed in a timely manner to prevent financial losses and exposure of personal information. Thus, in addition to providing documentation, we believe that it should be easy for a customer to get access to appropriate carrier resources that can help mitigate the significant harms caused by SIM swap or port-out fraud. As such, we seek comment on whether we should adopt rules addressing how wireless carriers deal with customers once they have become victims of SIM swapping and port-out fraud. What procedures do carriers have in place to assist customers in these circumstances and are these procedures effective? What additional steps can carriers take to recover the account and stop the ongoing fraudulent activity? How can carriers ensure that customers have easy access to the information they need to report SIM swap fraud? Should we require wireless carriers to establish a dedicated point or method of contact that is easily accessible by customers and is made available on the carrier's website so that customers can get timely assistance from their carriers?[128] Or, given the time-sensitive nature of most fraud, would it make sense to require carriers to have a dedicated and publicized fraud hotline that customers can call directly in the case of suspected fraud? What costs would such a requirement impose on carriers, and how long would it take for carriers to implement? Are any of the Commission's existing rules obstacles to helping customers recover following a SIM swap or port-out fraud incident?

70. We seek comment on whether there are other customer protections we could adopt to address the problems associated with SIM swap and port-out fraud. For example, should the Commission require wireless carriers to enable "fraud alerts" on accounts and publicize these services to customers? Such fraud alerts could trigger additional protections when changes are requested on the accounts. Would such a requirement be effective at deterring SIM swap and port-out fraud? Would it have any unintended consequences for customers? What would such a requirement cost? Are there any other consumer protections that would be effective in combatting SIM swap and port-out fraud and, if so, how would they operate? What would be their relative costs and benefits? For example, we understand that in other countries, carriers and financial institutions share information about SIM transfers to limit damages to consumers resulting from incidents of SIM swap fraud.[129] As discussed above, section 222 strictly limits carriers' ability to share a customer's CPNI without the customer's consent. Can we, and should we, encourage carriers to establish a mechanism based on express customer consent that would enable a financial institution to determine whether a SIM transfer had been recently completed to help protect customers from the financial harms of SIM swap and port-out fraud? If so, should we require or encourage carriers to ask for customer permission upon set up of accounts (and to send out one-time notice to all existing customers asking if they want to permit this)? Should such a rule require retention of the record of this permission for some designated period of time? Should carriers be permitted to charge a fee for this service either to the wireless customer or to the financial institution? Are there other types of institutions that might need access to the same type of information to prevent fraud? Should our rules expressly permit or prohibit this type of service? What are the potential risks and benefits to consumers? We seek comment on how we can ensure that customers are able to take advantage of third-party fraud services to protect against SIM swap and port-out fraud.

**25 71. We tentatively conclude that our broad Title III authority would support imposing additional consumer protection obligations such as those discussed in this section on wireless carriers. We also seek comment on whether authority derived from sections 4, 201, 222, 251, 303, and 332 would support such additional consumer protection measures. Should we extend any new consumer protection *14146 requirements to interconnected VoIP services, one-way VoIP services, or landline services? If so, pursuant to what legal authority would the Commission adopt such rules? We invite commenters to discuss the relative costs and benefits of these proposals and any foreseeable unintended consequences of the measures we discuss.

72. We seek comment on whether there are standards-setting bodies, industry organizations, or consumer groups that could evaluate this issue to augment our understanding and present possible solutions. For example, could the Alliance for Telecommunications Industry Solutions (ATIS) provide technical expertise that would be useful in determining the best course of action by the Commission to protect customers from SIM swap or port-out fraud? Could relevant trade associations work to develop industry consensus solutions to the problem?

73. *Digital Equity and Inclusion*. Finally, the Commission, as part of its continuing effort to advance digital equity for all,[130]

including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations[131] and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.

IV. PROCEDURAL MATTERS

74. *Ex Parte Rules*. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[132] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with Rule 1.1206(b). In proceedings governed by Rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format ***14147** (*e.g.*,.doc,.xml,.ppt, searchable.pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

****26** 75. *Initial Regulatory Flexibility Analysis*. Pursuant to the Regulatory Flexibility Act (RFA),[133] the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and actions considered in this *Notice of Proposed Rulemaking*. The text of the IRFA is set forth in Appendix B. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the *Notice of Proposed Rulemaking*. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of the *Notice of Proposed Rulemaking*, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration.[134]

76. *Comment Filing Procedures*. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

· Electronic Filers: Comments may be filed electronically using the Internet by accessing ECFS: https://www.fcc.gov/ecfs/.

· Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.

Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

· Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.

· U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street, NE, Washington DC 20554.

· Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, 35 FCC Rcd 2788 (2020). https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy

77. People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at (202) 418-0530 (voice), 202-418-0432 (TTY).

**27 78. *Paperwork Reduction Act of 1995 Analysis*. This document may contain proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) *14148 to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.[135]

79. *Contact Person*. For further information about this rulemaking proceeding, please contact Melissa Kirkel, Competition Policy Division, Wireline Competition Bureau, at (202) 418-7958 or melissa.kirkel@fcc.gov.

V. ORDERING CLAUSES

80. Accordingly, IT IS ORDERED that, pursuant to the authority contained in sections 1, 4, 201, 222, 251, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154, 201, 222, 251, 303(r), and 332, this Notice of Proposed Rulemaking in WC Docket No. 21-341 IS ADOPTED.

81. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

*14149 APPENDIX A

Proposed Rules
The Federal Communications Commission proposes to amend Parts 52 and 64 of Title 47 of the Code of Federal Regulations as follows:

PART 52 — NUMBERING

1. The authority citation for part 52 continues to read as follows:
Authority: 47 U.S.C. 151, 152, 153, 154, 155, 201-205, 207-209, 218, 225-227, 251-252, 271, 303, 332, unless otherwise noted.

2. Add § 52.37 to subpart C to read as follows:

§ 52.37 Number Portability Requirements for Wireless Providers
(a) A wireless provider, including a reseller of wireless service, may only require the data described in paragraphs (b) and (c) of this section to accomplish a simple wireless-to-wireless port order request from an end user customer's new wireless provider.

(b) *Required standard data fields*.

(1) Ported telephone number;

(2) Account number;

(3) Zip code;

(c) *Optional standard data field*. A Passcode field shall be optional unless the passcode has been requested and assigned by the end user, in which case it is required.

(d) *Notification required after port request*. A wireless provider, including a reseller of wireless service, shall notify an end user customer that a port request has been received for the customer's account before executing a simple wireless-to-wireless port request. A wireless provider shall provide this notification to the end-user customer via text message to the telephone number of record for the customer's account or via push notification.

(e) *Account freezes*. A wireless provider, including a reseller of wireless service, shall offer customers the option to lock their accounts to prohibit unauthorized port requests. If the customer chooses to lock the customer's account, the wireless provider shall not fulfill a simple wireless-to-wireless port order request until the customer deactivates the lock on the account.

PART 64 — MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

3. The authority citation for part 64 continues to read as follows:

Authority: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 262, 276, 403(b)(2)(B), (c), 616, 620, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091.

4. Revise § 64.2010 to read as follows:

§ 64.2010 Safeguards on the disclosure of customer proprietary network information.

***14150** (a) *Safeguarding CPNI*. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

(b) *Telephone access to CPNI*. Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (g) of this section, that is not prompted by the carrier asking for readily available biographical information or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) *Online access to CPNI*. A telecommunications carrier must authenticate a customer without the use of readily available biographical information, account information, recent payment information, or call detail information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (g) of this section, that is not prompted by the carrier asking for readily available biographical information, account information, recent payment information, or call detail information.

(d) *In-store access to CPNI*. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.

(e) *Subscriber Identity Module (SIM) changes*. Telecommunications carriers shall not effectuate a SIM change unless the

carrier uses a secure method of authenticating its customer. For purposes of this paragraph, the following shall be considered secure methods of authenticating a customer: (1) use of a pre-established password; (2) a one-time passcode sent via text message to the account phone number or a pre-registered backup number; (3) a one-time passcode sent via e-mail to the e-mail address associated with the account; or (4) a one-time passcode sent using a voice call to the account phone number or a pre-registered backup number. These methods shall not be considered exhaustive and an alternative customer authentication measure used by a carrier must be a secure method of authentication. For purposes of this section, SIM means a physical or virtual card contained with a device that stores unique information that can be identified to a specific mobile network.

(f) *Procedures for failed authentication for SIM changes*. Wireless carriers shall develop, maintain, and implement procedures for responding to multiple failed authentication attempts.

(g) *Establishment of a password and back-up authentication methods for lost or forgotten passwords*. To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, account information, recent payment information, or call detail information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, account information, recent payment information, or call detail information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

***14151** (h) *Notification of account changes*. Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information. Telecommunications carriers shall notify customers immediately of any requests for SIM changes through means that effectively alert customers in a timely manner.

(i) *Business customer exemption*. Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

***14152 APPENDIX B**

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[136] the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the Notice of Proposed Rulemaking (NPRM). Written comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the NPRM provided on the first page of the item. The Commission will send a copy of the NPRM, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[137] In addition, the NPRM and IRFA (or summaries thereof) will be published in the Federal Register.[138]

A. Need For, and Objectives of, the Proposed Rules

2. This item focuses developing protections to address SIM swapping and port-out fraud. In SIM swapping, the bad actor targets a consumer's subscriber identity module (SIM) and convinces the victim's wireless carrier to transfer the victim's service from the original device (and that device's SIM) to a cell phone in the bad actor's possession. A consumer's wireless phone number is associated with the SIM in that consumer's cell phone; by "swapping" the SIM associated with a phone number, the bad actor can take control of a consumer's cell phone account. In "port-out fraud," the bad actor, posing as the victim, opens an account with a carrier other than the victim's current carrier. The bad actor then arranges for the victim's phone number to be transferred to (or ""ported out") to the account with the new carrier controlled by the bad actor.

3. We have received numerous consumer complaints from people who have suffered significant distress, inconvenience, and

financial harm as a result of SIM swapping and port-out fraud. Today, we take aim at these scams, with the goal of foreclosing these opportunistic ways in which bad actors take over consumers' cell phone accounts. Section 222 of the Communications Act of 1934, as amended (the "Act"), and our Customer Proprietary Network Information (CPNI) rules, which govern the use, disclosure, and protection of sensitive customer information to which a telecommunications carrier has access, require carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to customers' private information. Our Local Number Portability (LNP) rules govern the porting of telephone numbers from one carrier to another. Yet, it appears that neither our CPNI rules nor our LNP rules are adequately protecting consumers against SIM swap and port-out fraud. We, therefore, propose to amend our CPNI and LNP rules to require carriers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or carrier. We also propose to require providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts, and we seek comment on other ways to protect consumers from SIM swapping and port-out fraud.

B. Legal Basis

4. The legal basis for any action that may be taken pursuant to this NPRM is contained in sections 1, 4(i), 4(j), 201, 222, 251, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154, 201, 222, 251, 303(r), 332.

***14153 C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply**

5. The RFA directs agencies to provide a description of, and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules and policies, if adopted.[139] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[140] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[141] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[142]

6. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[143] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[144] These types of small businesses represent 99.9 percent of all businesses in the United States, which translates to 30.7 million businesses.[145]

7. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[146] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[147] Nationwide, for tax year 2018, there were approximately 571,709 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[148]

***14154** 8. Finally, the small entity described as a "small governmental jurisdiction"" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[149] U.S. Census Bureau data from the 2017 Census of Governments[150] indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[151] Of this number there were 36,931 general purpose governments (county,[152] municipal and town or township[153]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[154] with enrollment populations of less than 50,000.[155]

1. Providers of Telecommunications and Other Services

9. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By

exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[156] The SBA has developed a small ***14155** business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[157] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.[158] Of this total, 3,083 operated with fewer than 1,000 employees.[159] Thus, under this size standard, the majority of firms in this industry can be considered small.

10. *Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers.[160] Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[161] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated for the entire year.[162] Of that total, 3,083 operated with fewer than 1,000 employees.[163] Thus under this category and the associated size standard, the Commission estimates that the majority of local exchange carriers are small entities.

11. *Incumbent Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers.[164] Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[165] U.S. Census Bureau data for 2012 indicate that 3,117 firms operated the entire year.[166] Of this total, 3,083 operated with fewer than 1,000 employees.[167] Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our actions. According to Commission data, one thousand three hundred and seven (1,307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers.[168] Of this total, an estimated 1,006 have 1,500 or ***14156** fewer employees.[169] Thus, using the SBA's size standard the majority of incumbent LECs can be considered small entities.

12. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. The closest applicable NAICS Code category is Wired Telecommunications Carriers.[170] The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[171] U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year.[172] Of that number, 3,083 operated with fewer than 1,000 employees.[173] According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.[174] Of this total, an estimated 317 have 1,500 or fewer employees.[175] Consequently, the Commission estimates that the majority of interexchange service providers are small entities.

13. *Competitive Local Exchange Carriers (Competitive LECs). Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate NAICS Code category is Wired Telecommunications Carriers[176] and under that size standard, such a business is small if it has 1,500 or fewer employees.[177] U.S. Census Bureau data for 2012 indicate that 3,117 firms operated during that year.[178] Of that number, 3,083 operated with fewer than 1,000 employees.[179] Based on these data, the Commission concludes that the majority of Competitive LECS, CAPs, Shared-Tenant Service Providers, and Other Local Service Providers, are small entities. According to Commission data, 1,442 carriers reported that they were engaged in the provision of either competitive local exchange services or competitive access provider services.[180] Of these 1,442 carriers, an ***14157** estimated 1,256 have 1,500 or fewer employees.[181] In addition, 17 carriers have reported that they are Shared-Tenant Service Providers, and all 17 are estimated to have 1,500 or fewer employees.[182] Also, 72 carriers have reported that they are Other Local Service Providers.[183] Of this total, 70 have 1,500 or fewer employees.[184] Consequently, based on internally researched FCC data, the Commission estimates that most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities.[185]

****28** 14. *Local Resellers*. The SBA has not developed a small business size standard specifically for Local Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[186] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[187] Under that size standard, such a business is small if it has 1,500 or fewer employees.[188] 2012

U.S. Census Bureau data show that 1,341 firms provided resale services during that year.[189] Of that number, 1,341 operated with fewer than 1,000 employees.[190] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[191] Of this total, an estimated 857 have 1,500 or fewer employees.[192] Consequently, the Commission estimates that the majority of local resellers are small entities.

***14158** 15. *Toll Resellers*. The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[193] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[194] Under that size standard, such a business is small if it has 1,500 or fewer employees.[195] 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year.[196] Of that number, 1,341 operated with fewer than 1,000 employees.[197] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[198] Of this total, an estimated 857 have 1,500 or fewer employees.[199] Consequently, the Commission estimates that the majority of toll resellers are small entities.

****29** 16. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[200] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[201] For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.[202] Of this total, 955 firms employed fewer than 1,000 employees and 12 firms employed of 1000 employees or more.[203] Thus under this category and the associated size standard, the Commission estimates that the majority of Wireless Telecommunications Carriers (except Satellite) are small entities.

***14159** 17. The Commission's own data—available in its Universal Licensing System—indicate that, as of August 31, 2018 there are 265 Cellular licensees that will be affected by our actions.[204] The Commission does not know how many of these licensees are small, as the Commission does not collect that information for these types of entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) Telephony services.[205] Of this total, an estimated 261 have 1,500 or fewer employees, and 152 have more than 1,500 employees.[206] Thus, using available data, we estimate that the majority of wireless firms can be considered small.

18. *Satellite Telecommunications*. This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[207] Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $35 million or less in average annual receipts, under SBA rules.[208] For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[209] Of this total, 299 firms had annual receipts of less than $25 million.[210] Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

19. *All Other Telecommunications*. The "All Other Telecommunications" category is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[211] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[212] Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[213] The SBA has developed a small business size standard for "All Other ***14160** Telecommunications," which consists of all such firms with annual receipts of $35 million or less.[214] For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year.[215] Of those firms, a total of 1,400 had annual receipts less than $25 million and 15 firms had annual receipts of $25 million to $49,999,999.[216] Thus, the Commission estimates that the majority of " All Other

Telecommunications" firms potentially affected by our action can be considered small.

2. Internet Service Providers

****30** 20. *Internet Service Providers (Broadband)*. Broadband Internet service providers include wired (e.g., cable, DSL) and VoIP service providers using their own operated wired telecommunications infrastructure fall in the category of Wired Telecommunication Carriers.[217] Wired Telecommunications Carriers are comprised of establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies.[218] The SBA size standard for this category classifies a business as small if it has 1,500 or fewer employees.[219] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.[220] Of this total, 3,083 operated with fewer than 1,000 employees.[221] Consequently, under this size standard the majority of firms in this industry can be considered small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

21. In this NPRM, we propose to prohibit wireless carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer. We also propose to amend our CPNI rules to require wireless carriers to develop procedures for responding to failed authentication attempts and to notify customers immediately of any requests for SIM changes. We also seek comment on whether we should impose customer service, training, and transparency requirements specifically focused on preventing SIM swap fraud. We likewise propose to amend our number porting rules to combat port-out fraud while continuing to encourage robust competition through efficient number porting. Specifically, the Commission also proposes to amend the LNP rules to require carriers to send customers a text message or push notification whenever a porting request is made; to require carriers to allow customers the option to freeze their accounts to prevent any unauthorized port-out requests; and to codify the data fields wireless carriers must use to validate a port request. Finally, we also seek comment ***14161** whether we should adopt any other changes to our rules to address SIM swap and port-out fraud, including the difficulties encountered by victims of these schemes.

22. Should the Commission decide to modify existing rules or adopt new rules to protect customers from SIM swap or porting-out fraud, such action could potentially result in increased, reduced, or otherwise modified recordkeeping, reporting, or other compliance requirements for affected providers of service. We seek comment on the effect of any proposals on small entities. Entities, especially small businesses, are encouraged to quantify the costs and benefits of any reporting, recordkeeping, or compliance requirement that may be established in this proceeding.

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

****31** 23. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[222]

24. In this NPRM, we seek comment whether the Commission should modify its CPNI or LNP rules to protect customers from SIM swap and port-out fraud, and, if so, whether our proposals would be effective to do so. In this NPRM, we seek comment on the impact that any proposed rules could have on smaller carriers. We also seek comment on the benefits and burdens, especially the burdens on small entities, of adopting any new or revised rules regarding the customer authentication and porting process. Specifically, we seek comment whether the proposed requirements would impose additional burdens on smaller carriers; whether smaller carriers would face different costs than larger carriers in implementing the new requirements, if adopted; whether smaller carriers would need more time to comply with any new or modified authentication or port-out rules; and whether smaller providers face other obstacles that we have not considered here. The Commission expects to consider the economic impact on small entities, as identified in comments filed in response to the NPRM, in reaching its final conclusions and taking action in this proceeding.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules
25. None.

***14162 STATEMENT OF ACTING CHAIRWOMAN JESSICA ROSENWORCEL**

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341 (September 30, 2021).
We download so much of our daily lives into our mobile devices. Those devices are in our palms, pockets, and purses—they're with us always. They provide us with connections a million times more powerful than what was available on Apollo 11. It's pretty incredible. It also makes them a terrific target for fraud.

One of the most dangerous scams is called SIM swapping fraud. SIM cards are small plastic chips, about the size of a dime, that are inserted into a mobile phone to identify and authenticate the subscriber.

SIM cards are increasingly at the center of scams involving our mobile devices. Here's how it works: A fraudster calls up your wireless provider and convinces the customer service representative that they are you and need your phone number switched to a new SIM card that they control. These cybercrooks do not need your phone to do this, they simply need to convince your carrier to make a change to your account. Once they do, they can use your phone number to divert your incoming messages and easily complete the kind of two-factor authentication checks that financial institutions and social media companies use. They also can be used to take over your e-mail and drain your bank accounts.

****32** By all accounts, including a big, recent Princeton University study, this type of fraud is growing. At the Federal Communications Commission, we've seen complaints from consumers who have suffered significant distress, inconvenience, and financial harm because of SIM swapping. To make matters worse, recent carrier data breaches that have made headlines may have exposed the very kind of customer information that could make it easier to pull off these kinds of attacks.

As Senator Ron Wyden has said, "Consumers are at the mercy of wireless carriers when it comes to being protected against SIM swaps." He's right. But we have tools at this agency we can use so consumers are better protected, and their devices are more secure. In fact, we have rules on the books designed to prevent your carrier from sharing personal and private information. These rules govern how carriers are supposed to protect what is known in the law as customer proprietary network information, or CPNI. But these rules need an update to address new types of fraud like SIM swapping.

That's what we start here today. We propose to update our CPNI and related local number portability rules to require carriers to securely authenticate a customer before transferring a phone number to a new device or carrier, and we seek comment on the best way to do that. We also propose that carriers immediately notify customers whenever a SIM change or port request has been made. These proposals will help protect consumers from both SIM swaps and a related kind of fraud known as "port-out fraud," where fraudsters pose as their victims and then arrange to transfer their victim's phone number to a new account that they control.

It's important we do this now. The Princeton University study I mentioned found that four out of five SIM swap attempts in the United States are successful. We can help fix this. I look forward to the record that develops and putting an end to this cyber fraud.

For their efforts to protect consumers and their privacy, thank you to Pam Arluk, Brian Cruikshank, Justin Faulb, Lisa Hone, Dan Kahn, Melissa Kirkel, Kris Monteith, and Christi Shewman of the Wireline Competition Bureau; Eduard Bartholme, Zac Champ, Aaron Garza, Eliot Greenwald, Kurt Schroeder, Mark Stone, Patrick Webre, and Kimberly Wild of the Consumer and Governmental Affairs Bureau; Ken Carlberg, Lisa Fowlkes, Jeffery Goldthorp, Debra Jordan, Lauren Kravetz, Nicole McGinnis, Zenji Nakazawa, Erika Olsen, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Michael Epshteyn, James Graves, Phillip Rosario, Kimbarly Taylor, Kristi Thompson, ***14163** and Shana Yates of the Enforcement Bureau; Mark Azic, Patrick Brogan, Eugene Kiselev, Eric Ralph, and Emily Talaga of the Office of Economics and Analytics; and Doug Klein, Rick Mallen, Linda Oliver, and Bill Richardson of the Office of General Counsel.

***14164 STATEMENT OF COMMISSIONER GEOFFREY STARKS**

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341 (September 30, 2021).

****33** You may not know exactly how SIM swapping works, but you have probably heard about its harmful results. In 2019, hackers used a SIM swap to take control of Twitter CEO Jack Dorsey's singular twitter handle, @jack. In just 20 minutes, the hackers sent out two dozen tweets and retweets to @jack's millions of followers, including many toxic messages.[223] For Mr. Dorsey and his followers, the security breach caused alarm and offense. For other victims, there have been even more devastating consequences, from drained bank balances to lost email accounts containing years of communication.

SIM swapping and port-out fraud, a related scam, occur when a bad actor successfully poses as the victim in a transaction with the victim's phone company. The scammer can then take control of the Customer Proprietary Network Information associated with the victim's account, leverage that control to access bank accounts and other private information, and impersonate the victim in other harmful ways. These attacks are especially insidious because they are difficult for individuals—even those with all the security resources a large tech company can provide its senior leaders—to prevent on their own.

Protecting consumers from these kinds of scams will require systemic changes. I am pleased to support this Notice of Proposed Rulemaking because it begins the process of modernizing our CPNI and Local Number Portability rules to require carriers to act. I thank my colleagues for agreeing to two changes that I believe will make this NPRM even better. First, we have asked commenters to address the possibility of "future proofing" our guidelines for authenticating user identities by incorporating the National Institute of Standards and Technology's Digital Identity Guidelines or another authoritative source. As authentication technology improves and adapts to new threats, we will want our rules to keep up. Second, we will seek comment on whether and how the Commission should audit compliance with any carrier obligations we decide to adopt. There's good reason to think consumer complaints alone may not reliably surface problems like improper authentication procedures. After all, a consumer who calls her wireless company and gets the assistance she hoped for could be forgiven for not noticing if the customer service representative skips steps in the authentication process. I look forward to robust comments on these issues and the many other important questions raised in the NPRM, and I thank staff of the Wireline Competition Bureau for their hard work on this item.

STATEMENT OF ACTING CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341 (September 30, 2021).

We download so much of our daily lives into our mobile devices. Those devices are in our palms, pockets, and purses—they're with us always. They provide us with connections a million times more powerful than what was available on Apollo 11. It's pretty incredible. It also makes them a terrific target for fraud.

****34** One of the most dangerous scams is called SIM swapping fraud. SIM cards are small plastic chips, about the size of a dime, that are inserted into a mobile phone to identify and authenticate the subscriber.

SIM cards are increasingly at the center of scams involving our mobile devices. Here's how it works: A fraudster calls up your wireless provider and convinces the customer service representative that they are you and need your phone number switched to a new SIM card that they control. These cybercrooks do not need your phone to do this, they simply need to convince your carrier to make a change to your account. Once they do, they can use your phone number to divert your incoming messages and easily complete the kind of two-factor authentication checks that financial institutions and social media companies use. They also can be used to take over your e-mail and drain your bank accounts.

By all accounts, including a big, recent Princeton University study, this type of fraud is growing. At the Federal Communications Commission, we've seen complaints from consumers who have suffered significant distress, inconvenience, and financial harm because of SIM swapping. To make matters worse, recent carrier data breaches that have made headlines may have exposed the very kind of customer information that could make it easier to pull off these kinds of attacks.

As Senator Ron Wyden has said, "Consumers are at the mercy of wireless carriers when it comes to being protected against SIM swaps." He's right. But we have tools at this agency we can use so consumers are better protected, and their devices are more secure. In fact, we have rules on the books designed to prevent your carrier from sharing personal and private

information. These rules govern how carriers are supposed to protect what is known in the law as customer proprietary network information, or CPNI. But these rules need an update to address new types of fraud like SIM swapping.

That's what we start here today. We propose to update our CPNI and related local number portability rules to require carriers to securely authenticate a customer before transferring a phone number to a new device or carrier, and we seek comment on the best way to do that. We also propose that carriers immediately notify customers whenever a SIM change or port request has been made. These proposals will help protect consumers from both SIM swaps and a related kind of fraud known as "port-out fraud," where fraudsters pose as their victims and then arrange to transfer their victim's phone number to a new account that they control.

It's important we do this now. The Princeton University study I mentioned found that four out of five SIM swap attempts in the United States are successful. We can help fix this. I look forward to the record that develops and putting an end to this cyber fraud.

For their efforts to protect consumers and their privacy, thank you to Pam Arluk, Brian Cruikshank, Justin Faulb, Lisa Hone, Dan Kahn, Melissa Kirkel, Kris Monteith, and Christi Shewman of the Wireline Competition Bureau; Eduard Bartholme, Zac Champ, Aaron Garza, Eliot Greenwald, Kurt Schroeder, Mark Stone, Patrick Webre, and Kimberly Wild of the Consumer and Governmental Affairs Bureau; Ken Carlberg, Lisa Fowlkes, Jeffery Goldthorp, Debra Jordan, Lauren Kravetz, Nicole McGinnis, Zenji Nakazawa, Erika Olsen, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Michael Epshteyn, James Graves, Phillip Rosario, Kimbarly Taylor, Kristi Thompson, and Shana Yates of the Enforcement Bureau; Mark Azic, Patrick Brogan, Eugene Kiselev, Eric Ralph, and Emily Talaga of the Office of Economics and Analytics; and Doug Klein, Rick Mallen, Linda Oliver, and Bill Richardson of the Office of General Counsel.

STATEMENT OF COMMISSIONER GEOFFREY STARKS

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341 (September 30, 2021).

****35** You may not know exactly how SIM swapping works, but you have probably heard about its harmful results. In 2019, hackers used a SIM swap to take control of Twitter CEO Jack Dorsey's singular twitter handle, @jack. In just 20 minutes, the hackers sent out two dozen tweets and retweets to @jack's millions of followers, including many toxic messages.[224] For Mr. Dorsey and his followers, the security breach caused alarm and offense. For other victims, there have been even more devastating consequences, from drained bank balances to lost email accounts containing years of communication.

SIM swapping and port-out fraud, a related scam, occur when a bad actor successfully poses as the victim in a transaction with the victim's phone company. The scammer can then take control of the Customer Proprietary Network Information associated with the victim's account, leverage that control to access bank accounts and other private information, and impersonate the victim in other harmful ways. These attacks are especially insidious because they are difficult for individuals—even those with all the security resources a large tech company can provide its senior leaders—to prevent on their own.

Protecting consumers from these kinds of scams will require systemic changes. I am pleased to support this Notice of Proposed Rulemaking because it begins the process of modernizing our CPNI and Local Number Portability rules to require carriers to act. I thank my colleagues for agreeing to two changes that I believe will make this NPRM even better. First, we have asked commenters to address the possibility of "future proofing" our guidelines for authenticating user identities by incorporating the National Institute of Standards and Technology's Digital Identity Guidelines or another authoritative source. As authentication technology improves and adapts to new threats, we will want our rules to keep up. Second, we will seek comment on whether and how the Commission should audit compliance with any carrier obligations we decide to adopt. There's good reason to think consumer complaints alone may not reliably surface problems like improper authentication procedures. After all, a consumer who calls her wireless company and gets the assistance she hoped for could be forgiven for not noticing if the customer service representative skips steps in the authentication process. I look forward to robust comments on these issues and the many other important questions raised in the NPRM, and I thank staff of the Wireline Competition Bureau for their hard work on this item.

Footnotes

1 Each mobile device has its own unique SIM. A SIM can be a physical card or a digital, virtual card embedded into the phone itself (eSIM card). FCC, eSIM Cards FAQ, https://www.fcc.gov/consumers/guides/esim-cards-faq. In either form, the SIM "contains unique information that identifies it to a specific mobile network" and "allows subscribers to use their mobile devices to receive calls, send SMS messages, or connect to mobile internet services." Russell Ware, *What is a SIM Card?*, Lifewire (updated May 21, 2021), https://www.lifewire.com/what-are-sim-cards-577532.

2 In this item, when we use the term "wireless carrier" or "wireless provider," we intend to encompass mobile wireless services.

3 *See, e.g.*, T-Mobile, *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats* (Aug. 19, 2021), https://www.tmobile.com/brand/data-breach-2021. Breaches of customer information can lead to further fraud through SIM swaps and port-out schemes. *See, e.g.*, WSJ Pro Cyber Newsletter, *Cyber Daily: Watch for Identity Theft, SIM Swapping in T-Mobile Hack, Security Researchers Warn* (Aug. 19, 2021), https://www.wsj.com/articles/cyber-daily-watch-for-identity-theft-sim-swapping-in-t-mobile-hack-security-researchers-warn-11629379373?mod=searchresults_pos3&page=1.

4 *See, e.g.*, U.S. Department of Justice, Office of the U.S. Attorneys, District of Maryland, *Two Men Facing Federal Indictment in Maryland for Scheme to Steal Digital Currency and Social Media Accounts Through Phishing and "Sim-Swapping,"* Oct. 28, 2020, https://www.justice.gov/usao-md/pr/two-men-facing-federal-indictment-maryland-scheme-steal-digital-currency-and-social-media (reporting that a federal grand jury indicted two individuals on federal charges in connection with their unauthorized takeovers of victims' wireless phone and other electronic accounts and to steal digital currency and valuable social media accounts); U.S. Department of Justice, Office of the U.S. Attorneys, Eastern District of Michigan, *Nine Individuals Connected to a Hacking Group Charged With Online Identity Theft and Other Related Charges*, May 9, 2019, https://www.justice.gov/usao-edmi/pr/nine-individuals-connected-hacking-group-charged-online-identity-theft-and-other (reporting the indictment of nine individuals alleged to have participated in thefts of victims' identities to steal cryptocurrency via "SIM Hijacking"); Lorenzo Franceschi-Bicchierai, *Hacker Who Stole $5 Million By SIM Swapping Gets 10 Years in Prison*, Motherboard, Feb. 1, 2019, https://www.vice.com/en/article/gyaqnb/hacker-joel-ortiz-sim-swapping-10-years-in-prison (reporting that a 20-year old student who stole more than $5 million in cryptocurrency by hijacking the phone numbers of around 40 victims pleaded guilty and accepted a plea deal of 10 years in prison, believed to be the first person convicted of a crime for SIM swapping); Gertrude Chavez-Dreyfuss, Reuters, *U.S. Investor Sues AT&T for $224 million over loss of cryptocurrency*, Aug. 15, 2018, https://www.reuters.com/article/us-cryptocurrency-at-t-lawsuit/u-s-investor-sues-att-for-224-million-over-loss-of-cryptocurrency-idUSKBN1L01AA.

5 *See* Krebs on Security, *Can We Stop Pretending SMS Is Secure Now?*, Mar. 16, 2021, https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/; Joseph Cox, *A Hacker Got All My Texts for $16*, Vice, Mar. 15, 2021, https://www.vice.com/amp/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber?__twitter_impression=true; *see also* Joseph Cox, *T-Mobile, Verizon, AT&T Stop SMS Hijacks After Motherboard Investigation*, Vice, Mar. 25, 2021, https://www.vice.com/en/article/5dp7ad/tmobile-verizon-att-sms-hijack-change (reporting that "[a]ll the mobile carriers have mitigated a major SMS security loophole that allowed a hacker to hijack text messages for just $16.") (Cox Mar. 25, 2021).

6 Federal Trade Commission, Consumer Sentinel Network Data Book 2020 (Feb. 2021), at Appx. B, p. 88, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf; *see* Letter from Ajit V. Pai, Chairman, FCC, to Sen. Ron Wyden, U.S. Senate at 3 (Feb. 14, 2020), https://docs.fcc.gov/public/attachments/DOC-362599A2.pdf (stating that the Commission received 218 informal consumer complaints discussing port-out fraud or SIM swapping in 2017, 211 informal consumer complaints in 2018, and 183 informal

consumer complaints in 2019).

7 *See* Kevin Lee, Ben Kaiser, Jonathan Mayer, Arvind Narayanan, Center for Information Technology Policy, Princeton University, *An Empirical Study of Wireless Carrier Authentication for SIM Swaps*, August 2020, at Appx., available at https://www.usenix.org/system/files/soups2020-lee.pdf.

8 Lee et al. at 1.

9 *Id.*

10 *Id.*

11 *Id.* at 2.

12 *Id.*

13 *Id.* at 2-3.

14 *Id.*

15 *Id.*

16 *Id.*

17 *Id.* at 3.

18 *Id.*

19 *Id.*

20 *Id.* at 1.

21 *Id.*

22 47 U.S.C. § 222. *See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket Nos. 96-115, et al., Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14419-20, paras. 12-14 (1999) (*CPNI Reconsideration Order*) (denying petitions for reconsideration and forbearance seeking different treatment for wireless providers under the Commission's CPNI rules, concluding that "there is nothing in the statute or its legislative history to indicate that Congress intended the CPNI requirements in section 222 should not apply to wireless carriers").

23 47 U.S.C. § 222(a).

24 47 U.S.C. § 222(b).

25 47 U.S.C. § 222(c)(1). Section 222(d) delineates certain exceptions to the general principle of confidentiality, including permitting a carrier to use, disclose, or permit access to CPNI obtained from its customers to protect telecommunications services users "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services. Subsequent to the adoption of section 222(c)(1), Congress added section 222(f). Section 222(f) provides that for purposes of section 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location information concerning the user of a commercial mobile service or (2) automatic crash notification information of any person other than for use in the operation of an automatic crash notification system. 47 U.S.C. § 222(f).

26 47 U.S.C. § 222(h)(1).

27 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, 22 FCC Rcd 6927, 6930, para. 5 (2007) (*2007 CPNI Order*); *see also AT&T, Inc.*, File No.: EB-TCD-18-00027704, Notice of Apparently Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1757, paras. 33-35 (2020) (finding that customer location information is CPNI under the Act).

28 *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket Nos. 96-115, et al., Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) (*CPNI Order*).

29 *See id.* at 8195, para. 193.

30 *See* 47 CFR § 64.2009(b); *see also CPNI Order*, 13 FCC Rcd at 8198, para. 198.

31 47 CFR § 64.2009(e); *see also CPNI Order*, 13 FCC Rcd at 8198-200, paras. 199-202; *CPNI Reconsideration Order*, 14 FCC Rcd at 14468 n.331 (clarifying that carriers must "make these certifications available for public inspection, copying and/or printing at any time during regular business hours at a centrally located business office of the carrier").

32 *2007 CPNI Order*, 22 FCC Rcd at 6928 n.1.

33 *Id.* at 6934, para. 12.

34 *Id.*

35 The Commission defined "call detail" information to include "any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call." *2007 CPNI Order*, 22 FCC Rcd at 6936 n.45.

36 *See generally 2007 CPNI Order*, 22 FCC Rcd at 6933-46, paras. 12-36; 47 CFR § 64.2010(b)-(e).

37 *See 2007 CPNI Order*, 22 FCC Rcd at 6945-46, paras. 33-36; 47 CFR § 64.2010(a).

38 *See 2007 CPNI Order*, 22 FCC Rcd at 6942, para. 24; 47 CFR § 64.2010(f).

39 47 CFR § 64.2010(f).

40 *2007 CPNI Order*, 22 FCC Rcd at 6943-45, paras. 26-32.

41 *See id.* at 6929, para. 3. In addition, the Commission required affirmative customer consent ("opt-in consent") before a carrier could disclose a customer's CPNI to a carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer. *See id.* at 6947-53, paras. 37-50.

42 *2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59.

43 Telephone Records and Privacy Protection Act of 2006, Pub. L. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039).

44 47 U.S.C. § 251(b)(2).

45 47 U.S.C. § 153(30); 47 CFR § 52.21(m). The Commission has interpreted this language to mean that consumers must be able to change providers while keeping their telephone number as easily as they may change providers without taking their telephone

number with them. *See Telephone Number Portability; Carrier Requests for Clarification of Wireless-Wireless Porting Issues*, Memorandum Opinion and Order, 18 FCC Rcd 20971, 20975, para. 11 (2003) (*Wireless Number Portability Order*), *aff'd, Central Tex. Tel. Coop., Inc. v. FCC*, 402 F.3d 205 (D.C. Cir. 2005).

46 47 U.S.C. § 251(e)(1).

47 *See Telephone Number Portability*, First Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 8352, 8431, para. 153 (1996) (*First Number Portability Order*); *Telephone Number Portability*, First Memorandum Opinion and Order on Reconsideration, 12 FCC Rcd 7236, 7315-17, paras. 140-42 (1997) (*First Number Portability Order on Reconsideration*) (affirming the Commission's decision to impose number portability obligations on CMRS providers). The Commission has defined commercial mobile radio service as a mobile service that is "(1) provided for profit, *i.e.*, with the intent of receiving compensation or monetary gain; (2) An interconnected service; and (3) Available to the public, or to such classes of eligible users as to be effectively available to a substantial portion of the public," or the "functional equivalent of such a mobile service." 47 CFR § 20.3.

48 *See First Number Portability Order*, 11 FCC Rcd at 8393, paras. 77-78; *see also Cellular Telecommunications Industry Association's Petition for Forbearance from Commercial Mobile Radio Services Number Portability Obligations and Telephone Number Portability*, CC Docket No. 95-116 et al., Memorandum Opinion and Order, 14 FCC Rcd 3092 (1999) (extending implementation deadline for CMRS providers).

49 *See Wireless Number Portability Order*, 18 FCC Rcd 20971.

50 *See id.* at 20978, para. 24.

51 *Id.* at 20979-80, para. 26.

52 *See Telephone Number Requirements for IP-Enabled Services Providers; Local Number Portability Porting Interval and Validation Requirements; IP-Enabled Services; Telephone Number Portability; Numbering Resource Optimization*, Report and Order, Declaratory Ruling, Order on Remand, and Notice of Proposed Rulemaking, 22 FCC Rcd 19531, 19553, para. 42 (2007) (*2007 VoIP LNP Order* or *2007 LNP Four Fields Declaratory Ruling*), *aff'd sub nom. National Telecomms. Cooperative Ass'n v. FCC* (D.C. Cir. Apr. 28, 2009).

53 *Id.* at 19556-57, para. 47.

54 A simple port is a port that (1) does not involve unbundled network elements; (2) involves an account only for a single line; (3) does not include complex switch translations (e.g., Centrex, ISDN, AIN services, remote call forwarding, or multiple services on the loop); and (4) does not include a reseller. *See, e.g., 2007 VoIP LNP Order*, 22 FCC Rcd at 19556, n.153.

55 *2007 VoIP LNP Order*, 22 FCC Rcd at 19557, para. 48.

56 *Id.* at 19557-58, para. 49 ("We are persuaded that the approach we adopt here reasonably balances consumer concerns about slamming with competitors' interest in ensuring that LNP may not be used in an anticompetitive manner to inhibit consumer choice.").

57 *See generally Local Number Portability Porting Interval and Validation Requirements; Telephone Number Portability*, WC Docket No. 07-244, CC Docket No. 95-116, Report and Order and Further Notice of Proposed Rulemaking, 24 FCC Rcd 6084 (2009) (*Porting Interval Order and FNPRM*).

58 *See id.* at 6087, para. 6.

59 *See Local Number Portability Porting Interval and Validation Requirements; Telephone Number Portability*, Report and Order, 25 FCC Rcd 6953, 69659-62, paras. 9-17 (2010) (*LNP Standard Fields Order*). The Commission also codified its long-standing requirement that non-simple ports must be completed within four business days. *See* 47 CFR § 52.35(d).

60 *See LNP Standard Fields Order*, 25 FCC Rcd 6953, 6959-62, paras. 9-17. The Commission required that service providers use the following 14 fields to accomplish a wireline or intermodal simple port: (1) "Ported Telephone Number"—the customer's telephone number; (2) "Account Number"—the customer's account number with the current service provider; (3) "Zip Code"— the zip code for the customer's address associated with the account; (4) ""Company Code"—the operating company number, or OCN, of the new service provider; (5) "New Network Service Provider"—the name of the new service provider; (6) "Desired Due Date"—the date by which the customer wants the port completed; (7) "Purchase Order Number"— the customer's unique purchase order or requisition number that authorizes issuance of the port request; (8) ""Version"— the version number of the order submitted by the new service provider; (9) "Number Portability Direction Indicator"— information to let the new service provider direct the correct administration of E-911 records; (10) ""Customer Carrier Name Abbreviation"— the three-letter code for the name of the new service provider; (11) "Requisition Type and Status"— the type of order to be processed, such as number portability, loop with number portability, retail/bundled, resale, directory listings, etc.; (12) ""Activity"— the activity involved in the service request, such as porting, new account installation, disconnection, suspension, restoration, etc.; (13) ""Telephone Number (Initiator)"— the telephone number for the new service provider initiating the port request; and (14) "Agency Authority Status"— which indicates that the new service provider initiating the port request has an authorization to initiate a port on file. *Id.* We note that when requesting a port, some of the information described above is supplied by the customer to the new or gaining carrier and some of the information is provided by the new carrier to the current carrier.

61 *See* 47 CFR § 52.36(c).

62 *See generally LNP Standard Fields Order*, 25 FCC Rcd at 6956-62, paras. 6-10.

63 NPAC, Number Portability Best Practices, https://numberportability.com/industry-info/lnpa-working-group/lnp-best-practices/?page=1 (last visited Aug. 20, 2021).

64 Best Practice 73 addresses three types of unauthorized ports: disputed ports (usually a result of two or more parties each claiming to be the authorized end user, including business partner disputes, personal relationship disputes, dissolution of franchises); inadvertent ports (which occur as a result of an error, including incorrect number provided by End User and typographical errors in local service requests); and fraudulent ports (which occur as a result of an intentional act of fraud, theft and/or misrepresentation). *See* Best Practice 73, NPAC, *Number Portability Best Practices*, https://numberportability.com/industry-info/lnpa-working-group/lnp-best-practices/?page=1 (last visited Aug. 20, 2021).

65 *See* Best Practice 73, NPAC, *Number Portability Best Practices*, https://numberportability.com/industry-info/lnpa-working-group/lnp-best-practices/?page=1 (last visited Aug. 20, 2021).

66 At the same time, we emphasize that carriers have statutory duties to protect the confidentiality of their customers' private information and to maintain just and reasonable practices and that these statutory duties are not necessarily coterminous with our rules. *See* 47 U.S.C. §§ 222(a), 201(b); *TerraCom, Inc., and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014). Recent breaches appear to demonstrate that current safeguards are not sufficient to protect consumers' data.

67 As used in our proposed rules, the term "carrier" includes "any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment." *See* 47 U.S.C. § 217.

68 As used here, a "pre-established password" is a password chosen by the customer for future use to authenticate a customer for access to account information or to make account changes.

69 *See generally* Lee et al.

70 *See* Lee et al. at 1, 9.

71 *See* Lucky225, *It's time to stop using SMS for anything*, Mar. 15, 2021, https://lucky225.medium.com/its-time-to-stop-using-sms-for-anything-203c41361c80; Joseph Cox, *A Hacker Got All My Texts for $16*, Vice, Mar. 15, 2021, https://www.vice.com/amp/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber; Krebs on Security, *Can We Stop Pretending SMS Is Secure Now?*, Mar. 16, 2021, https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/.

72 *See* Cox Mar. 25, 2021 at 1 (reporting that "[a]ll the mobile carriers have mitigated a major SMS security loophole that allowed a hacker to hijack text messages for just $16").

73 *2007 CPNI Order*, 22 FCC Rcd at 6945, para. 33.

74 *Id.*

75 National Institute of Standards and Technology, Department of Commerce, NIST Special Publication 800-63B, Digital Identity Guidelines — Authentication and Lifecyle Management, at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf.

76 *Id.*

77 47 CFR § 64.2010(c).

78 *See* Lee et al. at 2-3.

79 *See* 47 CFR § 64.2010(d).

80 *See* 47 CFR § 64.2010(e).

81 *See* 47 CFR § 64.2010(b), (c).

82 *See* 47 CFR § 64.2010(e).

83 47 CFR § 64.2010(f).

84 *Id.*

85 *2007 CPNI Order*, 22 FCC Rcd at 6942, para. 24.

86 A push notification is "a message sent to a smartphone relating to one of its apps, even when it is not running, or the act of sending such messages." Cambridge Dictionary (visited Aug. 20, 2021), available at https://dictionary.cambridge.org/us/dictionary/english/push-notification.

87 *Cf., e.g.*, 47 CFR § 64.1190 (governing preferred carrier freezes).

88 *See also infra* Part III.C.

89 47 CFR § 64.2010(a) ("Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.").

90 47 U.S.C. § 222(a) (imposing a general duty on carriers to "protect the confidentiality of proprietary information of, and relating to

... customers").

91 *2007 CPNI Order*, 22 FCC Rcd at 6946, para. 35.

92 The frequency of customer data breaches since 2007 appears to indicate that current safeguards are not sufficient to protect consumers' data. *See, e.g., AT&T Services, Inc.*, Order, 30 FCC Rcd 2808 (EB 2015) (reaching $25 million settlement of investigation into three breaches); T-Mobile, *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats* (Aug. 19, 2021), https://www.t-mobile.com/brand/data-breach-2021 (providing notice of an August 2021 breach that exposed names, dates of birth, and social security numbers for more than 50 million current, former, and prospective customers); Selena Larson, *Verizon data of 6 million users leaked online*, CNN Business (July 12, 2017), https://money.cnn.com/2017/07/12/technology/verizon-data-leaked-online/index.html.

93 *See* 47 CFR § 64.2011 (requiring telecommunications carriers to notify law enforcement when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI).

94 *See* 5G Americas, *The Future of Voice in Mobile Wireless Communications* at 25, Feb. 2021, www.5gamericas.org/wp-content/uploads/2021/02/InDesign-Future-of-Voice-Feb-2021-1.pdf.

95 47 CFR § 9.3.

96 *See, e.g.*, T-Mobile, *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats* (Aug. 19, 2021), https://www.t-mobile.com/brand/data-breach-2021 (providing notice that personal information was stolen from T-Mobile systems).

97 *See 2007 CPNI Order*, 22 FCC Rcd at 6930, para. 4; *id.* at 6955-58, paras. 54-59 (relying on "our Title I ancillary jurisdiction" to the extent necessary to apply CPNI rules to interconnected VoIP). We note that, in 2008, Congress ratified the Commission's decision to apply section 222's requirements to interconnected VoIP by adding language to section 222 that expressly covers "IP-enabled voice service," defined by reference to the Commission's definition of "interconnected VoIP service." *See* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283 (2008); 47 U.S.C. § 222(d)(4), (f)(1), (g) (applying provisions of section 222 to "IP-enabled voice service"); *id.* § 615b(8) (defining "IP-enabled voice service" as having "the meaning given the term 'interconnected VoIP service' by section 9.3 of the Federal Communications Commission's regulations (47 CFR 9.3)").

98 *See, e.g.*, 47 U.S.C. § 1004 ("A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.").

99 We note that though the Act makes it unlawful for any telecommunications carrier to "submit or execute a change in a subscriber's selection of a provider of telephone exchange service ... except in accordance with such verification procedures as the Commission shall prescribe," the Commission's slamming rules implementing this provision do not currently apply to wireless carriers. As a result, wireless subscribers are not afforded the same protections as wireline customers when their service is switched to another carrier without their authorization. *See* 47 U.S.C. § 258(a); 47 CFR § 64.1120(a)(3) (excluding CMRS providers from the

verification requirements of the slamming rules).

100 *LNP Standard Fields Order*, 25 FCC Rcd at 6962, para. 16.

101 *2007 LNP Four Fields Declaratory Ruling*, 22 FCC Rcd at 19532, para. 1.

102 Verizon, *Transfer (port-out) your number to another carrier FAQs*, https://www.verizon.com/support/port-out-faqs/ (last visited Aug. 20, 2021).

103 *Id.*

104 AT&T, *Prevent Porting to Protect Your Identity*, https://about.att.com/pages/cyberaware/ni/blog/porting (last visited Aug. 20, 2021).

105 *See, e.g.*, 47 U.S.C. § 227(e)(8)(C) (defining "text message" in the Truth in Caller ID context); 47 CFR § 9.10(q)(9), (10)(iv) (defining ""911 text message" and setting forth certain exclusions).

106 *See supra* para. 24.

107 CTIA, *Protecting Your Wireless Account Against SIM Swap Fraud*, https://www.ctia.org/protecting-against-sim-swap-fraud (last visited Aug. 20, 2021).

108 Verizon, *Transfer (port-out) your number to another carrier FAQs*, https://www.verizon.com/support/port-out-faqs/ (last visited Aug. 20, 2021).

109 *Id.*

110 AT&T, *Prevent Porting to Protect Your Identity*, https://about.att.com/pages/cyber-aware/news-information/blog/prevent_porting.html (last visited Aug. 23, 2021).

111 AT&T, *Transfer Your Wireless Number to Another Provider*, https://www.att.com/support/article/wireless/KM1447526/ (last visited Sept. 23, 2021).

112 T-Mobile, *How T-Mobile Helps Customers Fight Account Takeover Fraud* (Oct. 29, 2019),

https://www.t-mobile.com/news/press/how-to-fight-account-takeover-fraud.

113 AT&T, *Learn about ZenKey*, https://www.att.com/support/article/wireless/KM1375558/ (last visited Aug. 23, 2021).

114 AT&T, *Mobile Authentication Taskforce to Unveil ZenKey at MWC Los Angeles*, https://about.att.com/story/2019/mobile_authentication_taskforce_zenkey.html (last visited Aug. 23, 2021).

115 *See* North American Numbering Council Local Number Portability Administration Working Group Report on Wireless Wireline Integration, May 8, 1998, CC Docket No. 95-116 (filed May 18, 1998); North American Numbering Council Wireless Number Portability Subcommittee Report on Wireless Number Portability Technical, Operational, and Implementation Requirements Phase II, CC Docket No. 95-116 (filed Sept. 26, 2000); ATIS Operations and Billing Forum, Wireless Intercarrier Communications: Interface Specification for Local Number Portability, Version 2, at 6, para. 2 (Jan. 2003).

116 *See* 47 CFR § 64.1190(a).

117 Verizon, *Transfer (port-out) your number to another carrier FAQs*, https://www.verizon.com/support/port-out-faqs/ (last visited Aug. 23, 2021).

118 *See* 47 CFR § 64.1190(d).

119 *See Protecting Consumers from Unauthorized Carrier Changes and Related Unauthorized Charges*, CG Docket No. 17-169, Report and Order, 33 FCC Rcd 5773, 5784, para. 31 (2018). The Commission declined to adopt a default preferred carrier freeze requirement, finding that default freezes could potentially inhibit consumer switching and competition and the ability of carriers to quickly port customers. *Id.*

120 *See* 47 CFR § 52.36(b)(1)-(3).

121 *LNP Standard Fields Order*, 25 FCC Rcd at 6958, para. 8.

122 *See* NPAC, *About NPAC*, https://numberportability.com/about-us/about-npac/ (last visited Aug. 20, 2021).

123 NPAC, *How LNP Works*, https://numberportability.com/about-us/how-lnp-works/ (last visited Aug. 20, 2021).

124 NPAC, *Number Portability Best Practices*, https://numberportability.com/industry-info/lnpa-working-group/lnp-best-practices/?page=1 (last visited Aug. 20, 2021).

125 NPAC, *Number Portability Best Practices*, https://numberportability.com/industry-info/lnpa-working-group/lnp-best-practices/?page=1 (last visited Aug. 20, 2021).

126 *See generally First Number Portability Order*, 12 FCC Rcd at 7232, 7242, 7273, paras. 2, 11, 61; *Porting Interval Order and FNPRM*, 24 FCC Rcd at 6084, para. 1; *LNP Standard Fields Order*, 25 FCC Rcd at 6954-55, paras. 2-3.

127 *See, e.g., Implementation of the National Suicide Hotline Improvement Act of 2018*, Report and Order, 35 FCC Rcd 7373, 7394, para. 40 (2020) (relying on section 251(e) to apply requirements to interconnected and one-way VoIP).

128 *Cf., e.g.*, 47 CFR § 64.2113 (requiring covered providers to make contact information for the receipt and handling of rural call completion issues available on their websites, and requiring that the contact information must be easy to find and use).

129 *See* Andy Greenberg, Wired, *The SIM Swap Fix That the US Isn't Using*, Apr. 26, 2019, https://www.wired.com/story/sim-swap-fix-carriers-banks/.

130 Section 1 of the Communications Act of 1934 as amended provides that the FCC "regulat[es] interstate and foreign commerce in communication by wire and radio so as to make [such service] available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex." 47 U.S.C. § 151.

131 The term "equity" is used here consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. *See* Exec. Order No. 13985, 86 Fed. Reg. 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (January 20, 2021).

132 47 CFR §§ 1.1200 *et seq*.

133 *See* 5 U.S.C. § 603.

134 *See* 5 U.S.C. § 603(a).

135 *See* 44 U.S.C. § 3506(c)(4).

136 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

137 *See* 5 U.S.C. § 603(a).

138 *See id.*

139 5 U.S.C. § 603(b)(3).

140 5 U.S.C. § 601(6).

141 5 U.S.C. § 601(3) (incorporating by reference the definition of ""small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

142 15 U.S.C. § 632.

143 *See* 5 U.S.C. § 601(3)-(6).

144 *See* U.S. Small Business Administration, Office of Advocacy, *What's New With Small Business?* (Sept. 2019), https://cdn.advocacy.sba.gov/wp-content/uploads/2019/09/23172859/Whats-New-With-Small-Business-2019.pdf.

145 *Id.*

146 5 U.S.C. § 601(4).

147 The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. See IRS, *Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), Who May File Form 990-N to Satisfy Their Annual Reporting Requirement*, https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard (last visited Aug. 2, 2021). We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

148 *See* Exempt Organizations Business Master File Extract (EO BMF), ""CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for Region 1-Northeast Area (76,886),

Region 2-Mid-Atlantic and Great Lakes Areas (221,121), and Region 3-Gulf Coast and Pacific Coast Areas (273,702) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

149 5 U.S.C. § 601(5).

150 *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and ""7." *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

151 *See* U.S. Census Bureau, 2017 Census of Governments — Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* Table 2. CG1700ORG02 Table Notes_ Local Governments by Type and State_2017.

152 *See id.* at Table 5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

153 *See id.* at Table 6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

154 *See id.* at Table 10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* Table 4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

155 This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations Tables 5, 6, and 10.

156 *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

157 *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

158 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

159 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

160 *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

161 *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

162 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

163 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

164 *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

165 *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

166 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

167 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

168 *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

169 *Id.*

170 *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

171 *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

172 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

173 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

174 *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010), https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf (*Trends in Telephone Service*).

175 *Id.*

176 *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

177 *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

178 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

179 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

180 *See* Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division, Trends in Telephone Service at Table 5.3 (Sept. 2010), https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf (*Trends in Telephone Service*).

181 *Id.*

182 *Id.*

183 *Id.*

184 *Id.*

185 We have included small incumbent LECs in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small business size standard (e.g., a telephone communications business having 1,500 or fewer employees), and "is not dominant in its field of operation." The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent LECs are not dominant in their field of operation because any such dominance is not "national" in scope. We have therefore included small incumbent LECs in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

186 *See* U.S. Census Bureau, *2017 NAICS Definition, "517911 Telecommunications Resellers,"* https://www.census.gov/naics/?input=517911&year=2017&details=517911.

187 *See* 13 CFR § 121.201, NAICS Code 517911.

188 *Id.*

189 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517911, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

190 *Id.* Available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA's size standard.

191 *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

192 *See id.*

193 *See* U.S. Census Bureau, *2017 NAICS Definition, "517911 Telecommunications Resellers,"* https://www.census.gov/naics/?input=517911&year=2017&details=517911.

194 *See* 13 CFR § 121.201, NAICS Code 517911.

195 *Id.*

196 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517911, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

197 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

198 *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

199 *See id.*

200 *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517312&search=2017NAICSSearch.

201 *See* 13 CFR § 121.201, NAICS Code 517312 (previously 517210).

202 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517210, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517210&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false&vintage=2012.

203 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

204 *See* http://wireless.fcc.gov/uls. For the purposes of this IRFA, consistent with Commission practice for wireless services, the Commission estimates the number of licensees based on the number of unique FCC Registration Numbers.

205 *See* Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division, Trends in Telephone Service at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*), https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf.

206 *See id.*

207 *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517410&search=2017+NAICS+Search&search=2017.

208 *See* 13 CFR § 121.201, NAICS Code 517410.

209 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517410, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517410&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false&vintage=2012.

210 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $35 million or less.

211 *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications*", https://www.census.gov/naics/?input=517919&year=2017&details=517919.

212 *Id.*

213 *Id.*

214 *See* 13 CFR § 121.201, NAICS Code 517919.

215 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517919, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517919&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

216 *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

217 *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/naics/?input=517311&year=2017&details=517311.

218 *Id.*

219 *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

220 *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

221 *Id.* The largest category provided by the census data is "1000 employees or more" and a more precise estimate for firms with fewer than 1,500 employees is not provided.

222 *See* 5 U.S.C. § 603(c).

223 Brian Barrett, *How Twitter CEO Jack Dorsey's Account Was Hacked* (Aug. 30, 2019), https://www.wired.com/story/jack-dorsey-twitter-hacked/.

224 Brian Barrett, *How Twitter CEO Jack Dorsey's Account Was Hacked* (Aug. 30, 2019), https://www.wired.com/story/jack-dorsey-twitter-hacked/.

36 FCC Rcd. 14120 (F.C.C.), 36 F.C.C.R. 14120, 2021 WL 4735472

2022 WL 1240864
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

Daniel FRASER, Plaintiff,

v.

MINT MOBILE, LLC, Defendant.

No. C 22-00138 WHA
|
Signed 04/27/2022

Attorneys and Law Firms

David Chad Silver, Pro Hac Vice, Silver Miller, Coral Springs, FL, Mathieu Harris Putterman, Putterman Law, APC, Newport Beach, CA, for Plaintiff.

Michael Benjamin Sachs, Clark Hill LLP, San Francisco, CA, Ernest F. Koschineg, Pro Hac Vice, Jessica M. Heinz, Pro Hac Vice, Jill H. Fertel, Pro Hac Vice, Ethan Feldman, Pro Hac Vice, Cipriani & Werner, P.C., Blue Bell, PA, for Defendant.

ORDER RE MOTION TO DISMISS

WILLIAM ALSUP, United States District Judge

INTRODUCTION

***1** Hackers took cell phone users' information from their carrier and this information was used to port plaintiff's cellular service to another carrier whereupon a criminal pretending to be plaintiff acquired access to and then drained plaintiff's cryptocurrency account maintained by a cryptocurrency exchange. The issue is the extent to which the carrier is liable for the lost funds once held by the cryptocurrency exchange. For the following reasons, the motion to dismiss is **Granted in Part** and **Denied in Part.**

STATEMENT

Defendant Mint Mobile, LLC is a mobile virtual network operator that currently uses T-Mobile's network infrastructure to provide wireless cellular services to its customers. One of those customers was plaintiff Daniel Fraser. This action involves three incidents that eventually led to the theft of Fraser's cryptocurrency, held by a non-party cryptocurrency exchange.

First, between June 8, 2021, and June 10, 2021, Mint (the mobile carrier) suffered a large-scale data breach. The leak exposed the personal identifying information (PII) of many of its cellphone customers, including their names, addresses, email addresses, phone numbers, account numbers, and passwords. Fraser was one of the customers affected by the breach (Compl. ¶¶ 3, 12).

Second, criminals purportedly used the information exposed in the data breach to hijack Fraser's cellphone service. SIM hijacking represents a growing crime in telecommunications. A subscriber identity module, or "SIM" card, authenticates a cellphone subscription. Switch the SIM card from an old phone into a new phone and the cellular service shifts to the new device.

Relevant here, SIM porting, or port-out fraud, is a genus of SIM hijacking where a criminal, posing as the victim, opens an account with a carrier different from that of the hacked carrier and arranges for the victim's cellular service to be transferred to the new carrier and put under control of the criminal. On June 11, 2021, an unknown criminal ported Fraser's cellular service with Mint to another service provider, Metro by T-Mobile. Fraser alleges that the earlier Mint data breach exposed all the information needed to port out his service. Additionally, Fraser alleges that, three days before his service was fraudulently ported to the other provider, he had implemented a PIN verification feature on his Mint account to enhance his electronic security with two-factor authentication, *i.e.*, making changes to his account required both a password and a pin verification code. Fraser alleges that Mint bypassed this enhanced security when it allowed the porting out of his account. All of this occurred before Mint notified affected customers of the breach on July 9, 2021 (Compl. ¶¶ 2–6, 37–43, 59–66).

Third, Fraser's cryptocurrency account (with a completely separate firm) was then hacked and his assets stolen. Besides the loss of one's cell service, port-out fraud places the victim's other personal accounts at risk as well. Personal accounts — *e.g.*, for email, banking, or cryptocurrency — will often use the account holder's telephone number as a means for the account holder to recover access to their account when, for example, they forget their password. In many instances, all the account holder needs to do to regain access to their account is verify their identity by entering a pin number automatically

sent to their phone via their cellular service (like the pin verification Fraser put on his Mint account). This means once a criminal successfully ports a victim's cellphone service, the criminal acquires a key to steal the victim's identity and access a variety of the victim's accounts (so long as the criminal has other, basic information regarding the victim's accounts, such as the email address used to maintain the account) (Compl. ¶¶ 1, 49, 59 62–67).

***2** Fraser had an account with Ledger, a specific cryptocurrency exchange, where he stored his cryptocurrency. He alleges that the combination of Mint's data breach (which occurred from June 8 through June 10) and the fraudulent SIM port (which occurred on June 11 at 8:08 a.m.) provided criminals with all the information and access required to hack into and drain his Ledger account (Compl. ¶ 63). As a result, starting on June 11 at 9:19 a.m., a criminal began to drain Fraser's Ledger account, and eventually stole the equivalent of $466,000.00 in cryptocurrency (Compl. ¶¶ 59–67).

Fraser filed this lawsuit to hold Mint responsible for its purported role in the theft of his cryptocurrency. Fraser broadly asserts claims for violation of the Federal Communications Act, violations of California Business & Professions Code Section 17200, negligence, and breach of contract. He does not assert his claims on behalf of a putative class. Now, Mint moves to dismiss the complaint for failure to state a claim. At the hearing, Mint withdrew its motion to dismiss the prayer for injunctive relief pursuant to the Federal Communications Act as well as its motion to compel arbitration. This order follows full briefing and oral argument.

ANALYSIS

A motion to dismiss tests the legal sufficiency of the complaint. To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain sufficient factual matter, accepted as true, to state a claim for relief that is plausible on its face. A claim is facially plausible when there are sufficient factual allegations to draw a reasonable inference that the defendant is liable for the misconduct alleged. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). While a court must take all of the factual allegations in the complaint as true, it is "not bound to accept as true a legal conclusion couched as a factual allegation." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "Factual allegations must be enough to raise a right to relief above the speculative level." *Ibid.*

1. Proximate Cause (All Counts).

Mint argues that the complaint fails to adequately allege the data breach and SIM port proximately caused the theft of Fraser's cryptocurrency from a third-party, and that the complaint should be dismissed in its entirety (Br. 6). This order disagrees.

"It is a well established principle of the common law that in all cases of loss, we are to attribute it to the proximate cause, and not to any remote cause." *Bank of Am. Corp. v. City of Miami*, 137 S. Ct. 1296, 1305 (2017) (cleaned up). Generally, the proximate cause requirement "bars suits for alleged harm that is 'too remote' from the defendant's unlawful conduct." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 133 (2014). Under California law, proximate cause has two aspects. The *first* is cause in fact, sometimes referred to as but-for causation. Under the substantial factor test, which generally subsumes but-for causation, a cause in fact is an act or omission that was a substantial factor in bringing about the plaintiff's harm. The *second* aspect of proximate cause incorporates considerations of public policy. "These additional limitations are related not only to the degree of connection between the conduct and the injury, but also with public policy." *State Dep't of State Hosps. v. Super. Ct.*, 61 Cal. 4th 339, 352–53 (2015) (quotation omitted); *Frausto v. Dep't of Cal. Highway Patrol*, 53 Cal. App. 5th 973, 996 (2020). "Ordinarily, proximate cause is a question of fact which cannot be decided as a matter of law from the allegations of a complaint. Nevertheless, where the facts are such that the only reasonable conclusion is an absence of causation, the question is one of law, not of fact." *State Hosps.*, 61 Cal. 4th at 353 (cleaned up).

***3** *First*, Mint argues that "holes in [p]laintiff's conclusory chain of causation overcome proximate causation" (Br. 8). The complaint, however, adequately explains how the combination of Mint's data breach and the SIM port-out gave criminals the information and access needed to drain Fraser's Ledger account. The data breach exposed, among other information, Fraser's name, address, telephone number, email address, and Mint password. Moreover, the data breach did not merely expose some of Fraser's PII, it purportedly revealed the specific PII necessary for a criminal to port out Fraser's wireless service to an account under the criminal's control (Compl. ¶¶ 61–63).

Mint argues the complaint does not adequately connect the dots between its conduct and the theft of Fraser's cryptocurrency from his Ledger account. Fraser alleges,

however, that once a criminal gains access to a victim's email, it is a straight-forward inquiry to determine what sort of financial accounts the victim maintains. A simple query of the victim's email account would reveal any number of accounts a criminal could then try to access (*id.* ¶¶ 59–67). That logical progression suffices. Remember, the criminal began draining Fraser's Ledger account at 9:19 a.m., just one hour, eleven minutes after the SIM port-out. And the SIM port-out occurred (at most) a few days after the Mint data breach. The allegations of proximate cause here are sufficiently direct and not comparable to the "Rube Goldbergesque system of fortuitous linkages" where California courts have held proximate cause lacking as a matter of law. *Steinle v. United States*, 17 F.4th 819, 822–23 (9th Cir. 2021).

Second, Mint contends the allegations fail due to their reliance upon multiple independent illegal acts of third parties (Br. 9). Under California law: "The defense of superseding cause absolves the original tortfeasor, even though his conduct *was* a substantial contributing factor, when an independent event subsequently intervenes in the chain of causation, producing harm of a kind and degree so far beyond the risk the original tortfeasor should have foreseen that the law deems it unfair to hold him responsible." *Chanda v. Fed. Home Loans Corp.*, 215 Cal. App. 4th 746, 755 (2013) (cleaned up). In other words:

> To qualify as a superseding cause so as to relieve the defendant from liability for the plaintiff's injuries, both the intervening act and the results of that act must not be foreseeable.... Whether an intervening force is superseding or not generally presents a question of fact, but becomes a matter of law where only one reasonable conclusion may be reached.

Id. at 755–56. Here, "it could hardly be argued that the risk of the harm that befell plaintiffs was as a matter of law unforeseeable." *Lawson v. Safeway Inc.*, 191 Cal. App. 4th 400, 417 (2010). Fraser alleges that Mint provided criminals with all the information and access they needed to hack his accounts and steal his assets (Compl. ¶ 63). He further explains that SIM hijacking represents a national problem, one that has spurred FCC action (Compl. ¶¶ 68–80). At this posture, given the known threat of SIM hijacking and that Mint purportedly bypassed the pin verification Fraser set up, the complaint plausibly alleges foreseeable acts that do not qualify as superseding causes.

Mint disagrees and asserts it "lacks the legal and practical ability to control the acts of criminals" (Br. 10). "However, this expectation does not exonerate a defendant whose 'conduct has created or increased the risk of harm.' " *Lawson*, 191 Cal. App. 4th at 418 (quoting Rest. 2d Torts § 449, cmt. a). The modern standard addressed herein does not take the rigid view Mint proposes that criminal acts necessarily constitute superseding causes. *See also Bigbee v. Pac. Tel. & Tel. Co.*, 34 Cal. 3d 49, 58 (1983); 6 Witkin, Summary of Cal. Law, Torts § 1366 (11th ed. 2021). The opinions that Mint cites are inapposite. For example, the decision in *Martinez v. Pacific Bell*, 225 Cal. App. 3d 1557, 1565–66 (1990), is distinguishable because, in that matter, plaintiff asserted a telephone company proximately caused his injuries resulting from a robbery because the robbers were attracted to the neighborhood because of a public telephone booth. In contrast, Mint's conduct here much more directly created or increased the risk of harm. Other cited cases do not address California law or apply the previous standard. *See Citizens Bank of Pa. v. Reimbursement Techs., Inc.*, 2014 WL 2738220, at *3 (E.D. Pa. June 17, 2014) (Judge L. Felipe Restrepo); *O'Keefe v. Inca Floats, Inc.*, 1997 WL 703784, at *4 (N.D. Cal. Oct. 31, 1997) (Judge Vaughn R. Walker); *Jesse v. Malcmacher*, 2016 WL 9450683, at *10 (C.D. Cal. Apr. 5, 2016) (Judge Stephen V. Wilson). Fraser plausibly alleges that Mint's data breach and role in the SIM port-out created the opportunity for the cryptocurrency theft.

***4** In sum, at least at this stage, where pleadings are liberally construed and the pleader has not yet had an opportunity to obtain discovery, this order holds it was reasonably foreseeable to both plaintiff and defendant that a breach of the type alleged of defendant's system would pose the risk of a follow-on injury of the type alleged.

2. Section 17200 Claims. (Counts IV–VI).

Turning to Fraser's Section 17200 claims, Mint argues that Fraser cannot be awarded monetary damages pursuant to Section 17200 and that he has not adequately pleaded he is entitled to restitution (Br. 10–11).

First, California's unfair competition law prohibits any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200 *et seq.* Although a plaintiff must allege a loss of money or property caused by the purported unfair competition to qualify for relief, the remedies available under a Section 17200 claim are limited to restitution and injunctive relief. *Id.* § 17204; *Clark v. Super. Ct.*, 50 Cal. 4th 605, 610 (2010). This order consequently **Dismisses with Prejudice** the remedies sought in the "Wherefore" paragraphs contained within Counts IV–VI to the extent they seek relief

beyond restitution and injunctive relief for violations of Section 17200.

Second, the complaint fails to adequately state a claim for restitution. In the context of Section 17200, "restitution means the return of money to those persons from whom it was taken or who had an ownership interest in it." *Shersher v. Super. Ct.*, 154 Cal. App. 4th 1491, 1497 (2007) (citation and quotation omitted); *see also Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1149 (2003).

Here, Fraser vaguely alleges in Count IV that "Plaintiff has lost the benefit of his bargain for his purchased services from Mint that he would not have paid had he known the truth regarding Mint's inadequate data security" (Compl. ¶ 166). His Section 17200 allegations focus, however, on how the "harm caused by Mint's actions and omissions ... is substantial in that it has caused Plaintiff to suffer approximately $466,000.00 in actual financial harm because of Mint's unfair business practices (*id.* ¶ 186; *see also* ¶¶ 165, 194). But a "restitution order against a defendant thus requires both that money or property have been lost by a plaintiff, on the one hand, and that it have been acquired by a defendant, on the other." *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 336 (2011). It was not Mint that acquired Fraser's cryptocurrency, but a third-party criminal. Fraser, consequently, has failed to allege he is entitled to restitution from Mint. Because Fraser does not seek injunctive relief, he fails to adequately state a claim for relief under Section 17200, generally. Counts IV, V, and XI are accordingly **Dismissed.**

3. Computer Fraud and Abuse Act (Count III).

Next up is Fraser's Computer Fraud and Abuse Act (CFAA) claim. Mint contends this claim should be dismissed because the complaint fails to adequately plead conduct and losses necessary for a civil CFAA claim.

"The CFAA was enacted in 1984 to enhance the government's ability to prosecute computer crimes." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130 (9th Cir. 2009). The CFAA also includes a private right of action. 18 U.S.C. § 1030(g). To state a civil claim under the CFAA, the plaintiff must allege: (1) that he or she "suffer[ed] damage or loss by reason of [the defendant's] violation" of the Act; and (2) that one of five enumerated circumstances in Section 1030(c)(4)(A)(i)(I) through (V) is present.

***5** Fraser generally alleges Mint violated CFAA Sections 1030(a)(2)(C) and 1030(a)(4). Section 1030(a)(2)(C) ascribes liability to one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer." Section 1030(a)(4), in turn, finds liable one who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." Fraser then further alleges, per Section 1030(c)(4)(A)(i)(I), losses aggregating more than $5,000 in value (Compl. ¶¶ 146, 151).

As an initial matter, Fraser has asserted an aiding and abetting theory of liability (Compl. ¶ 146). As Judge Beth Labson Freeman of our district recently explained in *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *4 (N.D. Cal. Nov. 20, 2020), it is an open question whether such a claim can be asserted under the CFAA in a civil suit. Regardless, the parties failed to brief aiding-and-abetting liability and this order finds Fraser's CFAA claim fails for the more fundamental reason that the pleading does not adequately allege harm recognized under the Act.

The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). It defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). As the Supreme Court recently held: "The statutory definitions of 'damage' and 'loss' thus focus on technological harms — such as the corruption of files — of the type unauthorized users cause to computer systems and data.... The term's definitions are ill fitted, however, to remediating 'misuse' of sensitive information...." *Van Buren v. United States*, 141 S. Ct. 1648, 1659–60 (2021). In other words, "the CFAA creates the right to recover damages and losses related to a computer or system, not damages that flow from the use of unlawfully obtained information." *Delacruz v. State Bar of Cal.*, 2017 WL 7310715, at *6 (June 21, 2017) (Judge Susan Van Keulen), *report and recommendation adopted*, 2017 WL 3129207 (N.D. Cal. July 24, 2017) (Judge Beth Labson Freeman).

Here, the complaint recites only conclusory allegations that, due to Mint's conduct and the interruption of "[p]laintiff's service, he has suffered damage far in excess of Five Thousand Dollars" (Compl. ¶¶ 151–52). The only damage or loss that Fraser cites in his complaint, however, is the theft of his cryptocurrency, which does not constitute loss related to a computer or system. Rather, the loss here flows from the use of the unlawfully obtained information to hack Fraser's Ledger account. This order finds this type of damage or loss is not recognized by the CFAA. *See also Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1263 (9th Cir. 2019).

Accordingly, the CFAA claim is **Dismissed.**

4. Contract-Related Claims (Count XI, XII).

Mint next challenges two of Fraser's contract-related claims.

First, Mint argues that the claim for breach of the implied covenant of good faith and fair dealing should be dismissed because Fraser merely alleges that Mint failed to comply with the express terms of the contract (Br. 23). This order finds the implied covenant claim duplicative of Fraser's breach of contract claim. The only justification for asserting a separate cause of action for breach of the implied covenant is to obtain a tort recovery in those limited circumstances in which such tort recovery is allowed. Those narrow circumstances do not apply here. *See Nasseri v. Wells Fargo Bank, N.A.*, 147 F. Supp. 3d 937, 943 (N.D. Cal. 2015); *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990).

***6** Fraser's claim for breach of the implied covenant of good faith and fair dealing parrots his breach of contract claim and seeks the same relief. The separate claim for the implied covenant is consequently **Dismissed with Prejudice.** The allegations will be treated as part of the contract claim.

Second, Fraser also asserts a claim for breach of an implied-in-fact contract. A "contract implied in fact consists of obligations arising from a mutual agreement and intent to promise where the agreement and promise have not been expressed in words." *Retired Emps. Ass'n of Orange Cty., Inc. v. Cty. of Orange*, 52 Cal. 4th 1171, 1178 (2011) (quotation omitted). Instead, the existence and terms are manifested by conduct; beyond that, implied-in-fact contracts have the same legal effect and basic elements as express contracts. *Dones v. Life Ins. Co. of N. Am.*, 55 Cal. App. 5th 665, 691 (2020); *Yari v. Producers Guild of Am., Inc.*, 161 Cal. App. 4th 172, 182 (2008).

Mint asserts the claim should be dismissed because there are insufficient factual allegations regarding Mint's intent to create an implied-in-fact contract, the "very heart" of such an agreement. *See Div. of Labor Law Enf't v. Transpacific Transp. Co.*, 69 Cal. App. 3d 268, 275 (1977). Fraser, however, adequately alleges his subscription to Mint's service and how it violated its "commitment to maintain confidentiality and security" as reflected in its privacy policy and terms and conditions (Compl. ¶¶ 243–44). Further, per Rule 8, Fraser properly asserts this theory of recovery in the alternative and alleges that it would apply "[t]o the extent that Mint's Privacy Policy and Terms and Conditions did not form express contracts" (*id.* ¶ 242). *Cf. Lance Camper Mfg. Corp. v. Republic Indem. Co.*, 44 Cal. App. 4th 194, 203 (1996). This order finds the specific allegations for the implied-in-fact contract limited but, for now, may proceed.

5. Negligence (Counts VII–IX).

To state a claim for negligence in California, a plaintiff must establish a duty, a breach of that duty, proximate cause, and damages. *See Corales v. Bennett*, 567 F.3d 554, 572 (9th Cir. 2009). Generally, purely economic losses are not recoverable in tort. *Seely v. White Motor Co.*, 63 Cal. 2d 9, 18 (1965). Put simply, "the economic loss rule prevent[s] the law of contract and the law of tort from dissolving one into the other." *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004) (quotation omitted).

If a plaintiff's harms are purely economic, courts employ a six-part test to determine whether a "special relationship" existed between the parties that demonstrates that defendant owed plaintiff a duty of care such that an action in tort may be maintained. *See J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979). The *J'Aire* test considers: (1) the extent to which the transaction was intended to affect the plaintiff; (2) the foreseeability of harm to the plaintiff; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the defendant's conduct and the injury suffered; (5) the moral blame attached to the defendant's conduct; and (6) the policy of preventing future harm. *Ibid.* "The *J'Aire* court emphasized that the foreseeability of the economic harm to the plaintiff from the defendant's negligent conduct was the critical factor." *N. Am. Chem. Co. v. Super Ct.*, 59 Cal. App. 4th 764, (1997). Reviewing courts, nevertheless, perform a holistic review. *See Southern California Gas Leak Cases*, 7 Cal. 5th 391, 401 (2019).

***7** As an initial matter, Mint does not contest the third or sixth factors, which, on this procedural posture, this order

will view as favoring a special relationship. We turn to the remaining factors.

First, previous SIM-hijacking decisions have split on whether the first factor supports a special relationship. *Compare Terpin v. AT&T Mobility, LLC*, 2020 WL 883221, at *4 (C.D. Cal. Feb. 24, 2020) (Judge Otis D. Wright, II), *with Shapiro v. AT&T Mobility, LLC*, 2020 WL 4341778, at *3 (C.D. Cal. May 18, 2020) (Judge Consuelo B. Marshall). This order finds *Shapiro* persuasive on this issue — there are no allegations that the wireless services Mint offered to Fraser were " 'intended to affect' the plaintiff[ ] in any way particular to the plaintiff[ ], as opposed to all potential purchasers" of the service. *Ott v. Alf-Laval Agri, Inc.*, 31 Cal. App. 4th 1439, 1455 (1995). The allegations here do not support a plausible inference Fraser can satisfy the first factor.

Second, the complaint provides sufficient allegations that the harm to Fraser was foreseeable. The complaint avers that SIM hijacking is an increasingly common crime that can arise out of the data breach of a wireless carrier (Compl. ¶¶ 37–40, 48, 61–62). Mint's customers were actively petitioning the company for enhanced security such that Mint's co-founder Rizwan Kassim released a public response to their inquiries (*id.* ¶¶ 45–47). The complaint explains how Mint has a federal statutory obligation to protect the personal information of its customers, and that the FCC has promulgated rules on these issues (*id.* ¶¶ 68–80). Further, Mint's own terms and conditions and privacy policy explicitly reference the importance of privacy and keeping data secure (*id.* ¶¶ 81–86). As noted above, Fraser alleges that he added extra security (PIN verification) to his account prior to the SIM port out, but that Mint "bypassed th[at] enhanced security" when it took away control of his account (*id.* ¶ 60). Finally, the complaint alleges how Mint's data breach and the SIM port-out provided all the information and access criminals needed to drain Fraser's Ledger account (*id.* ¶ 63–67). This order finds these allegations sufficient to plausibly satisfy the second *J'Aire* factor. *See Shapiro*, 2020 WL 4341778, at *3; *Terpin*, 2020 WL 883221, at *4; *Ross v. AT&T Mobility, LLC*, 2020 WL 9848766, at *15 (N.D. Cal. May 14, 2020) (Judge Jon S. Tigar).

Skipping to the *fourth* factor, for the same reasons discussed in the proximate cause analysis above, the complaint plausibly alleges a sufficiently close connection between Mint's conduct and Fraser's injury. *See, e.g., Shapiro*, 2020 WL 4341778, at *3.

Considering the *fifth* factor, the allegations previously discussed support this order's conclusion that the complaint plausibly alleges Mint's moral blame. For example, the complaint alleges that Mint bypassed or failed to implement the PIN verification Fraser put in place to protect his account days before the SIM port-out occurred (Compl. ¶¶ 60–66). This plausibly demonstrates a level of moral blame. *See Shapiro*, 2020 WL 4341778, at *4.

Upon a holistic review, this order finds the *J'Aire* factors support the conclusion, at this stage, that Mint had a special relationship with Fraser. Fraser adequately states claims for negligence.

6. Punitive Damages (All Counts).

***8** Mint next argues the complaint fails to properly allege punitive damages. Fraser generally seeks punitive damages in his prayers for relief and specifically seeks punitive damages in "Wherefore" paragraphs for all his claims except declaratory judgment of the unenforceability of Mint's consumer agreement.

For the state-law claims, under California Civil Code Section 3294(a), a plaintiff may recover punitive damages "[i]n an action for the breach of an obligation not arising from contract, where it is proven by clear and convincing evidence that the defendant has been guilty of oppression, fraud, or malice." To establish corporate punitive damages liability, the plaintiff must prove "the wrongful act giving rise to the exemplary damages [were] committed by an 'officer, director, or managing agent.' " *White v. Ultramar, Inc.*, 21 Cal. 4th 563, 572 (1999) (quoting Cal. Civ. Code § 3294(b)). Punitive damages are appropriate if the defendant's acts are reprehensible, fraudulent, or in blatant violation of law or policy. *Tomaselli v. Transamerica Ins. Co.*, 25 Cal. App. 4th 1269, 1287 (1994).

To start, as a matter of law, punitive damages are not available for Section 17200 claims and contract claims. *See Clark*, 50 Cal. 4th at 610 (Section 17200); *Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal. 4th 503, 516 (1994) (contract). This order accordingly **Dismisses with Prejudice** the individual requests for punitive damages contained in the "Wherefore" paragraphs of Counts IV–VI and X–XII. *See Whittlestone, Inc. v. Handi–Craft Co.*, 618 F.3d 970, 974–76 (9th Cir. 2010).

The only remaining state-law claims to consider, then, are Fraser's negligence claims. The California Supreme Court has stated that "punitive damages sometimes may be assessed in

unintentional tort actions under Civil Code section 3294." *Potter v. Firestone Tire & Rubber Co.*, 6 Cal. 4th 965, 1004 (1993). However, "Negligence, even if gross or reckless, cannot justify punitive damages." *Lee v. Bank of Am.*, 218 Cal. App. 3d 914, 920 (1990); *see also Flayac v. Humrichouse*, 855 F.2d 861 (9th Cir. 1988) (mem.).

Fraser's factual allegations on this issue rank as conclusory and lack any factual underpinning:

> MINT's misconduct as alleged herein is malice, fraud, or oppression in that it was despicable conduct carried on by MINT with a willful and conscious disregard of the rights or safety of Plaintiff and despicable conduct that has subjected Plaintiff to cruel and unjust hardship in conscious disregard of his rights

(Compl. ¶ 209; *see also* ¶ 230). The complaint contains no factual allegations that Mint's conduct went beyond recklessness or otherwise qualified as conscious disregard of its duty of care towards Fraser. The instant allegations are distinguishable from those in *Ross*, where the punitive damages claim survived. In *Ross*, the plaintiff alleged that AT&T's employees had worked with the hackers who performed the SIM hijacking, and that the FCC had previously fined AT&T because its employees had accessed and sold the data of thousands of AT&T customers to third parties. 2020 WL 9848766, at *2, *18. Here, Fraser's allegations regarding Mint employees' conscious involvement in a SIM hijacking (*e.g.*, Compl. ¶ 41), rank as conclusory and need not be accepted as true. Fraser's request for punitive damages for his state-law negligence claims are **Dismissed.**

***9** Turning to plaintiff's federal claims, the analysis is similar. Generally, "absent clear direction to the contrary by Congress, the federal courts have the power to award any appropriate relief in a cognizable cause of action brought pursuant to a federal statute." *Franklin v. Gwinnett Cnty. Pub. Schs.*, 503 U.S. 60, 70–71 (1992).

The plain language of the CFAA does not authorize punitive damages. Section 1030(g) recites, in relevant part: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Given the plain language of the statute, this order finds that the CFAA limits monetary relief to compensatory damages and does not permit a request for punitive damages. S*ee, e.g., Massre v. Bibiyan*, 2014 WL 2722849, at *3 (S.D.N.Y. June 16, 2014) (Judge Katherine P. Failla).

Turning to the Federal Communications Act, Section 206 states in relevant part, that upon a finding of liability the common carrier "shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney's fee." The Supreme Court has "held that where a statute provides recovery for 'damages sustained,' the recovery does not include punitive damages." *Nat'l Comms. Ass'n, Inc. v. Am. Tel. & Tel. Co.*, 1998 WL 118174, at *31–33 (S.D.N.Y. Mar. 16, 1998) (Judge Loretta A. Preska) (citing *Local 20, Teamsters, Chauffeurs & Helpers Union v. Morton*, 377 U.S. 252, 260–61 (1964)). In light of the plain language of the statute, this order finds the Federal Communications Act does not permit a punitive damages remedy. *See also, e.g., Cahnmann v. Sprint Corp.*, 133 F.3d 484, 491 (7th Cir. 1998). Consequently, this order **Dismisses with Prejudice** the individual requests for punitive damages specified in the "Wherefore" paragraphs for Counts II and III.

CONCLUSION

For the foregoing reasons, the motion is **Granted in Part** and **Denied in Part.** Plaintiff's specific requests for punitive damages for his Section 17200 claims, contract claims, CFAA claim, and Federal Communications Act claim are **Dismissed with Prejudice.** His specific request for remedies beyond restitution and injunctive relief as to his Section 17200 claims are also **Dismissed with Prejudice.** His request for punitive damages as to his negligence claims are **Dismissed.**

Further, plaintiff's separate implied covenant of good faith and fair dealing claim is **Dismissed with Prejudice.** Those allegations shall be treated as part of the breach of contract claim. Plaintiff's CFAA claim and Section 17200 claims are **Dismissed.** Defendant's motion is otherwise **Denied.**

Plaintiff may move for leave to amend as to the claims dismissed without prejudice. Any such motion shall be due by **May 11 at Noon.** Any such motion must include as an exhibit a redlined version of the proposed amendment that clearly identifies all changes from the current complaint. This order highlighted certain deficiencies in the complaint, but it will not necessarily be enough to add sentences parroting each missing item identified herein. If plaintiff moves for leave to

file another amended complaint, he should be sure to plead his best case and account for all criticisms, including those not reached by this order.

***10 IT IS SO ORDERED.**

All Citations

Slip Copy, 2022 WL 1240864

End of Document

KeyCite Yellow Flag - Negative Treatment
Distinguished by In re Apple iPhone 3G Products Liability Litigation, N.D.Cal., April 2, 2010

2003 WL 21530185
Only the Westlaw citation is currently available.
United States District Court, C.D. California.

Bruce **GATTON** and Richard Samko, on behalf of themselves and on behalf of the general public, Plaintiff(s),

v.

T–MOBILE USA, INC., a foreign corporation, and Does 1 through 20, inclusive, **T–Mobile**(s).

No. SACV 03–130 DOC
|
April 18, 2003.

Synopsis

Background: Customers sued provider of wireless telephone services in state court, challenging provisions of service contract. Provider removed and moved to compel arbitration. Customers moved for remand.

Holdings: The District Court, Carter, J., held that:

[1] amount in controversy requirement for diversity jurisdiction was not satisfied;

[2] challenge to non carryover of unused monthly minutes was challenge to rates, raising federal question and allowing for removal;

[3] arbitration clause was procedurally unconscionable; and

[4] contract was not substantively unconscionable, except as to provision barring class actions.

Motions granted in part, denied in part.

West Headnotes (7)

[1] **Federal Courts** Claims for declaratory or injunctive relief

Customers suing wireless telephone services provider could not satisfy amount in controversy requirement for diversity jurisdiction by claiming expenses that would be incurred by provider if forced to obey sought after injunction would exceed $75,000. 28 U.S.C.A. § 1332.

[2] **Removal of Cases** Allegations in Pleadings

States Telecommunications; wiretap

Telecommunications Rates and charges

Federal Communications Act prohibition on state regulation of rates charged by wireless telephone providers did not completely preempt state regulation of providers, creating federal question jurisdiction over non-rate related state court case and allowing for removal, even though only state causes of action were pleaded. 28 U.S.C.A. § 1332.

8 Cases that cite this headnote

[3] **Removal of Cases** Allegations in Pleadings

There was no federal question jurisdiction over removed state law claims, brought by customers of wireless telephone provider, challenging arbitration provision in service contract, cancellation policy and advertising practices, despite contention that they were artfully pleaded claims that should have been brought under Federal Communications Act (FCA). Communications Act of 1934, § 1 et seq., as amended, 47 U.S.C.A. § 151 et seq.

14 Cases that cite this headnote

[4] **Removal of Cases** Allegations in Pleadings

State court suit by customers, against wireless telephone provider, challenging practice of not carrying over unused minutes paid for in previous billing period, was artfully pleaded attempt to challenge rates, prohibited in state court actions by Federal Communications Act (FCA), creating federal question and allowing for removal of suit. 28 U.S.C.A. § 1332, 1441; Communications Act of 1934 § 332(c)(2), as amended, 47 U.S.C.A. § 332(c)(2).

2 Cases that cite this headnote

[5] Alternative Dispute Resolution Unconscionability

Arbitration clause in contract for wireless telephone services was procedurally unconscionable, for purposes of enforceability under Federal Arbitration Act (FAA), due to inequality of bargaining power between services provider and customer and lack of opportunity to negotiate terms, even though provision was conspicuously displayed. 9 U.S.C.A. §§ 3,4.

[6] Alternative Dispute Resolution Unconscionability

Arbitration clause of services contract, between wireless telephone services provider and customer, was not substantively unconscionable, for purposes of enforcement under Federal Arbitration Act (FAA), even though provider could assign accounts receivable to collection agencies not required to arbitrate, there was liability limitation, arbitration expenses were allegedly high, and discovery opportunities were limited. 9 U.S.C.A. §§ 3,4.

1 Case that cites this headnote

[7] Alternative Dispute Resolution Unconscionability

Provision of arbitration clause, in contract providing for wireless telephone service, precluding class actions against services provider, was substantively unconscionable and unenforceable under Federal Arbitration Act (FAA), due to lack of mutuality. 9 U.S.C.A. §§ 3,4.

1 Case that cites this headnote

ORDER (1) DENYING PLAINTIFFS' MOTION TO REMAND; AND (2) GRANTING DEFENDANT'S MOTION TO STAY ACTION AND COMPEL ARBITRATION

CARTER, J.

***1** Before the Court is (1) Plaintiffs Bruce **Gatton** and Richard Samko's motion to remand to Superior Court for the State of California for the County of Orange, and (2) Defendant **T–Mobile** USA, Inc.'s (**T–Mobile**) motion to dismiss and/or stay proceedings and compel arbitration. After reviewing the moving, opposing and replying papers, and after oral argument on March 10, 2003 and April 7, 2003, and for the reasons set forth below, the Court DENIES Plaintiffs' motion to remand and GRANTS **T–Mobile's** motion to stay the action and compel arbitration.

I. BACKGROUND

Plaintiffs in this case are **T–Mobile** wireless subscribers. **T–Mobile** is a provider or wireless telephone service. As part of its business practices, **T–Mobile** requires prospective subscribers to sign a standard Customer Service Agreement (CSA). As part of the CSA, any claim or dispute between a subscriber and **T–Mobile** is subject to mandatory arbitration.

The provision in question is the third paragraph out of twenty-five paragraphs set forth in the "**T–Mobile** Terms and Conditions" portion of the CSA. The terms and conditions begins at the second page of the CSA. The provision is entitled, in bold "Mandatory Arbitration; Dispute Resolution." Approximately half of the provision is set forth in capital letters.

Under the provision, the signatory to the CSA agrees that: (1) virtually any claim or dispute between the subscriber and **T–Mobile** will be submitted to binding arbitration with the American Arbitration Association (AAA), pursuant to AAA wireless industry rules; (2) the arbitration will be subject to a choice of law provision; (3) representative or consolidated actions, including class actions, are not permitted; (4) no

lost profits, punitive, incidental or consequential damages, other than the prevailing party's direct damages, may be awarded; (5) the expenses of arbitration will be split by the parties, unless the claim is less than $1000.00, in which case the subscriber pays either $25.00 or nothing; (6) each party will pay the fees and costs of its own counsel, experts and witnesses; (6) the signatory waives "disclaimed damages," jury trial, or participation in a class action even if the clause is deemed inapplicable.

Plaintiffs brought this action in Orange County Superior Court on December 18, 2002. T–Mobile subsequently removed the case to this Court on February 6, 2003. T–Mobile now moves for dismissal or stay of Plaintiffs' case and an order compelling Plaintiffs to arbitrate their claims under the terms of the Agreement. Plaintiffs concurrently move to remand the case to state court.

II. DISCUSSION

A. Removal and Subject Matter Jurisdiction

The FAA provides both federal and state courts with the power to compel arbitration. *See* *Southland Corp. v. Keating,* 465 U.S. 1, 15, 104 S.Ct. 852, 860–61, 79 L.Ed.2d 1 (1984). The FAA does not, however, provide an independent basis for federal jurisdiction. *Id.* As a result, an independent basis for jurisdiction in federal court must be established to enforce arbitration provisions generally. *Id.* Accordingly, the Court must determine that the action was properly removed – i.e. that the Court has subject matter jurisdiction to hear the matter – before considering T–Mobile's motion to compel arbitration.

***2** Under the well pleaded complaint rule, the plaintiff is the master of the complaint, free to avoid federal jurisdiction through pleading only state law claims even though a federal claim may also be available. *See* *Caterpillar Inc. v. Williams,* 482 U.S. 386, 392, 107 S.Ct. 2425, 2429–30, 96 L.Ed.2d 318 (1987). Removal to federal court of an action brought in state court is only proper if the case could have originally been brought in federal court. *See* 28 U.S.C. § 1441(a). There is a strong presumption against removal jurisdiction. *See* *Glaus v. Miles, Inc.,* 980 F.2d 564, 566 (9th Cir.1992). An action improperly removed to federal court may be remanded to state court "[i]f at any time before final judgment it appears that the district court lacks subject matter jurisdiction." 28 U.S.C. § 1447(c). The party seeking removal of the action bears the burden of establishing federal subject matter jurisdiction over the action. *See* *Emrich v. Touche Ross & Co.,* 846 F.2d 1190, 1195 (9th Cir.1988). In the present case, T–Mobile contends that the Court has federal subject matter jurisdiction based on both federal question and diversity jurisdiction.

1. Diversity Jurisdiction

[1] T–Mobile argues that the Court has subject matter jurisdiction based on diversity of citizenship and an amount in controversy greater than $75,000.00. *See* 28 U.S.C. § 1332. Neither Plaintiffs nor T–Mobile dispute that there is complete diversity of citizenship between the parties. Plaintiffs contend, however, that because the claims asserted in the complaint do not satisfy the $75,000.00 amount in controversy requirement, the Court does not have jurisdiction based on diversity.

Plaintiffs' complaint seeks both damages and injunctive relief. The monetary relief requested by each Plaintiffs is less than $10,000. T–Mobile argues, however, that the injunctive relief sought makes the value of the relief sought greater than the $75,000.00 jurisdictional minimum. Specifically, T–Mobile contends that the equitable relief requested by Plaintiffs would result in: (1) rewriting the CSA; (2) printing copies of the new CSA; and (3) mailing copies of the new CSA to customers. (Gray Decl. ¶ 5(a)-(c) .) According to T–Mobile, such an effort would costs hundreds of thousands of dollars. *Id.*[1]

There is a strong presumption that the plaintiff has not claimed a large amount in order to confer jurisdiction on a federal court or that the parties have colluded to that end. *Glaus v. Miles, Inc.,* 980 F.2d 564, 566 (9th Cir.1992) (per curiam). As the party asserting diversity jurisdiction, T–Mobile bears the burden of establishing that the amount in controversy requirement is met. *See* *In re Ford Motor Co./Citibank (South Dakota), N.A., Cardholder Rebate Program Litigation,* 264 F.3d 952, 957 (9th Cir.2001) (citing *Sanchez v. Monumental Life Ins. Co.,* 102 F.3d 398, 404 (9th Cir.1996)). In the Ninth Circuit, the court should look to the value of the right asserted by the plaintiff in determining whether the jurisdictional minimum is satisfied. *See* *Snow v. Ford Motor Co. .,* 561 F.2d 787, 788 (9th Cir.1977); *Ridder Bros., Inc. v. Blethen,* 142 F.2d 395, 398–99 (9th Cir.1944). According to this proposition, T–Mobile contends that the injunctive relief sought necessarily carries the present action across the amount in jurisdiction threshold.

***3** T–Mobile relies on the distinction between class actions and non-class actions as the basis for its amount in

controversy argument. According to **T–Mobile**, the amount in controversy requirement is satisfied if the cost to the **T–Mobile** of the equitable relief sought in a non-class action exceeds $75,000.00. Two recent pronouncements from the Ninth Circuit, both class actions, analyze this interplay.

In *Kanter v. Warner–Lambert Co.,* 265 F.3d 853 (9th Cir.2001), a group of plaintiffs brought a state court class action against the manufacturer of head lice remedies that the plaintiffs alleged were ineffective. *Id.* at 855. The defendant removed the case to federal court on the basis of diversity jurisdiction, but the district court remanded the case to state court, holding that the amount in controversy requirement was not met. *Id.* at 856. The *Kanter* court held that it would be inappropriate to include the cost of plaintiffs' proposed injunctive relief, which would prohibit the defendant from advertising and selling a defective product, in evaluating whether the plaintiffs' claims exceeded the amount in controversy requirement. *Id.* at 861. In reaching its conclusion, the *Kanter* court focused on the "nature of the right asserted," explaining that it would be "reluctant to allow a request for injunctive relief to provide the basis for federal jurisdiction in a case, such as this one, where that relief does not appear to be the primary object of the litigation." *Id.* at 860. While cognizant that proposed injunction was a component of the relief sought, the *Kanter* court focused on the monetary damages as the "essential goal" of the plaintiffs in the litigation. *Id.*

Similarly, in *In re Ford Motor Co./Citibank,* 264 F.3d at 952, defendants to a class action seeking, among other things, injunctive relief, argued that the costs of compliance with the proposed injunction established the amount in controversy for diversity purposes. *Id.* at 958. The *In re Ford Motor Co./ Citibank* court concluded that the administrative costs of compliance with the proposed injunction did not serve to establish that the amount in controversy requirement was satisfied. *Id.* at 960. More importantly, the Ninth Circuit noted that its holding would be the same whether the administrative costs of the injunctive relief were incurred in reference to one plaintiff or six million plaintiffs. *Id.* The rationale for this non-distinction is compelling:

> "It is fundamentally violative of the principle underlying the jurisdictional amount requirement – to keep small diversity suits out of federal court. If the argument were accepted, and the administrative costs of complying with an injunction were permitted to count as the amount in controversy, then every case, however trivial, against a large company would cross the threshold. It would be an invitation to file state-law nuisance suits in federal court."

***4** *Id.* (internal citations omitted).

Although *In re Ford Motor Co./Citibank* was a class action, the rule against counting administrative costs of an injunction toward the amount in controversy requirement "should apply to all multi-party complaints." *Id.* at 958. The Ninth Circuit has demonstrated in both *Kanter* and *In re Ford Motor Co./ Citibank* that the administrative costs of complying with a claim for injunctive relief that accompanies other claims for monetary relief should not provide the basis upon which removal is allowed. If the Court were to accept **T–Mobile's** logic, virtually no plaintiff, whether individually or part of a multi-party complaint, could bring an action for injunctive relief against a large corporation in state court because the administrative costs of compliance—here, printing and mailing—would necessarily cross the $75,000.00 threshold. While the principle in *Ridder* that a court should look at the value of the right asserted certainly remains valid, it can hardly be maintained that such a rule was intended to effectively provide "safe harbor" for large corporations from suits in state court simply because it would cost them more to comply with a proposed injunction due to their size.

Accordingly, the amount in controversy requirement is not met in the present case, and, therefore, the Court lacks subject matter jurisdiction based on diversity jurisdiction.

2. Preemption and Artful Pleading

T–Mobile also argues that the Court has subject matter jurisdiction based on federal question jurisdiction. **T–Mobile** makes two arguments in support of this assertion. First, **T–Mobile** contends that the Federal Communications Act (FCA) of 1934, 47 U.S.C. § 151 *et seq.,* completely preempts state law regulation of the rates charged for the mobile service at issue in this case. Second, **T–Mobile** argues that the case may be removed under the artful pleading doctrine.

a. Complete Preemption

[2] In certain limited areas, "Congress may so completely pre-empt a particular area that any civil complaint raising this select group of claims is necessarily federal in character." *Met. Life Ins. Co. v. Taylor,* 481 U.S. 58, 63–64, 107 S.Ct. 1542, 1547, 95 L.Ed.2d 55 (1987). In such a case, removal from state court is proper despite the plaintiff's intention to avoid federal jurisdiction by pleading only state law claims. *See Bastien v. AT & T Wireless Services, Inc.,* 205 F.3d 983,

986 (7th Cir.2000). Complete preemption is thus a judicially crafted 'independent corollary' to the well-pleaded complaint rule. *TPS Utilicom Services, Inc. v. AT & T Corp.,* 223 F .2d 1089, 1097 (C.D.Cal.2002). In situations where federal statutory or common law "so utterly dominates a preempted field that all claims brought within that field arise under federal law, a complaint purporting to raise state law claims in that field actually raises federal claims. Therefore, the well pleaded complaint is satisfied, and removal is proper." *Marcus v. AT & T Corp.,* 138 F.3d 46, 52 (2d Cir.1998).

***5** The "touchstone of the federal district court's removal jurisdiction is ... the intent of Congress." *Met. Life,* 481 U.S. at 66, 107 S.Ct. at 1548. According to the Ninth Circuit, complete preemption is proper when the federal law in question (1) conflicts with state law (conflict preemption); and (2) provides remedies that displace state law remedies (displacement). *Botsford v. Blue Cross & Blue Shield,* 314 F.3d 390, 393 (9th Cir.2002), *as amended,* 319 F.3d 1078 (9th Cir.2003). The complete preemption doctrine is, however, extremely narrow. *TPS Utilicom,* 223 F.2d. at 1097. The doctrine's limited applicability is evidenced by the fact that only three areas have been deemed areas of complete preemption by the United States Supreme Court: (1) claims under the Labor Management Relations Act, *see Avco Corp. v. Aero Lodge No. 735,* 390 U.S. 557, 561–62, 88 S.Ct. 1235, 1237–38, 20 L.Ed.2d 126 (1968); (2) claims under the Employment Retirement and Insurance Security Act (ERISA), *see Met. Life,* 481 U.S. at 66–67, 107 S.Ct. at 1547–48; and (3) certain Indian land grant rights, *see Oneida Indian Nation v. County of Oneida,* 414 U.S. 661, 666–67, 94 S.Ct. 772, 776–77, 39 L.Ed.2d 73 (1974).

The FCA provides that "no State or local government shall have any authority to regulate the entry of or the rates charged by any commercial mobile service or any private mobile service, except that this paragraph shall not prohibit a State from regulating the other terms and conditions of commercial mobile services." 47 U.S.C. § 332(c)(3). In addition, the savings clause to the FCA states: "[n]othing in this chapter shall in any way abridge or alter the remedies now existing at common law or by statute, but the provisions of this chapter are in addition to such remedies." 47 U.S.C. § 414.

The Seventh Circuit, in *Bastien,* concentrated on the plain language of the statute in concluding that the clause completely preempted the regulation of rates, thereby allowing removal to federal court. 205 F.3d at 987 ("This clause completely preempted the regulation of rates"). On the other hand, the Second Circuit reached a contrary conclusion. *See Marcus v. AT & T Corp.,* 138 F.3d 46, 53 (2d Cir.1998) (the "mere fact that the [FCA] governs certain aspects of [AT & T's] billing relationships with its customers does not mean that [the appellants'] claims arise under the Act") (quoting *Nordlicht v. New York Tel. Co.,* 799 F.2d 859, 861 (2d Cir.1986).

T–Mobile's argument for complete preemption relies heavily on *Bastien.* **T–Mobile** also relies on the Ninth Circuit's holding in *AT & T Corp. v. Coeur d'Alene Tribe,* 295 F.3d 899 (9th Cir.2002), as establishing displacement remedies under 47 U.S.C. § 332, which is part of Subchapter III of the FCA. The *Coeur d'Alene* court considered whether a tribal court had jurisdiction to hear a suit brought under Subchapter II of the FCA. *Id.* at 904–905. In holding that Congress vested exclusive jurisdiction in the federal courts and the Federal Communications Commission for suits against common carriers under Subchapter II of the FCA the Ninth Circuit stated that 47 U.S.C. § 207 "establishes concurrent jurisdiction in the FCC and federal district courts only, leaving no room for adjudication in any other forum—be it state, tribal or otherwise." *Id.* at 905.[2]

***6** While the Ninth Circuit has not addressed whether the FCA completely preempts state claims, this Court has previously held, after examining both *Bastien* and *Marcus,* along with other district court opinions, that the FCA does not provide complete preemption. *TPS Utilicom,* 223 F.2d at 1100. Although section 207 establishes jurisdiction to enforce claims under the FCA brought against common carriers, the Court does not find congressional intent to create removal jurisdiction under the FCA. Several factors lead to the Court to its conclusion.

As an initial matter, the Court must proceed cautiously in determining whether an entire area of the law is completely preempted in light of the extremely limited circumstances under which courts have previously applied the doctrine. Second, the preemptive effect of Section 332 is limited to certain state law causes of action. In *TPS Utilicom,* this Court determined that section 332(c)(3)(A) is limited in its preemptive reach to choice of law rather than removal jurisdiction. *Id.* Although contrary to the *Bastien* court's holding that the plain language of the preemption clause triggers complete preemption, the *TPS Utilicom* court did not share as expansive a view of the FCA. *Id.* Instead, the court held that the intent of Congress was not so clearly stated as to support an intent to confer complete preemption. *Id.* "The

language that 'no state or local government shall have *any* authority to regulate the entry of or the rates charged,' 47 U.S.C. § 332(c)(3)(A) (emphasis added), only supports the proposition that the FCA preempts state claims within the scope of this provision." *Id.*

In addition, the savings clause of 47 U.S.C. § 414 does not evidence congressional intent to create removal jurisdiction. "The FCA not only does not manifest a clear Congressional intent to preempt state law actions prohibiting deceptive business practices, false advertisement, or common law fraud, it evidences Congress's intent to allow such claims to proceed under state law." *Marcus,* 138 F.3d at 54. Neither the Labor Management Relations Act nor ERISA, two other areas where the federal courts have found an area of law completely preempted, contain a savings clause similar to the FCA. Several district courts have found this situation persuasive, if not determinative. *See TPS Utilicom,* 223 F.2d at 1099; *Bryceland v. AT & T Corp.,* 122 F.Supp.2d 703, 709 (N.D.Tex.2000); *Aronson v. Sprint Spectrum, L.P.,* 90 F.Supp.2d 662, 668 (W.D.Pa.2000). As congressional intent is the "touchstone" of the federal district courts' removal jurisdiction, removal jurisdiction cannot lie where clear evidence of such intent is lacking. *Met. Life,* 481 U.S. at 66, 107 S.Ct. at 1548.

Faced with a seeming lack of congressional intent, the existence of a savings clause, no definitive pronouncement on the issue from the Ninth Circuit, and considering the limited and narrow areas in which state law is deemed completely preempted, complete preemption based on the FCA does not provide the Court with subject matter jurisdiction over the present case.

b. Artful Pleading

***7 [3]** **T–Mobile** argues alternatively that the Court has subject matter jurisdiction because Plaintiffs' state law claims are in reality artfully pled federal claims. The artful pleading doctrine is an outgrowth of the well-pleaded complaint rule. *Sullivan v. First Affiliated Securities, Inc.,* 813 F.2d 1368, 1372, *cert. denied,* 484 U.S. 850, 108 S.Ct. 150, 98 L.Ed.2d 106 (1987). "[A]lthough the plaintiff is master of the complaint and may rely on either federal or state law to define his or her cause of action, and thereby control the forum for the complaint's adjudication, it is also an accepted rule that 'the plaintiff cannot defeat removal by masking or 'artfully pleading' a federal claim as a state claim." ' *Ethridge v. Harbor House Restaurant,* 861 F.2d 1389, 1403 (9th Cir.1988) (quoting *Sullivan,* 813 F.2d at 1372). "Under the artful pleading doctrine, a plaintiff may not avoid federal jurisdiction by 'omitting from the complaint federal law essential to his claim, or by casting in state law terms a claim that can be made only under federal law." ' *Rains v. Criterion Systems, Inc.,* 80 F.3d 339, 344 (9th Cir.1996) (citing *Olguin v. Inspiration Consol. Copper Co.,* 740 F.2d 1468, 1472 (9th Cir.1984)). A federal court may therefore recharacterize an artfully pleaded state claim as a federal claim. *Id.* The artful pleading doctrine does not, however, allow a defendant to rewrite a plaintiff's properly pled state law claim in order to remove it to federal court. *Id.*

According to **T–Mobile**, Plaintiffs' claims challenge **T–Mobile's** rates and therefore arise under 47 U.S.C. §§ 201(b) and 207, and necessarily cannot be properly brought under state law. Plaintiffs' complaint alleges that certain provisions of the "Terms and Conditions" agreement, which the customer signs when purchasing a **T–Mobile** telephone and service plan, constitute unlawful business practices. Specifically, Plaintiffs allege in their first cause of action that several of the following clauses set forth in the Terms and Conditions are unlawful or unconscionable: (1) paragraph 3 because it compels mandatory arbitration of claims, precludes class action or representative lawsuits, includes a waiver of damages, (including punitive damages), and includes a waiver of jury trial; (2) paragraph 15 in its limitations on liability and limitation of remedy; (3) paragraph 16 concerning indemnification; (4) paragraph 22 regarding the one year statute of limitations; (5) paragraph 7 concerning the $200.00 contract cancellation fee; (6) paragraph 14 because it requires the waiver of any implied warrant regarding the telephone unit. Plaintiffs complaint also seeks to enjoin **T–Mobile** from enforcing the CSA as to the provisions Plaintiffs deem unlawful or unconscionable, as well as requesting restitution and disgorgement of ill-gotten profits and rescission of Plaintiffs agreements with **T–Mobiles**. (Compl.¶ 18.)

Plaintiffs' second cause of action alleges unfair business practices concerning the **T–Mobile** Terms and Conditions agreement. Plaintiffs specifically complain about paragraph 11, which allows **T–Mobile** to keep any security balance of $5.00 or less; paragraph 4, which allows **T–Mobile** to modify the CSA through sending out notice to subscribers; paragraph 12, whereby any minutes purchased but not used in a particular billing period expire at the end of that billing period; and delayed billing practices. (Compl.¶ 28.) Plaintiffs also seek to enjoin the practices set forth in their second cause of action, as well as restitution of monies obtained

and restoration of unused minutes. Finally, Plaintiffs' third cause of action alleges false and deceptive advertising based on T–Mobile's marketing of plans containing the Terms and Conditions Plaintiffs allege are unlawful or unconscionable.

***8** Thus, the Court must determine whether the gravamen of Plaintiffs' complaint is a challenge merely to the Terms and Conditions of the CSA, or a challenge to T–Mobile "rates." T–Mobile argues that challenges to rates are explicitly preempted by section 332 of the FCA. *See In re Comcast Cellular Telecomm. Litig .,* 949 F.Supp. 1193, 1200 (E.D.Pa.1996), and therefore that Plaintiffs' claims are in reality federal claims under section 332, artfully pled under state law.

[4] Plaintiffs' challenges to T–Mobile's advertising practices and the arbitration clause clearly do not implicate the "rates" charged to subscribers. *See Crump v. Worldcom, Inc.,* 128 F.Supp.2d 549, 560 (W.D.Tenn.2001); *see also Esquivel v. Southwestern Bell Mobile Sys., Inc.,* 920 F.Supp. 713, 715 (S.D.Tex.1996) (liquidated damages provision is a "term and condition" rather than a rate under section 332(c)(3)(A), and thus is not preempted). The closer question is whether Plaintiffs' claims relating to T–Mobile's billing practices actually constitute such a challenge. Plaintiffs' contend that because the minutes that are unused in a particular billing period expire if not used, they do not roll over for use in the next billing period.[3] Plaintiffs also contest T–Mobile's so-called delayed billing practice, whereby minutes used in a particular month may be billed in a later month, potentially subjecting the subscriber to additional fees if the total minutes used exceed the plan's allotted monthly minutes.[4]

In *In re Comcast Cellular Telecomm. Litig.,* 949 F.Supp. 1193 (E.D.Pa.1996), the plaintiff brought a state law complaint (1) challenging Comcast's practice of collecting fees from its subscribers for "non-connection" time, and (2) seeking restitution for Comcast's unjust enrichment stemming from the challenged billing practices. *Id.* at 1200. The *Comcast* court held that the claims presented clear and direct challenges to the reasonableness of Comcast's rates and billing practices, and thus were preempted by section 332 of the FCA. *Id.* In addition, the *Comcast* court examined the injunctive relief and restitution sought by the plaintiffs and determined that "[the remedies sought by the Plaintiffs further demonstrate that the true gravamen behind their allegations is a challenge to Comcast's rates and the way in which they are applied .... [the remedies [plaintiffs] seek would require a state court to engage in regulation of the rates charged by a CMRS provider, something it is explicitly prohibited from doing." *Id.* at 1201.

Unlike cases in which a plaintiff challenges only the disclosure of certain billing practices or other aspects of a telecom service provider that may have a "merely incidental" impact on rates, the present case requires the Court to assess the reasonableness of a billing factor. *See Crump,* 128 F.Supp.2d at 560; *see also Fedor v. Cingular Wireless Corp.,* 2001 WL 1465813, *3 (N.D.Ill.2001) (delayed billing challenged appropriateness of roaming fees and was therefore preempted under the artful pleading doctrine). Specifically, Plaintiffs ask the Court to, in effect, determine the reasonableness of T–Mobile's practice not to roll-over unused minutes to the next month. It is inescapable that this form of relief implicates the rates charged by T–Mobile for its cellular telephone service. Plaintiffs basically contend that they pay for 1000 minutes each month, but only receive 800 minutes. The rate paid by subscribers per month is inextricably intertwined with the allocation of minutes received for payment of that rate. There is simply no reasonable way to separate Plaintiffs' challenge to the number of minutes available per month for use and the rate paid for those minutes. There is little doubt that the relief sought by Plaintiffs—i.e. carrying over minutes from one month to the next—would change the way T–Mobile calculates its rates. The relief sought by Plaintiffs would therefore involve the state court in the business of regulating T–Mobile's rates, which Congress, through the FCA, has prohibited.

***9** Plaintiffs claims concerning the arbitration provision, cancellation policies and advertising practices do not raise a federal question and are thus appropriate claims under state law. These claims do not concern T–Mobile's rates, but rather attack certain aspects of the agreement between subscriber and service provider. Nevertheless, Plaintiffs claims challenging the expiration of unused minutes and delayed billing practices are artfully pled federal claims that raise a federal question. Accordingly, it is proper to exercise jurisdiction over the state law claims under the Court's supplemental jurisdiction. 28 U.S.C. § 1367.

C. T–Mobile's Arbitration Provision

After finding that the Court has subject matter jurisdiction to hear the present case, the Court must now consider T–Mobile's motion to stay the present action.

1. Arbitration Generally

In cases governed by the Federal Arbitration Act (FAA) of 1947, federal courts are empowered to compel arbitration and to stay actions arising out of disputes that are subject to an arbitration agreement. 9 U.S.C. § 3. A party aggrieved by another party's failure to submit a dispute to arbitration may petition a district court for an order compelling arbitration. 9 U.S.C. § 4. "The Court shall hear the parties, and upon being satisfied that the making of the agreement for arbitration or the failure to comply therewith is not in issue, the court shall make an order directing the parties to proceed to arbitration...." *Id.* Further, the Court should then stay all arbitrable claims. 9 U.S.C. § 3 ("[U]pon being satisfied that the issue involved in such suit or proceeding is referable to arbitration under such an agreement, [the court] *shall* on application of one of the parties stay the trial of the action until such arbitration has been had in accordance with the terms of the agreement ....") (emphasis added). When a case includes both arbitrable and non-arbitrable claims, the district court has discretion either to stay all the claims or to stay only the arbitrable claims and proceed with the non-arbitrable claims. *Moses H. Cone Mem'l Hosp. v. Mercury Constr. Corp.,* 460 U.S. 1, 21 n. 23, 103 S.Ct. 927, 939 n. 23, 74 L.Ed.2d 765 (1983); *United States for the Use & Benefit of Newton v. Neumann Caribbean Int'l, Ltd.,* 750 F.2d 1422, 1426–27 (9th Cir.1985).

There are some exceptions to arbitration. If the arbitration clause is not enforceable as a matter of contract law, or if no agreement to arbitrate was ever actually entered into, the dispute need not be sent to arbitration. In addition, the legislature may indicate that a statutory claim is not subject to arbitration. In the present case, Plaintiffs argue that the arbitration provision is unenforceable because it is an unconscionable, mandatory, and one-sided adhesion clause according to *Armendariz v. Foundation Health Psychcare Servs.,* 24 Cal.4th 83, 99 Cal.Rptr.2d 745, 6 P.3d 669 (Cal.2000).[5]

An adhesion contract is "a standardized contract, which, imposed and drafted by the party of superior bargaining strength, relegates to the subscribing party only the opportunity to adhere to the contract or reject it." *Neal v. State Farm Ins. Cos.,* 188 Cal.App.2d 690, 10 Cal.Rptr. 781, 784 (1961). An adhesion contract is unconscionable when both procedural unconscionability, meaning surprise or distress stemming from unequal bargaining power, and substantive unconscionability, meaning overly harsh or one-sided terms, are present. *See Armendariz,* 99 Cal.Rptr.2d at 767, 6 P.3d 669. However, procedural and substantive unconscionability "need not be present in the same degree." *Id.* When great substantive unconscionability is present, less procedural unconscionability is required before the agreement will be invalidated. *See id.*

1. Procedural Unconscionability

***10** **[5]** The arbitration clause contained in the Agreement was an adhesion contract. **T–Mobile** was in a position of superior bargaining strength, and Plaintiffs had to sign the agreement in order to obtain service from **T–Mobile**. Therefore, at least some element of procedural unconscionability is present in the Agreement. *Ferguson v. Countrywide Credit Indus., Inc.,* 298 F.3d 778, 784 (9th Cir.2002); *Lozano v. AT & T Wireless,* 216 F.Supp.2d 1071, 1075 (C.D.Cal.2002).

Plaintiffs also contend that the elements of the provision are essentially unreadable, and the positioning of the provision on the Agreement, as well as the font used, make the provision nearly impossible to read, thus constituting a "surprise component." *American Software, Inc. v. Ali,* 46 Cal.App.4th 1386, 54 Cal.Rptr.2d 477, 480 (Cal.Ct.App.1996). The arbitration provision is set forth on the second of five pages in the Agreement. (Compl.Ex. A.) It is not, therefore, buried deep within a heap of paper or otherwise lengthy agreement. *See Villa Milano Homeowners Ass'n v. II Davorge,* 84 Cal.App.4th 819, 102 Cal.Rptr.2d 1, 7 (Cal.Ct.App.2000). Furthermore, the provision is the third of twenty-five terms, and the first two terms are rather short. (Compl.Ex. A.) Therefore, even if a subscriber read only the first few terms, they would read the arbitration provision. In addition, approximately half of the provision is set out in capital letters. *Id.* Of the twenty-five provisions in the Terms and Conditions section of the Agreement, only four contain capital lettering of any sort. *Id.* Contrary to Plaintiffs' assertion that the arbitration provision is hidden away and is too small to read, it is actually one of the most conspicuous terms in the entire Agreement.

Nonetheless, because the arbitration provision is the result of unequal bargaining power between the subscriber and **T–Mobile**, with no opportunity to negotiate the offending terms, the Court narrowly finds the provision procedurally unconscionable.

2. Substantive Unconscionability

[6] Plaintiffs must also show that the arbitration provision is substantively unconscionable. Substantive unconscionability "traditionally involves contract terms that are so one-

sided as to 'shock the conscience' or that impose harsh or oppressive terms." *24 Hour Fitness, Inc. v. Superior Court,* 66 Cal.App.4th 1199, 78 Cal.Rptr.2d 533, 541 (Cal.Ct.App.1998). In *Stirlen v. Supercuts, Inc.,* for instance, the court found the arbitration clause in an adhesion contract to be substantively unconscionable because it relegated all employee claims to arbitration while allowing the employer to go to court, restricted the discovery available to the employee but not the employer, and unilaterally deprived the employee of remedies. 51 Cal.App.4th 1519, 60 Cal.Rptr.2d 138, 151–52 (Cal.Ct.App.1997). The California Supreme Court likewise found an arbitration provision substantively unconscionable for lack of mutuality and a restriction on the employee's remedies. *Armendariz,* 99 Cal.Rptr.2d at 772, 6 P.3d 669.

***11** Plaintiffs argue substantive unconscionability on several grounds. First, Plaintiffs contend that the arbitration provision is unconscionably unilateral because **T–Mobile** can assign certain claims against subscribers to a collection agency, who are not forced to arbitrate those claims. Here, **T–Mobile** itself is subject to the same arbitration terms as its subscribers. (Compl.Ex. A.) The only exception to mandatory arbitration is in the event a past due account is assigned to a collection agency. The Court does not agree that allowing such collection efforts by a collection agency is so one-sided as to "shock the conscience." *Bischoff v. DircTV, Inc.,* 180 F.Supp.2d 1097, 1110 (C.D.Cal.2002). The Court therefore finds no substantive unconscionability on that ground.

Second, the arbitration provision's limitation on damages, according to Plaintiffs, is substantively unconscionable. Plaintiffs do not provide support for the proposition that a limitation on punitive damages, standing alone, renders a contract substantively unconscionable. *See Lozano,* 216 F.Supp.2d at 1075–76; *Kinney v. United Health Care Serv., Inc.,* 70 Cal.App.4th 1322, 83 Cal.Rptr.2d 348, 355 (Cal.Ct.App.1999). The damages limitation, therefore, while not determinative, is among the group of factors that may contribute to a finding of unconscionability.

Third, Plaintiffs challenge the allocation of fees and administrative expenses between the parties. The arbitration provision provides that administrative expenses will be equally divided unless the claim is less than $1,000.00, whereby the subscriber's fees are capped at $25.00. (Compl.Ex. A.) If the claim is less than $25.00, the subscriber pays nothing. Plaintiff contends, however, that arbitration fees, regardless of **T–Mobile's** cap on administrative costs, are unconscionable because they may rise into the thousands of dollars. In addition to failing to address the speculative nature of the potential fees, Wireless Industry Arbitration Rules appear to cap consumer responsibility for arbitrator's fees in claims or counterclaims not exceeding $10,000.00 to a maximum of $125.00. (Def.Ex. A.) Thus, this does not appear to be a situation where, as Plaintiffs contend, thousands of dollars of fees and expenses are likely as a result of an arbitration, or where the parties are required to split the costs of the arbitrator's fees in an employment contract setting. *See Circuit City Stores, Inc. v. Adams,* 279 F.3d 889, 894 (9th Cir.2002); *Armendariz,* 99 Cal.Rptr.2d at 763–64, 6 P.3d 669. The fees, therefore, do not appear excessive, and do not render the arbitration provision substantively unconscionable.

Fourth, Plaintiffs challenge the Wireless Industry Arbitration Rules pertaining to discovery. According to Plaintiffs, no discovery is available for so-called "Fast Track" claims under $2,000.00. **T–Mobile** argues, apparently correctly, that the very rule relied on by Plaintiffs allows discovery when the arbitrator determines that "the demands of justice require it." (Franklin Depo., Ex. B at F–9 .) Both parties in the present case are subject to the same limitations on discovery. Plaintiffs point to no authority establishing that a limitation on discovery is an independent ground for substantive unconscionability.

***12** A limitation on discovery may work an injustice in certain situations, such as an employment contract situation, where an employee would necessarily need to substantiate a claim against an employer through obtaining discoverable information. *See Ferguson,* 298 F.3d at 786–87; *Kinney,* 83 Cal.Rptr.2d at 355. The present case, however, involves claims concerning subscriber agreements for wireless telephone service. The mutual discovery limitations imposed by the arbitration provision and the Wireless Industry Arbitration Rules no not appear in any way to prevent a subscriber from successfully bringing a claim. Arbitration clauses may properly limit discovery to less than a party might have obtained in court. *Armendariz,* 99 Cal.Rptr.2d at 745, 6 P.3d 669. In addition, it is appropriate for an arbitrator to balance the need for simplicity, one of the chief reasons claims are arbitrated in the first place, against the need for discovery sufficient for a party to substantiate a claim. *Ferguson,* 298 F.3d at 787. The limitations on discovery, therefore, do not render the arbitration provision substantively unconscionable.

[7] Finally, Plaintiffs argue that the prohibition on representative and class actions is unconscionably unilateral, since T–Mobile would never practically bring a class action against a subscriber. The Ninth Circuit recently spoke to this issue in *Ting v. AT & T,* 319 F.3d 1126, 2003 WL 292296 (9th Cir.2003). In *Ting,* a residential long distance customer and a consumer group brought a class action against AT & T asserting, among other things, that contract provisions precluding class actions against AT & T were substantively unconscionable. *Id.* at 4–6. The *Ting* court held that a prohibition on representative or class actions in an adhesion contract violates the bilaterality requirement in all California arbitration agreements. *Id.* at *20.

T–Mobile argues that Plaintiffs do not have standing to challenge the arbitration provision on the basis of the class action prohibition because this action does not involve class claims. The Court does not agree. Under *Ting* and cases from this district, T–Mobile's standing argument would have merit if the arbitration provision merely limited class actions, as the two Plaintiffs bring this case on behalf of themselves individually and on behalf of the general public as a private attorney general, but not as a putative class action. *See id.; see also Bischoff,* 180 F.Supp. at 1108–09 (prohibition on class actions does not render clause substantively unconscionable); *Lozano v. AT & T Wireless,* 216 F.Supp.2d 1071, 1075–76 (C.D.Cal.2002) (same). However, the arbitration provision also bans the present claim, as Plaintiffs are "two or more individuals" whose claims are "determined in one proceeding." (Compl.Ex. A.) In addition, Plaintiffs bring their claims on behalf of the general public pursuant to California Business & Professions Code section 17204. (Compl., ¶ 1.) Such claims are technically barred by the arbitration provisions ban on actions on behalf of potential claimants. (Compl.Ex. A.)

***13** Accordingly, under *Ting,* the portions of the arbitration provision concerning a plaintiff or plaintiffs acting on a consolidated or representative basis appear substantively unconscionable. However, rather than finding the entire provision substantively unconscionable and void, California law favors severance of the unconscionable terms from the rest of the contract. *See Little v. Auto Stiegler, Inc.,* 29 Cal.4th 1064, 130 Cal.Rptr.2d 892, 63 P.3d 979, 2003 WL 548926, *5 (Cal.2003). As this portion of the arbitration provision is easily severable, that term should be deleted, leaving the rest of the arbitration provision enforceable. Because the remainder of the arbitration clause is enforceable, the Court does not find that the clause as a whole is unenforceable.

3. Scope of the Provision

The Court must also determine whether Plaintiffs claims are within the scope of the arbitration provision. The arbitration provision encompasses "ANY CLAIM OR DISPUTE BETWEEN YOU AND U.S. ARISING UNDER OR IN ANY WAY RELATED TO OR CONCERNING THE AGREEMENT, AND/OR OUR PROVISION TO YOU OF GOODS, SERVICE, OR UNITS SHALL BE SUBMITTED TO FINAL, BINDING ARBITRATION." (Compl.Ex. A.) This provision sufficiently covers plaintiffs claims. *See Lozano,* 216 F.Supp.2d at 1078. The Court therefore finds that Plaintiffs' claims are within the scope of the arbitration provision.

III. CONCLUSION

Accordingly, for the reasons set forth above, the Court DENIES Plaintiffs Bruce Gatton and Richard Samko's motion to remand this case to Orange County Superior Court and GRANTS Defendant T–Mobile's motion to stay the action and compel arbitration.

IT IS SO ORDERED.

All Citations

Not Reported in Fed. Supp., 2003 WL 21530185

Footnotes

1 While the Court does not doubt that the expense to T–Mobile in rewriting the CSA, printing new copies of the CSA and mailing those copies to customers would exceed $75,000.00, T–Mobile has not addressed with any specificity why each of those measures would be required, nor how much the activity would cost, except for the statement that the cost would be in the hundreds of thousands of dollars. This can hardly satisfy T–Mobile's burden of proof, especially where Plaintiffs' claims for damages are so far below the amount in controversy requirement.

2 47 U.S.C. § 207 provides that "[a]ny person claiming to be damaged by any common carrier subject to the provisions of this chapter may either make complaint to the Commission as hereinafter provided for, or may bring suit for the recovery

of the damages for which such common carrier may be liable under the provisions of this chapter, in any district court of the United States of competent jurisdiction; but such person shall not have the right to pursue both such remedies."

3 Plaintiffs' example at oral argument was that if a subscriber paid $39.99 per month for 1000 minutes, but only actually used 800 minutes, the additional 200 minutes that the customer paid for would simply disappear.

4 Plaintiffs' example has a subscriber using all of his allotted 1000 minutes in September. However, the subscriber is not billed for 200 of those minutes in September, but instead is billed for those minutes in, for example, November. The result, according to Plaintiffs, is that the subscriber is forced to pay for extra air time if the 200 minutes puts him over the 1000 allotment for the month of November, even though the minutes had theoretically already been paid for in September.

5 At oral argument on March 10, 2003, Plaintiffs represented to the Court that the AAA refused to arbitrate **T**–**Mobile** disputes because **T**–**Mobile** had not earlier complied with certain organizational policies concerning consumer claims. Plaintiff based his representation on a letter received from one Harry Hernandez, Jr. at AAA. **T**–**Mobile** has since produced a letter dated April 2, 2003 from the same Mr. Hernandez that AAA will administer **T**–**Mobile** claims.

End of Document

2023 WL 3182952
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

Christopher WARREN, Plaintiff,
v.
PNC BANK NATIONAL ASSOCIATION, Defendant.

Case No. 22-cv-07875-WHO
|
Signed April 30, 2023

Synopsis

Background: Homeowner brought action alleging that bank violated California Homeowner Bill of Rights (HBOR), California Unfair Competition Law (UCL), and federal Real Estate Settlement Procedures Act (RESPA) by failing to notify or provide him with certain information before foreclosing on and selling his home. Bank moved to dismiss for failure to state a claim.

Holdings: The District Court, William H. Orrick, J., held that:

[1] homeowner stated HBOR claims;

[2] homeowner failed to state California wrongful foreclosure claim;

[3] homeowner failed to state claim for cancellation of written instrument under California law;

[4] homeowner stated RESPA claim;

[5] homeowner stated California negligence claim;

[6] homeowner stated claim under "unlawful" prong of UCL; and

[7] homeowner failed to state claims under "unfair" and "fraudulent" prongs of UCL.

Motion granted in part and denied in part.

West Headnotes (35)

[1] **Federal Civil Procedure** Pleading over

If court dismisses complaint, it should grant leave to amend even if no request to amend pleading was made, unless it determines that pleading could not possibly be cured by allegation of other facts.

[2] **Federal Civil Procedure** Pleading over

In determining whether a pleading could possibly be cured by the allegation of other facts, as required for grant of leave to amend following dismissal, the court should consider factors such as the presence or absence of undue delay, bad faith, dilatory motive, repeated failure to cure deficiencies by previous amendments, undue prejudice to the opposing party and futility of the proposed amendment.

[3] **Mortgages and Deeds of Trust** Loss mitigation; duty to pursue foreclosure alternatives

The California's Homeowner Bill of Rights (HBOR) provides protections for homeowners facing non-judicial foreclosures and reforms aspects of the foreclosure process. Cal. Civ. Code §§ 2923.5, 2924.9.

[4] **Mortgages and Deeds of Trust** Loss mitigation; duty to pursue foreclosure alternatives

To state violations of sections of California's Homeowner Bill of Rights (HBOR) requiring pre-foreclosure notification of foreclosure-prevention options, a homeowner must allege that the subject property is owner-occupied. Cal. Civ. Code §§ 2923.5, 2924.9.

[5] **Mortgages and Deeds of Trust** Loss mitigation; duty to pursue foreclosure alternatives

Homeowner adequately alleged that his home was "owner-occupied," as required to state claim that bank violated California Homeowner Bill of Rights (HBOR) by failing to notify or provide him with certain information before foreclosing on and selling his home; homeowner alleged that he "owned the property and ha[d] lived within subject property years prior to foreclosure and when the notice of default was issued," and that the property was his "primary residence." Cal. Civ. Code §§ 2923.5, 2924.9, 2924.15, 2924.15(a), 2924.15(a)(1)(B).

[6] **Mortgages and Deeds of Trust** Pleading

While a homeowner need not prove materiality motion to dismiss stage of a California Homeowner Bill of Rights (HBOR) action, the homeowner must plead something to satisfy materiality requirement of California Civil Code section providing remedies for material violations of HBOR provisions, just as he must with any element of his claims. Cal. Civ. Code §§ 2923.5, 2924.9, 2924.12(b).

[7] **Mortgages and Deeds of Trust** Loss mitigation; duty to pursue foreclosure alternatives

A violation of California's Homeowner Bill of Rights (HBOR) is material, as required for a homeowner to be eligible for remedies for such violations, if it affected the plaintiff's loan obligations, disrupted her loan modification process, or caused her to suffer harm. Cal. Civ. Code §§ 2923.5, 2924.9, 2924.12(b).

[8] **Mortgages and Deeds of Trust** Loss mitigation; duty to pursue foreclosure alternatives

Mortgages and Deeds of Trust Default

Homeowner adequately alleged that bank materially violated section of California Homeowner Bill of Rights (HBOR) preventing a mortgage servicer, mortgagee, trustee, beneficiary, or agent from recording a notice of default until 30 days after it had contacted the borrower to assess the borrower's financial situation and explore options for the borrower to avoid foreclosure, or 30 days after satisfying due diligence requirements, where homeowner alleged that bank never contacted him before filing notice of default, making notice improper, and filing notice of default was first step in foreclosure process, which could disrupt homeowner's loan modification process by closing that process off before it could even begin or cause harm by foreclosing on home without proper notice. Cal. Civ. Code §§ 2923.5, 2923.5(a)(1)(A), 2923.5(a)(2), 2923.5(e), 2923.55, 2924, 2924.12, 2924.12(b).

[9] **Mortgages and Deeds of Trust** Loss mitigation; duty to pursue foreclosure alternatives

Where a mortgage servicer's violations of the California Homeowner Bill of Rights (HBOR) stem from its failure to communicate with the borrower before recording a notice of default, the servicer may cure these violations by postponing the foreclosure sale, communicating with the borrower about potential foreclosure alternatives, and fully considering any application by the borrower for a loan modification. Cal. Civ. Code §§ 2923.5, 2924.9.

[10] **Mortgages and Deeds of Trust** Loss mitigation; duty to pursue foreclosure alternatives

If a mortgage servicer takes corrective measures to cure violations of California's Homeowner Bill of Rights (HBOR) stemming from its failure to communicate with borrower before recording notice of default, any remaining violation relating to the recording of the notice of default is immaterial. Cal. Civ. Code §§ 2923.5, 2923.5(a)(2), 2924, 2924.9.

[11] **Mortgages and Deeds of Trust** Loss mitigation; duty to pursue foreclosure alternatives

Homeowner adequately alleged that bank materially violated section of California Homeowner Bill of Rights (HBOR) requiring a mortgage servicer to send a borrower a written communication within five business days after recording notice of default unless borrower had previously exhausted their first lien loan modification process, where homeowner alleged that bank did not contact him regarding foreclosure alternatives before or after recording notice of default, that if homeowner had received the required contact and communication, he would have taken action to avoid the foreclosure of his property with other lending sources, and that bank foreclosed on property and recorded trustee's deed upon sale. Cal. Civ. Code §§ 2924.9, 2924.9(a).

[12] **Federal Civil Procedure** Fact issues

District Court would not dismiss homeowner's claim under California Homeowner Bill of Rights (HBOR) section setting out pre-foreclosure communication requirements on basis that notice of default attached to complaint included declaration of compliance with box checked acknowledging that mortgage servicer had tried with due diligence to contact homeowner but had not made contact despite such due diligence, where that argument boiled down to a factual dispute that was inappropriate to decide on a motion to dismiss, given that the notice of default form did not detail what bank's due diligence efforts entailed, a checked box did not ensure that the law was followed, and homeowner had plausibly alleged that he never heard from bank at any point before it foreclosed on his home. Cal. Civ. Code §§ 2923.5, 2923.55(f).

[13] **Mortgages and Deeds of Trust** Existence, Nature, and Form of Remedy

"Wrongful foreclosure" is an equitable action under California law to set aside a foreclosure sale, or an action for damages resulting from the sale, on the basis that the foreclosure was improper.

[14] **Mortgages and Deeds of Trust** Elements, Grounds, and Defenses

To state a claim for wrongful foreclosure under California law, a plaintiff must allege: (1) the trustee or mortgagee caused an illegal, fraudulent, or willfully oppressive sale of real property pursuant to a power of sale in a mortgage or deed of trust; (2) the party attacking the sale was prejudiced or harmed; and (3) in cases where the trustor or mortgagor challenges the sale, the trustor or mortgagor tendered the amount of the secured indebtedness or was excused from tendering.

[15] **Mortgages and Deeds of Trust** Elements, Grounds, and Defenses

Mere technical violations of the foreclosure process will not give rise to a tort claim for wrongful foreclosure under California law; the foreclosure must have been entirely unauthorized.

[16] **Mortgages and Deeds of Trust** Pleading

Homeowner failed to state a claim against bank for wrongful foreclosure under California law, where it was unclear what homeowner based claim upon, given that complaint alleged that bank caused illegal, fraudulent, or willfully oppressive sale of subject property pursuant to power of sale in mortgage or deed of trust, which merely repeated elements of claim, it was not apparent from complaint itself which of bank's alleged wrongdoings was basis of claim, mere technical violations of foreclosure process could not give rise to wrongful foreclosure claim, and complaint was devoid of any allegations that homeowner tendered amount of mortgage, instead summarily arguing that homeowner was excused from tender requirement because of bank's violations of California Homeowner Bill

of Rights (HBOR). Cal. Civ. Code §§ 2923.5, 2924.9.

[17] **Cancellation of Instruments** Invalidity of instrument

Cancellation of Instruments Injury sustained or anticipated

To plead a claim to cancel an instrument under California law, a plaintiff must plausibly allege: (1) the instrument is void or voidable due to, for example, fraud; and (2) there is a reasonable apprehension of serious injury including pecuniary loss or the prejudicial alteration of one's position. Cal. Civ. Code § 3412.

[18] **Cancellation of Instruments** Invalidity of instrument

Homeowner failed to state a claim for cancellation of written instrument under California law in action arising from bank's alleged violations of California Homeowner Bill of Rights (HBOR), California Unfair Competition Law (UCL), and federal Real Estate Settlement Procedures Act (RESPA) by failing to notify or provide him with certain information before foreclosing on and selling his home; homeowner did not allege that an instrument was void or voidable, instead alleging that notice of default and election to sell under deed of trust was void because it did not contain declaration under penalty of perjury and because purported trustee failed to record substitution of trustee with county recorder's office, and homeowner did not allege that tender requirement was satisfied or excused. Real Estate Settlement Procedures Act of 1974 § 6, 12 U.S.C.A. § 2605; Cal. Bus. & Prof. Code § 17200; Cal. Civ. Code §§ 2923.5, 2924.9, 3412.

[19] **Cancellation of Instruments** Restoration of Consideration or Benefit

Mortgages and Deeds of Trust Conditions precedent

Quieting Title Conditions precedent

Under California law, the tender rule applies to equitable claims, such as claims to set aside a trustee's sale, to quiet title, to cancel an instrument, or for wrongful foreclosure.

[20] **Mortgages and Deeds of Trust** Conditions precedent

The "tender rule" under California law is premised on the notion that it would be futile to set aside a foreclosure sale on the technical ground that notice was improper, if the party making the challenge did not first make full tender and thereby establish his ability to purchase the property.

[21] **Cancellation of Instruments** Restoration of Consideration or Benefit

Quieting Title Conditions precedent

Under California law, if a plaintiff properly alleges that a foreclosure was void and not merely voidable, tender is not required to state a cause of action for quiet title or for cancellation of instruments.

[22] **Finance, Banking, and Credit** Servicing

The RESPA regulates the servicing of mortgage loans. Real Estate Settlement Procedures Act of 1974 § 6, 12 U.S.C.A. § 2605.

[23] **Finance, Banking, and Credit** Servicing

Regulation X implements RESPA. Real Estate Settlement Procedures Act of 1974 § 6, 12 U.S.C.A. § 2605.

[24] **Finance, Banking, and Credit** Requests and Inquiries from Borrowers, and Responses Thereto

Homeowner stated claim under RESPA's implementing Regulation X section requiring mortgage servicers to take certain steps upon receipt of any written notice from

borrower asserting error and including information allowing servicer to identify borrower's mortgage loan account and error borrower believed had occurred, which required servicers to maintain policies and procedures reasonable designed to achieve objectives including providing borrowers with timely and accurate information in response to requests for information; homeowner alleged that he immediately contacted bank via letter notifying it of payment error after he learned that his mortgage payment was not applied to his account, letter included homeowner's name, loan number, and address, and letter plausibly described error. Real Estate Settlement Procedures Act of 1974 § 6, 12 U.S.C.A. § 2605; 12 C.F.R. §§ 1024.35, 1024.35(a), 1024.35(b), 1024.35(b)(1)-(3), 1024.35(b)(11).

[25] **Negligence** Elements in general

The elements of a negligence claim are: (1) duty; (2) breach; (3) causation; and (4) damages.

[26] **Mortgages and Deeds of Trust** Negligence

Homeowner adequately alleged a claim for negligence under California law arising from bank's foreclosure on and sale of his home, where homeowner alleged that bank breached its duty of ordinary care and good faith and "duty not to put homeowner in a worse position" when it violated California Homeowner Bill of Rights (HBOR) and that bank owed homeowner a duty of care because its activities violated affirmative statutory duties extrinsic to loan modification, homeowner had plausibly alleged violations of HBOR and RESPA, and homeowner alleged breach of statutory duties via bank's purported failure to provide him certain information before foreclosing on his home. Real Estate Settlement Procedures Act of 1974 § 6, 12 U.S.C.A. § 2605; Cal. Civ. Code §§ 2923.5, 2924.9.

[27] **Antitrust and Trade Regulation** In general; unfairness

California's Unfair Competition Law (UCL) operates as three-pronged statute, where each captures a separate and distinct theory of liability. Cal. Bus. & Prof. Code § 17200.

[28] **Antitrust and Trade Regulation** Source of prohibition or obligation; lawfulness

"Unlawful" prong of California's Unfair Competition Law (UCL) incorporates other laws and treats violations of those laws as independently actionable unlawful business practices under state law. Cal. Bus. & Prof. Code § 17200.

[29] **Antitrust and Trade Regulation** Source of prohibition or obligation; lawfulness

Violation of almost any federal, state, or local law may serve as the basis for a claim under the unlawful prong of California's Unfair Competition Law (UCL). Cal. Bus. & Prof. Code § 17200.

[30] **Antitrust and Trade Regulation** Finance and banking in general; lending

Homeowner plausibly alleged violation of California Unfair Competition Law's (UCL) "unlawful" prong in action arising from bank's foreclosure on and sale of homeowner's home, where UCL incorporated other laws and treated violations of those laws as independently actionable unlawful business practices under state law, meaning that violation of almost any federal, state, or local law could serve as the basis for a claim under the unlawful prong of the UCL, and homeowner had plausibly alleged violations of the California Homeowner Bill of Rights (HBOR) and Real Estate Settlement Procedures Act (RESPA). Real Estate Settlement Procedures Act of 1974 § 6, 12 U.S.C.A. § 2605; Cal. Civ. Code §§ 2923.5, 2924.9.

[31] **Antitrust and Trade Regulation** In general; unfairness

The unfair prong of California's Unfair Competition Law (UCL) requires proving either: (1) the public policy which is a predicate to a consumer unfair competition action is tethered to specific constitutional, statutory or regulatory provisions, or (2) that the challenged business practice is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers. Cal. Bus. & Prof. Code § 17200.

[32] **Antitrust and Trade Regulation** Finance and banking in general; lending

Homeowner failed to adequately allege a claim under "unfair" prong of California Unfair Competition Law (UCL) in action arising from bank's foreclosure on and sale of his property; homeowner's complaint made a laundry list of allegations to support its claim that bank violated all three prongs of UCL, including many that did not appear to apply to homeowner's case, essence of complaint was that bank never provided homeowner information about loan mitigation process, as required by law, before foreclosure, and allegations that could support a claim under "unfair" prong were not clearly tied to public policy or alleged to be immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers, as required to support "unfair" prong UCL claim. Cal. Bus. & Prof. Code § 17200.

[33] **Federal Civil Procedure** Fraud, mistake and condition of mind

Fraudulent prong of California Unfair Competition Law (UCL) is subject to the heightened federal standard of pleading for claims sounding in fraud. Cal. Bus. & Prof. Code § 17200; Fed. R. Civ. P. 9(b).

[34] **Fraud** Elements of Actual Fraud

Fraud Fraudulent Concealment

"Fraud" under California law is an intentional misrepresentation, deceit, or concealment of material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury. Cal. Civ. Code § 3294(c)(3).

[35] **Federal Civil Procedure** Fraud, mistake and condition of mind

Homeowner failed to adequately allege a claim under "fraudulent" prong of California Unfair Competition Law (UCL) in action arising from bank's foreclosure on and sale of his home; complaint alleged that bank acted "purposefully" with regard to loan modification process by causing a lengthy delay and impeding timely loss mitigation denial or approval while expressing that homeowner was "in review," but those allegations were not relevant to homeowner's underlying case, given that he alleged that he never received any communication from bank before foreclosure, and complaint did not appear to allege that bank acted intentionally when it failed to provide homeowner statutorily required pre-foreclosure information. Cal. Bus. & Prof. Code § 17200; Cal. Civ. Code § 3294(c)(3); Fed. R. Civ. P. 9(b).

Attorneys and Law Firms

Anthony Paul Cara, CDLG, PC, Costa Mesa, CA, for Plaintiff.

Kelly Andrew Beall, Cathy Lynn Granger, Wolfe & Wyman LLP, Irvine, CA, for Defendant.

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Re: Dkt. No. 17

William H. Orrick, United States District Judge

***1** Defendant PNC Bank National Association ("PNC") moves to dismiss this complaint brought by plaintiff Christopher Warren, who alleges that PNC violated federal regulations and California law by failing to notify or provide

him with certain information before foreclosing on and selling his home. The motion is GRANTED in part and DENIED in part. Warren has plausibly alleged violations of the California Homeowner Bill of Rights ("HBOR") and Real Estate Settlement Procedures Act ("RESPA") based on PNC's alleged failure to provide him information before and after filing a notice of default, and alleged failure to respond to his notice of error. His negligence claim may proceed based on the statutory duties imposed by the HBOR and RESPA and the alleged breaches of those duties. His Unfair Competition Law ("UCL") claim may also proceed based on these predicate violations.

Other claims fall short and are DISMISSED with leave to amend. As pleaded, Warren's wrongful foreclosure claim is too conclusory to proceed, as is his cancellation of instruments claim. The UCL claim is also too conclusory with respect to the "unfair" and "fraudulent" prongs. To the extent that it relies on these theories of liability, it is DISMISSED.

BACKGROUND

According to the complaint, Warren was "the rightful and lawful owner" of a residence located at 1907 S. Forrest Hill Place in Danville, California ("the property"). Compl. [Dkt. No. 1-1] ¶ 1. It alleges that in January 2015, Warren obtained a $528,000 mortgage loan on the property from lender MB Financial Bank, N.A., which was memorialized by a deed of trust. *Id.* ¶ 9. The deed of trust was allegedly assigned to PNC on August 2, 2018. *Id.* ¶ 12.

On January 17, 2021, Warren allegedly tried to pay his mortgage payment on PNC's website, but "learned that his payment had not gone through and applied to his account." *Id.* ¶ 10. He "immediately contacted PNC" and notified it of the error, tendered $10,000 "to correct any arrears as a result of the error in payment," and told PNC that he was renovating the property "in preparation to place it on the market." *Id.* At some point (although the complaint does not specify when), Warren also attempted to contact PNC "to obtain a debt validation, alternatives to foreclosure as he was planning on selling, and [a] loan modification," but PNC allegedly "would not take his phone calls or respond to his correspondence." *See id.* ¶ 11.

On June 15, 2022, the complaint alleges that a notice of default and election to sell under a deed of trust was recorded at the Contra Costa County Recorder's Office. *Id.* ¶ 13. A notice of trustee's sale was recorded on August 9, 2022, with a sale date set for November 8. *Id.* ¶ 14.

Between October 26 and November 4, 2022, the complaint alleges that Warren "sent several correspondences to PNC" and "tendered payment in the amount of $19,500.00, $2457.25, while referencing his previous payment of $10,000." *Id.* ¶ 15. It further alleges that Warren "never heard from PNC ... either in response to his correspondence or to explore alternatives to foreclosure, at any time." *Id.*

***2** The complaint alleges that PNC foreclosed on the property and recorded a trustee's deed upon sale, but does not specify when. *See id.* ¶ 64. According to a copy of the deed upon sale proffered by PNC, it was recorded on January 3, 2023. *See* RJN [Dkt. No. 18] Ex. 4.[1]

Warren sued PNC in state court on November 25, 2022, alleging violations of RESPA, the HBOR, and UCL, along with claims of negligence, wrongful foreclosure, and cancellation of instruments. *See* Dkt. No. 1-1. PNC removed the matter to this court on December 9, 2022. Dkt. No. 1. It then moved to dismiss the complaint. Dkt. No. 17.

LEGAL STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), a district court must dismiss a complaint if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion, the plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). A claim is facially plausible when the plaintiff pleads facts that allow the court to "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (citation omitted). There must be "more than a sheer possibility that a defendant has acted unlawfully." *Id.* While courts do not require "heightened fact pleading of specifics," a plaintiff must allege facts sufficient to "raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555, 570, 127 S.Ct. 1955.

In deciding whether the plaintiff has stated a claim upon which relief can be granted, the court accepts his allegations as true and draws all reasonable inferences in his favor. *See Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However, the court is not required to accept as

true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008).

[1] **[2]** If the court dismisses the complaint, it "should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000). In making this determination, the court should consider factors such as "the presence or absence of undue delay, bad faith, dilatory motive, repeated failure to cure deficiencies by previous amendments, undue prejudice to the opposing party and futility of the proposed amendment." *Moore v. Kayport Package Express*, 885 F.2d 531, 538 (9th Cir. 1989).

DISCUSSION

I. CALIFORNIA HOMEOWNER BILL OF RIGHTS CLAIMS

***3** **[3]** The HBOR "provide[s] protections for homeowners facing non-judicial foreclosures and reform[s] aspects of the foreclosure process." *Patera v. Citibank, N.A.*, 79 F. Supp. 3d 1074, 1087 (N.D. Cal. 2015) (citation omitted and cleaned up). Warren asserts two violations of the HBOR: sections 2923.5 and 2924.9 of the California Civil Code. Compl. ¶¶ 18-34.[2]

A. "Owner-Occupied"

[4] **[5]** To state violations of sections 2923.5 and 2924.9, Warren "must allege that the subject property is owner-occupied." *See Greene v. Wells Fargo Bank, N.A.*, No. 15-CV-00048-JSW, 2016 WL 360756, at *2 (N.D. Cal. Jan. 28, 2016). California Civil Code section 2924.15 provides that sections 2923.5 and 2924.9 "shall apply only to a first lien mortgage or deed of trust" that is either "secured by owner-occupied residential real property containing no more than four dwelling units" or "secured by residential real property that is occupied by a tenant and that contains no more than four dwelling units" and meets certain other conditions. Cal. Civ. Code § 2924.15(a). " '[O]wner-occupied' means that the property is the principal residence of the borrower and is security for a loan made for personal, family, or household purposes." *Id.* § 2924.15(a)(1)(B).

PNC argues that Warren's first and third claims fail because the complaint does not allege that the property is "owner-occupied." Mot. to Dismiss ("MTD") [Dkt. No. 17] 4:17-5:4. Instead, PNC contends, the complaint "simply alleges in a conclusory manner" that Warren was the "rightful and lawful owner" of the property. *See id.* at 4:28-5:3 (citing Compl. ¶ 1).

Although Warren does not address this argument in his opposition, PNC's argument falls short. It overlooks allegations within the complaint that Warren "owned the property and has lived within subject property years prior to foreclosure and when the notice of default was issued." *See* Compl. ¶¶ 20, 32. PNC also brushes aside the allegation that the property "is [sic] primary residence." *See id.* ¶ 1. This appears to be a typographical error; coupled with the other allegations that Warren lived at the property for years prior to foreclosure and when the notice of default was issued, it plausibly supports that the property was "owner-occupied."

B. Material Violations

Next, PNC argues that Warren's first and third claims should be dismissed because the complaint does not allege specific facts showing that the alleged violations of sections 2923.5 and 2924.9 were "material." MTD at 5:5-6.1. Certain sections of the HBOR rely on California Civil Code section 2924.12 for remedies, which provides in part:

> After a trustee's deed upon sale has been recorded, a mortgage servicer, mortgagee, trustee, beneficiary, or authorized agent shall be liable to a borrower for actual economic damages ... resulting from a material violation of section 2923.55, 2923.6, 2923.7, 2924.9, 2924.10, 2924.11, or 2924.17 by that mortgage servicer, mortgagee, trustee, beneficiary, or authorized agent where the violation was not corrected and remedied prior to the recordation of the trustee's deed upon sale.

Cal. Civ. Code § 2924.12(b). But it only provides remedies for "material" violations of these provisions. *See id.*

***4** **[6]** **[7]** There is some disagreement over whether materiality should be considered at the pleadings stage. *See Cardenas v. Caliber Home Loans, Inc.*, 281 F. Supp. 3d 862, 869 (N.D. Cal. 2017) ("Some [district courts] have concluded that materiality is a factual question that should not be resolved on a motion to dismiss.") (citing cases). While Warren need not *prove* materiality at this point, I agree that he "must plead something to satisfy 2924.12's materiality

requirement"—just as he must with any element of his claims. *See Galvez v. Wells Fargo Bank, N.A.*, No. 17-CV-06003-JSC, 2018 WL 4849676, at *5 (N.D. Cal. Oct. 4, 2018). Courts who have weighed materiality at this juncture have considered a violation "material" if it affected the plaintiff's loan obligations, disrupted her loan modification process, or caused her to suffer harm. *See Cardenas*, 281 F. Supp. 3d at 869-870; *see also Billesbach v. Specialized Loan Servicing LLC*, 63 Cal. App. 5th 830, 837, 278 Cal.Rptr.3d 213 (2021) ("A material violation is one that affected the borrower's loan obligations, disrupted the borrower's loan-modification process, or otherwise harmed the borrower."); *Morris v. JPMorgan Chase Bank, N.A.*, 78 Cal. App. 5th 279, 304 n.14, 293 Cal.Rptr.3d 417 (2022) (adopting definition of "material" used in *Billesbach* and *Cardenas*).

[8] As a threshold matter, PNC argues that violations of both 2923.5 and 2924.9 must be material. *See* MTD at 6:1. But section 2923.5 is not listed among the statutes covered by section 2924.12—section 2923.55 is. *See* Cal. Civ. Code § 2924.12(b). Although the two provisions are "substantively similar," section 2923.55 "generally applies only to larger mortgage servicers," while section 2923.5 "applies to smaller servicers." *Billesbach*, 63 Cal. App. 5th at 844 n.7, 278 Cal.Rptr.3d 213. PNC has not cited to any authority confirming that section 2923.5 falls within section 2924.12 's ambit. *See* MTD at 5:5-6:1; Reply [Dkt. No. 23] 2:12-18.

Assuming (without deciding) that it does, Warren's complaint plausibly alleges a material violation. Section 2923.5 prevents a mortgage servicer, mortgagee, trustee, beneficiary, or agent from recording a notice of default until 30 days after it has contacted the borrower to "assess the borrower's financial situation and explore options for the borrower to avoid foreclosure" or 30 days after satisfying "due diligence requirements." Cal. Civ. Code § 2923.5(a)(1)(A). Under the latter, a notice of default may be filed "when a mortgage servicer has not contacted a borrower ... provided that the failure to contact the borrower occurred despite the due diligence of the mortgage servicer." *Id.* § 2923.5(e). The statute then sets forth what constitutes "due diligence," which includes attempts to contact the borrower by first-class mail, "by telephone at least three times at different hours and on different days," and by certified letter. *Id.*

The essence of Warren's claim is that PNC never contacted him before filing the notice of default and thus, the filing of that notice was improper. *See* Compl. ¶¶ 18-22. This violation is plausibly material. Filing a notice of default is the first step in the foreclosure process. *See* Cal. Civ. Code § 2924. Section 2923.5 requires a servicer to contact the borrower (or make diligent efforts to do so) to "assess the borrower's financial situation and explore options for the borrower to avoid foreclosure." *See id.* § 2923.5(a)(2). As alleged, PNC did not contact Warren. *See* Compl. ¶ 20. It is plausible, then, that this disrupted his loan modification process (by closing that process off before it could even begin) or caused him harm (by foreclosing upon his home without proper notice).

***5** **[9]** **[10]** *Billesbach* offers helpful framework. There, the California Court of Appeal held that

> where a mortgage servicer's violations stem from its failure to communicate with the borrower before recording a notice of default, the servicer may cure these violations by ... postponing the foreclosure sale, communicating with the borrower about potential foreclosure alternatives, and fully considering any application by the borrower for a loan modification.

Billesbach, 63 Cal. App. 5th at 837, 278 Cal.Rptr.3d 213. "Following these corrective measures," the court wrote, "any remaining violation relating to the recording of the notice of default is immaterial." *Id.* Warren's complaint is absent of any similar allegations that would render any of the purported violations immaterial. *See generally* Compl.

[11] The complaint plausibly alleges a material violation of section 2924.9 for similar reasons. Under section 2924.9, unless a borrower has previously exhausted their first lien loan modification process, a mortgage servicer must send the borrower a written communication within five business days after recording notice of default. Cal. Civ. Code § 2924.9(a). That communication must include certain information: (1) that the borrower may be evaluated for a foreclosure prevention alternative; (2) whether the borrower must submit an application in order to be considered for such; and (3) the means and process by which the borrower may obtain an application for a foreclosure prevention alternative. *Id.*

According to PNC, the complaint "contains no facts showing that PNC's purported violations of HBOR prevented plaintiff from a meaningful opportunity to be considered for a loan modification or caused plaintiff harm that would not have been suffered otherwise," and instead "reflect[s] only that plaintiff defaulted on the loan and made a failed attempt to reinstate the loan, which resulted in foreclosure." MTD at 5:20-27.

Warren responds that PNC did not contact him regarding foreclosure alternatives before or after recording the notice of default, and therefore his claim survives. Oppo. at 9:1-7. Although he does not specifically address whether this was a material violation, the complaint plausibly alleges this. *See id.* It alleges that a notice of default was filed on June 15, 2022, and that PNC failed to notify him of foreclosure prevention alternatives as required. Compl. ¶¶ 32-33, 34 (alleging that he "did not receive any phone calls or phone messages and did not receive any pieces of mail" that referred to foreclosure alternatives). It further alleges that if Warren had received "such contact and communication, he would have taken action to avoid the foreclosure of the subject property with other lending sources." *Id.* ¶ 34. Instead, PNC allegedly foreclosed on the property and recorded a trustee's deed upon sale. *Id.* ¶ 64.

Warren has plausibly pleaded that PNC's violation of section 2924.9 materially harmed him, for similar reasons as above. Based on the facts alleged, PNC's failure to communicate about foreclosure prevention alternatives disrupted his loan modification process or otherwise harmed him by closing the door to anything other than foreclosure.

***6** Warren has plausibly pleaded material violations of section 2924.9 and 2923.5.

C. Section 2923.5

[12] PNC argues that Warren's section 2923.5 claim otherwise fails because the notice of default attached to his complaint includes a declaration of compliance with this box checked:

> The mortgage servicer has tried with due diligence to contact the borrower as required by California Civil Code § 2923.55(f) but has not made contact despite such due diligence. The due diligence efforts were satisfied on March 3, 2022.

See MTD at 6:16-7:7 (citing Compl., Ex. C). According to PNC, because Warren's "vague and conclusory allegations" that it failed to comply with section 2923.5 are "expressly contradicted by the statement" in Exhibit C, the notice of default "is controlling" and the claim should be dismissed. *Id.* at 7:1-7.

Warren responds that regardless of the declaration that PNC attempted contact, "none was made." Oppo. at 7:20-22. He contends that although he was "available by phone and mail," he "never received a phone call from PNC nor any written notifications regarding [his] available options." *Id.* at 7:22-23.

This boils down to a factual dispute that is inappropriate to decide on a motion to dismiss. The notice of default attached to the complaint shows that a PNC agent (identified only as "Authorized Signer" on the form, with an unintelligible signature) attested that they tried to contact Warren "as required" by section 2923.55(f). *See* Compl., Ex. C. But the form does not detail what those efforts entailed, and a checked box does not ensure that the law was followed. Moreover, Warren has plausibly alleged that he never heard from PNC at any point before foreclosure. *See, e.g.*, Compl. ¶ 20 ("Plaintiff received no mail or messages from PNC."). Whether PNC in fact attempted to contact Warren will prove out as discovery is conducted and the case progresses. For now, he has sufficiently alleged a violation of section 2923.5.

II. WRONGFUL FORECLOSURE

[13] **[14]** **[15]** **[16]** Wrongful foreclosure "is an equitable action to set aside a foreclosure sale, or an action for damages resulting from the sale, on the basis that that the foreclosure was improper." *Sciarratta v. U.S. Bank Nat'l Ass'n*, 247 Cal. App. 4th 552, 561, 202 Cal.Rptr.3d 219 (2016). To state a claim for wrongful foreclosure under California law, a plaintiff must allege: "(1) the trustee or mortgagee caused an illegal, fraudulent, or willfully oppressive sale of real property pursuant to a power of sale in a mortgage or deed of trust; (2) the party attacking the sale ... was prejudiced or harmed; and (3) in cases where the trustor or mortgagor challenges the sale, the trustor or mortgagor tendered the amount of the secured indebtedness or was excused from tendering." *Cardenas*, 281 F. Supp. 3d at 871 (citation omitted). "[M]ere technical violations of the foreclosure process will not give rise to a tort claim; the foreclosure must have been entirely unauthorized." *Sciarratta*, 247 Cal. App. 4th at 562, 202 Cal.Rptr.3d 219 (citation omitted). PNC challenges Warren's wrongful foreclosure claim on the second and third elements. MTD at 9:12-10:28.

***7** I agree with PNC that this claim falls short. First, it is unclear what Warren bases it upon. The complaint alleges that PNC "caused an illegal, fraudulent, or willfully oppressive sale of the subject property pursuant to a power of sale in a mortgage or deed of trust." Compl. ¶ 65. This is too conclusory on its own; it merely repeats the elements of the claim. And unlike Warren's other claims, it is not apparent from the complaint itself which of PNC's alleged

wrongdoings the basis of this claim. By way of example, it could be based on PNC's alleged improper filing of the notice of default before any attempts to contact him, discussed in more detail above. But it could also be based on the allegation that the notices of default and of trustee's sale were void because the purported trustee "failed to record a substitution of trustee." *See id.* ¶ 28.[3] Because "mere technical violations of the foreclosure process" do not give rise to a wrongful foreclosure claim, and because the plaintiff must "show both that there was a failure to comply with the procedural requirements for the foreclosure sale and that the irregularity prejudiced the plaintiff," more specific allegations are needed for Warren to plausibly state his claim. *See Sciarratta*, 247 Cal. App. 4th at 562, 202 Cal.Rptr.3d 219; *see also Morris*, 78 Cal. App. 5th at 294-95, 293 Cal.Rptr.3d 417.

Similarly, the complaint is devoid of any allegations that Warren tendered the amount of the mortgage. *See generally* Compl. Instead, it summarily argues that he "is excused from the tender requirement because of PNC defendant's violations of" the HBOR. *See id.* ¶ 66. This too is conclusory, as Warren cites to no case law or other authority in the complaint (or his opposition) that supports this. *See id.*; *see also* Oppo. at 9:22-10:27.[4] Again, more specificity is needed for him to plausibly state a wrongful foreclosure claim.

Warren's wrongful foreclosure claim is DISMISSED with leave to amend.

III. CANCELLATION OF INSTRUMENTS

[17] **[18]** Under California Civil Code section 3412, a court may order the cancellation of a written instrument "in respect to which there is a reasonable apprehension that if left outstanding it may cause serious injury to a person against whom it is void or voidable." To plead a claim to cancel an instrument, a plaintiff must plausibly allege: "(1) the instrument is void or voidable due to, for example, fraud; and (2) there is a reasonable apprehension of serious injury including pecuniary loss or the prejudicial alteration of one's position." *U.S. Bank Nat'l Ass'n v. Naifeh*, 1 Cal. App. 5th 767, 778, 205 Cal.Rptr.3d 120 (2016).

[19] **[20]** **[21]** PNC again attacks tender, arguing that because Warren did not adequately plead tender in his complaint, this claim should also be dismissed. MTD at 12:1-16. "The tender rule applies to equitable claims, such as claims to set aside a trustee's sale, to quiet title, to cancel an instrument, or for wrongful foreclosure." *Green v. Cent. Mortg. Co.*, 148 F. Supp. 3d 852, 870 (N.D. Cal. 2015). The rule is "premised on the notion that it would be futile to set aside a foreclosure sale on the technical ground that notice was improper, if the party making the challenge did not first make full tender and thereby establish his ability to purchase the property." *Santana v. BSI Fin. Servs., Inc.*, 495 F. Supp. 3d 926, 937 (S.D. Cal. 2020) (citation omitted). However, there are exceptions to the tender rule, including that if a plaintiff properly alleges that a "foreclosure was void and not merely voidable, tender [is] not required to state a cause of action for quiet title or for cancellation of instruments." *Sciarratta*, 247 Cal. App. 4th at 568, 202 Cal.Rptr.3d 219.

The problem with this claim is two-fold. First, Warren does not sufficiently allege that an instrument was void or voidable, as required to state the first part of the claim. *See Naifeh*, 1 Cal. App. 5th at 778, 205 Cal.Rptr.3d 120. The complaint alleges that the notice of default and election to sell under deed of trust is void because it does not contain a declaration under the penalty of perjury, which Warren seems to allege is required by California Code of Civil Procedure section 2015.5(a). *See* Compl. ¶ 13. But the complaint does not adequately connect the dots between this provision and the documents at issue —i.e., it does not allege that such a declaration is required for these types of documents. *See id.* The complaint further alleges that the notice of default is "further void or voidable" because the purported trustee (identified as Quality Loan Service Corp.) "failed to record a substitution of trustee with the Solano County Recorder's Office." *Id.* ¶ 28. It is unclear why a substitution needed to be filed in Solano County when the property at issue is located in Contra Costa County. Moreover, a substitution of trustee was filed on June 15, 2022, substituting Clear Recon Corp. as the trustee. *See* RJN, Ex. 2. Warren's opposition does not mention the word "void" or "voidable," let alone expand on his earlier allegations. *See generally* Oppo.

***8** This leads to the second issue with Warren's claim. Because he has not adequately alleged that any instrument was void or voidable, he has not adequately alleged tender —either that it was satisfied or that he was excused from doing so. As explained, the allegations in the complaint regarding tender are too conclusory to proceed. Without more specificity, I cannot evaluate whether he is even required to state tender as part of this claim.

Warren's cancellation of instruments claim is DISMISSED with leave to amend.[5]

IV. RESPA CLAIMS

[22] **[23]** **[24]** "RESPA regulates the servicing of mortgage loans." *Hahn v. Select Portfolio Servicing, Inc.*, 424 F. Supp. 3d 614, 624 (N.D. Cal. 2020) (citing 12 U.S.C. § 2605). Regulation X implements RESPA. *See id.* The complaint alleges two violations of Regulation X: section 1024.35 and section 1024.38. *See* Compl. ¶¶ 35-49.[6]

Section 1024.35 requires servicers to take certain steps upon receipt of "any written notice from the borrower that asserts an error" and includes certain information, including the borrower's name, information that allows the servicer to identify the borrower's mortgage loan account, and "the error the borrower believes has occurred." 12 C.F.R. § 1024.35(a). Under section 1024.38, servicers must "maintain policies and procedures that are reasonably designed to achieve" certain enumerated objectives, including providing borrowers with timely and accurate information in response to requests for information. *See id.* §§ 1024.38(a), (b).

PNC first argues that a January 17, 2021, letter that Warren allegedly sent PNC does not constitute a notice of error under section 1024.35 because it "fails to specifically identify any errors in the servicing of the loan." MTD at 15:15-25.[7] According to PNC, "there is no language in the letter which specifically identifies any" of the errors covered by section 1024.35; no language "which specifically requests PNC to do anything, make corrections, or to provide a response"; and "no language whatsoever clearly and unequivocally stating that PNC has made any servicing errors which must be rectified." *Id.* at 15:17-21.

The complaint alleges that after Warren tried to make his mortgage payment on January 17, 2021, and learned that his payment had not been applied to his account, he "immediately contacted" PNC and notified it of the payment error. Compl. ¶ 10 (citing Ex. B). It then attaches the letter that PNC takes issue with. *See id.*, Ex. B. But the letter appears to provide sufficient detail to constitute a notice of error—at least as articulated in section 1024.35(a). It includes Warren's name, the loan number, and address of the property at issue. *See id.*; *see also* 12 C.F.R. § 1024.35(a) (providing that a notice of error must include "the name of the borrower" and "information that enables the servicer to identify the borrower's mortgage loan account"). And although the letter does not cite a specific provision within section 1024.35(b) in identifying the purported error, the information that Warren allegedly sent plausibly describes that error: that a "mix up regarding payments" had occurred, where Warren attempted to pay his mortgage payment online, but that PNC did not receive the payment made. *See* Compl., Ex. B. Warren then clarifies that he was "not sure what happened or how this transpired." *See id.*

***9** Accepting Warren's allegations as true, it is reasonable to infer that this provided PNC sufficient notice of one of the errors listed in section 1024.35(b). The circumstances that Warren's notice described could indicate a failure to accept payment, a failure to apply an accepted payment, or a failure to credit a payment to Warren's account. *See* 12 C.F.R. § 1024.35(b)(1)-(3) (listing these among the categories of errors). It could also constitute "[a]ny other error relating to the servicing of a borrower's mortgage loan." *See id.* § 1024.35(b)(11).

As alleged, PNC was then required to acknowledge Warren's notice of error within five days of receipt, and either correct the error or, after conducting a reasonable investigation, inform him that no error had occurred. *See id.* §§ 1024.35(d), (e)(1). According to the complaint, PNC never responded to Warren. *See* Compl. ¶ 11. Without further argument from PNC, it appears that the notice of error was sufficient for pleading purposes and Warren's claim arising from alleged violations of section 1024.35 may proceed.

Warren has not, however, plausibly stated a violation of section 1024.38. PNC argues that this claim fails as a matter of law because this regulation does not create a private right of action. MTD at 17:4-8. Although PNC relies on district court cases from Michigan, at least some courts within this Circuit have found the same. *See Courtois v. Shellpoint Mortg. Servicing, LLC*, No. CV-20-4095, 2020 WL 13586024, at *1 (C.D. Cal. May 26, 2020) ("numerous other courts have concluded that 12 C.F.R. § 1024.38 does not provide a private right of action"); *Minie v. Selene Fin. L.P.*, No. 18-CV-05364, 2019 WL 199948, at *5 (W.D. Wash. Jan. 15, 2019) (noting that "[t]he plaintiff concedes that there is no private right of action for" section 1024.38).

Warren wholly ignores this argument in his opposition. *See* Oppo. at 9:9-21. Without case law or other authority indicating that he may assert a claim for a violation of section 1024.38, it is DISMISSED with prejudice.

V. NEGLIGENCE

[25] **[26]** The elements of a negligence claim are well-known: (1) duty; (2) breach; (3) causation; and (4) damages.

See In re Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 314 (N.D. Cal. 2018). PNC argues that Warren's negligence claim fails on the first two elements. MTD at 12:17-14:10. I disagree.

Beginning with duty, PNC contends that Warren has not alleged that it owed him any statutory or tort duty of care. *Id.* at 12:20-13:20. Answering the statutory question is all that is needed for the claim to proceed. The complaint appears to rely on a statutory duty, alleging that PNC breached its "duty of ordinary care and good faith" and "duty not to put plaintiff in a worse position" when it violated the HBOR, and that PNC "owed plaintiff a duty of care because [its] activities violated affirmative statutory duties extrinsic to loan modification." *See* Compl. ¶¶ 51-59. According to PNC, because Warren's HBOR claims fail, he has not shown such a statutory duty. MTD at 12:20-26. But Warren has plausibly alleged violations of the HBOR, which plausibly support a duty of care. *See Sheen v. Wells Fargo Bank, N.A.*, 12 Cal. 5th 905, 920, 290 Cal.Rptr.3d 834, 505 P.3d 625 (2022) ("A duty of care may arise through statute or by operation of the common law.") (citation and quotations omitted); *Marcus v. Nationstar Mortg. LLC*, 2022 WL 1486831, at *1 (9th Cir. May 11, 2022) ("HBOR creates statutory duties concerning certain modification applications"); *Ogamba v. Wells Fargo Bank, N.A.*, No. 17-CV-01754, 2018 WL 2842495, at *4-5 (E.D. Cal. June 11, 2018) (allowing negligence claim to proceed because the plaintiff had plausibly alleged violations of the HBOR and the negligence claim "derives from the HBOR violations").

***10** Although the California Supreme Court recently settled a long-running split over whether a lender owed a borrower a *common law* duty of care to "process, review and respond carefully and completely to a borrower's loan modification application," that case, which PNC relies upon in arguing against such a duty here, is distinguishable. *See Sheen*, 12 Cal. 5th at 915, 290 Cal.Rptr.3d 834, 505 P.3d 625 (cleaned up). The issue is not whether Warren's loan modification application was carefully processed, reviewed, and responded to; instead, it is whether PNC provided him with certain information as required by the HBOR (and RESPA). Moreover, the *Sheen* court reiterated—multiple times—that the question was whether the narrow duty described by the plaintiff existed under the common law. *See, e.g.*, *id.* at 920, 290 Cal.Rptr.3d 834, 505 P.3d 625 ("Plaintiff does not identify any statute or regulation that requires Wells Fargo to treat his modification applications with due care."), 921, 290 Cal.Rptr.3d 834, 505 P.3d 625 ("He does not ground such a duty in the extensive body of state and federal legislation and regulations that address mortgage servicing ... including the California Homeowner Bills of Rights."), 921-22, 290 Cal.Rptr.3d 834, 505 P.3d 625 ("Likewise, plaintiff does not bring a claim under any other state or federal law governing mortgage loan modifications, such as ... the Real Estate Settlement Procedures Act."). Warren *does* ground his negligence claim in such statutes and regulations: the HBOR and RESPA.

Finally, and most importantly, *Sheen* listed examples of where "HBOR and complementary federal legislation specify various affirmative actions a servicer is obligated to take," including section 2924.9 of the California Civil Code—only of the violations that Warren plausibly alleges here. *See id.* at 921, 290 Cal.Rptr.3d 834, 505 P.3d 625.

Because Warren has plausibly alleged violations of the HBOR and RESPA, he has plausibly alleged that PNC owed him a statutory duty of care. This is enough for the claim to proceed, without deciding whether such a duty also exists under the common law.

He has also adequately alleged a breach of these duties, based on PNC's alleged failure to provide him certain information before foreclosing upon his home. PNC's argument that his allegations are too conclusory to show breach are not persuasive, for reasons similar to those that I explain above. *See* MTD at 13:21-14:10. Warren's negligence claim may proceed.

VI. UCL CLAIM

[27] The UCL prohibits "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. It "operates as three-pronged statute," where each "captures a separate and distinct theory of liability." *Beaver v. Tarsadia Hotels*, 816 F.3d 1170, 1177 (9th Cir. 2016) (citations and quotations omitted). Warren's complaint alleges violations of all three of the statute's prongs. Compl. ¶ 75.

[28] **[29]** **[30]** The "unlawful" prong of the UCL "incorporate[s] other laws and treats violations of those laws as independently actionable unlawful business practices under state law." *Colgate v. JUUL Labs, Inc.*, 402 F. Supp. 3d 728, 758 (N.D. Cal. 2019) (citation omitted). As a result, "[v]iolation of almost any federal, state, or local law may serve as the basis for a claim under the unlawful prong of the UCL." *Id.* (same). Because Warren has plausibly alleged

violations of the HBOR and RESPA, he has plausibly alleged a violation of the UCL's "unlawful" prong.

[31] **[32]** The "unfair" prong requires proving either: (1) "the public policy which is a predicate to a consumer unfair competition action" is "tethered to specific constitutional, statutory or regulatory provisions," or (2) that the challenged business practice is "immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers." *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1226 (N.D. Cal. 2014) (citations omitted). The complaint does not provide sufficient detail to evaluate Warren's "unfair" UCL claim. Instead, it makes a laundry list of allegations to support its claim that PNC violated all three prongs of the UCL, including many that do not appear to apply to Warren's case. For example, it alleges that PNC used a "purposefully lengthy" loss mitigation review process "so that loss mitigation and loan modification will not be timely provided"; "purposefully caused a lengthy delay in order to cause plaintiffs and borrowers like plaintiffs to incur continuing interest charges that would otherwise be mitigated, late fees, and untimely foreclosure costs"; "purposefully impeded timely loss mitigation denial or approval while expressing that plaintiff are [sic] in review," which "prevents plaintiff from seeking other external loss mitigation options including abandoning the property and/or short sale"; and that "the information provided to plaintiff was certainly misleading and not consistent as to the status of the loan modification and what *she* was supposed to do to satisfy the lender's demands." *See* Compl. ¶¶ 76-78, 84 (emphasis added). But Warren never alleges that he submitted a loan mitigation application or that PNC delayed review of such. *See generally id.* Instead, the essence of his complaint is that PNC *never* provided him information about this process, as required by the law. And the allegations that could support a claim under the "unfair" prong are not clearly tied to a public policy or alleged to be "immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers" to support his claim. *See Adobe Sys.*, 66 F. Supp. 3d at 1226. Put simply, Warren needs to be more specific with his allegations about his "unfair" UCL claim.

***11** **[33]** **[34]** **[35]** The same is true for any claim under the "fraudulent" prong of the UCL, which is subject to Federal Rule of Civil Procedure Rule 9(b)'s heightened standard of pleading. *See Beatty v. PHH Mortg. Corp.*, No. 19-CV-05145-DMR, 2019 WL 6716295, at *14 (N.D. Cal. Dec. 10, 2019). " 'Fraud' is an 'intentional misrepresentation, deceit, or concealment of material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury.' " *See id.* (citing Cal. Civ. Code § 3294(c)(3)). The complaint alleges that PNC acted "purposefully" with regard to the loan modification process—for example, that it "purposefully caused a lengthy delay," and "purposefully impeded timely loss mitigation denial or approval while expressing that plaintiff are [sic] in review." *See* Compl. ¶¶ 77-78. Again, these allegations are not relevant to Warren's underlying case. And the complaint does not appear to allege that PNC acted intentionally when it failed to provide Warren the required information. *See generally.*

Although the UCL claim may proceed as pleaded under the "unlawful" prong based on the predicate violations of the HBOR and RESPA, more is needed to state a UCL claim under the "unfair" or "fraudulent" theories of liability.

CONCLUSION

PNC's motion to dismiss is GRANTED in part and DENIED in part, with leave to amend the deficiencies described above unless otherwise noted. Any amended complaint is due within 20 days of the issuance of this Order.

IT IS SO ORDERED.

All Citations

--- F.Supp.3d ----, 2023 WL 3182952

Footnotes

1 PNC requests that I take notice of four documents related to the property that were each recorded in the Contra Costa County Recorder's Office: (1) the June 15, 2022, notice of default; (2) a substitution of trustee recorded on the same day; (3) the September 21, 2022, notice of trustee's sale; and (4) the deed upon sale. *See* RJN, Exs. 1-4. Courts commonly take notice of such documents. *See, e.g.*, *Mejia v. JPMorgan Chase Bank, N.A.*, No. 21-CV-01351-HSG, 2021 WL 2258710, at *2 (N.D. Cal. June 3, 2021) (taking notice of recorded notice of default, notice of trustee's sale, and trustee's deed upon sale) *Freitas v. Bank of Am. N.A.*, No. C-19-03347-WHA, 2019 WL 5872415, at *3 (N.D. Cal. Nov. 11, 2019) (taking

notice of recorded substitution of trustee, notice of trustee's sale, and trustee's deed upon sale). I will do the same, as these documents are matters of public record not generally subject to dispute, and Warren does not appear to oppose the request. *See* Fed. R. Evid. 201(b). I will also note that the notices of default and of trustee's sale are attached to the complaint as Exhibits C and D. *See* Compl., Exs. C, D.

2 Warren alleged a third HBOR violation in his complaint, of section 2924(a)(1), but conceded it in his opposition. *See* Compl. ¶¶ 23-30; Oppo. [Dkt. No. 22] 5:13-14 ("Plaintiff will cease to pursue a cause of action for violation of Civ. Code § 2924(a)(1)."). His second claim is therefore DISMISSED with prejudice.

3 If this forms the basis of Warren's claim, PNC contends a substitution of trustee was recorded on June 15, 2022. *See* MTD at 9:26-10:1 (citing RJN, Ex. 2).

4 PNC only argues that Warren "does not allege in his complaint that he tendered" the amount he owed, ignoring the allegation in the complaint that he was excused from doing so. *See* MTD at 10:19-28.

5 Because I am dismissing the claim on these grounds, I need not reach PNC's argument that the complaint fails to allege a serious injury. *See* MTD at 11:16-28.

6 The complaint alleges that these are violations of the Truth in Lending Act ("TILA"), which is found beginning at 15 U.S.C. § 1601. *See* Compl. ¶¶ 35-49. Although PNC noted the apparent discrepancy in its motion to dismiss, Warren does not offer any clarification in his opposition. *See* MTD at 14 n.2; Oppo. at 9:9-21. If Warren attempts to plead something other than violations of RESPA and Regulation X in these claims, he should clarify this in an amended complaint.

7 PNC alternatively argues that if Warren indeed asserts a claim under TILA, it is time-barred. *See* MTD at 16:1-22. I need not consider this issue unless Warren clarifies that he in fact brings a claim under TILA rather than RESPA.

End of Document