

BRIEF FOR RESPONDENTS

---

IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

\_\_\_\_\_  
No. 07-1312  
\_\_\_\_\_

NATIONAL CABLE & TELECOMMUNICATIONS  
ASSOCIATION

Petitioner,

v.

FEDERAL COMMUNICATIONS COMMISSION  
AND THE UNITED STATES OF AMERICA

Respondents,  
\_\_\_\_\_

ON PETITION FOR REVIEW OF AN ORDER OF THE  
FEDERAL COMMUNICATIONS COMMISSION  
\_\_\_\_\_

THOMAS O. BARNETT  
ASSISTANT ATTORNEY GENERAL

JAMES J. O'CONNELL, JR.  
DEPUTY ASSISTANT ATTORNEY GENERAL

CATHERINE G. O'SULLIVAN  
NANCY C. GARRISON  
ATTORNEYS

UNITED STATES  
DEPARTMENT OF JUSTICE  
WASHINGTON, D.C. 20530

MATTHEW B. BERRY  
GENERAL COUNSEL

JOSEPH R. PALMORE  
DEPUTY GENERAL COUNSEL

RICHARD K. WELCH  
ACTING DEPUTY ASSOCIATE GENERAL  
COUNSEL

JOEL MARCUS  
COUNSEL

FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554  
(202) 418-1740

---

## **CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES**

### A. Parties and Amici

Before the Court:

National Cable & Telecommunications Association  
Verizon Communications Inc.  
Qwest Communications International Inc.  
Federal Communications Commission  
United States of America

We have been informed that the Electronic Privacy Information Center plans to participate as *amicus curiae*.

Before the Commission:

All parties participating before the Federal Communications Commission are listed in Appendix A of the order on review (JA - ).

### B. Ruling Under Review

*Implementation of the Telecommunications Act of 1996*, Report and Order, 22 FCC Rcd 6972 (2007) (JA ).

### C. Related Cases

The order on review has not been before this Court or any other court.

# TABLE OF CONTENTS

	<u>Page</u>
QUESTIONS PRESENTED.....	1
JURISDICTION .....	2
STATUTES AND REGULATIONS .....	2
COUNTERSTATEMENT .....	2
SUMMARY OF ARGUMENT .....	14
ARGUMENT.....	18
I.    STANDARD OF REVIEW.....	18
II.   THE FIRST AMENDMENT DOES NOT FORBID OPT-IN.....	21
A.   The <i>Trans Union</i> Cases Compel The Conclusion That Opt-In Is Constitutional.....	22
B.   The Opt-In Requirement Survives Intermediate Scrutiny.....	26
1.   The Government Has Substantial Interests In Privacy And In Ensuring That Consumers Knowingly Assume The Risks Of Data Sharing.....	27
2.   Opt-In Furthers The Government’s Interest In Knowing Consent.....	29
a. <i>Opt-In Directly Advances The                   Government’s Interests.</i> .....	30
b. <i>The Government’s Interest Is Real.</i> .....	41
3.   Opt-In Is Sufficiently Tailored.....	45
III.  THE COMMISSION REASONABLY CHANGED FROM AN OPT-OUT TO A LIMITED OPT-IN APPROACH.....	53
CONCLUSION.....	60

## TABLE OF AUTHORITIES

<u>Cases</u>	<u>Page</u>
<i>44 Liquormart, Inc. v. Rhode Island</i> , 517 U.S. 484 (1996) .....	33, 47
<i>Anderson v. Treadwell</i> , 294 F.3d 453 (2d Cir. 2002) .....	20
<i>AT&amp;T v. FCC</i> , 832 F.2d 1285 (D.C. Cir. 1987) .....	55
<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001) .....	34
<i>Bell South Corp. v. FCC</i> , 144 F.3d 58 (D.C. Cir. 1998).....	39, 47
<i>Biloxi Reg'l Med. Ctr. v. Bowen</i> , 835 F.2d 345 (D.C. Cir. 1987).....	56
<i>Blount v. SEC</i> , 61 F.3d 938 (D.C. Cir. 1995) .....	38, 39
<i>Board of Education v. Pico</i> , 457 U.S. 853 (1982) .....	33
* <i>Board of Trustees v. Fox</i> , 492 U.S. 469 (1989) .....	27, 50
<i>Bolger v. Young Drugs Corp.</i> , 463 U.S. 60 (1983).....	34
<i>Carducci v. Regan</i> , 714 F.2d 171 (D.C. Cir. 1983) .....	19
<i>Central Hudson Gas &amp; Elec. Corp. v. Public Service Comm'n of New York</i> , 447 U.S. 557 (1980) .....	6, 19, 26
<i>Century Communications Corp. v. FCC</i> , 835 F.2d 292 (D.C. Cir. 1987) .....	43
<i>City of Cincinnati v. Discovery Network, Inc.</i> , 507 U.S. 410 (1993) .....	32
<i>Consumer Electronics Ass'n v. FCC</i> , 347 F.3d 291 (D.C. Cir. 2003) .....	21
<i>Curtis v. Thompson</i> , 840 F.2d 1291 (7th Cir. 1988).....	34
<i>Destination Ventures, Ltd. v. FCC</i> , 46 F.3d 54 (9th Cir. 1995).....	35
<i>Edenfield v. Fane</i> , 507 U.S. 761 (1993) .....	32
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001) .....	36
* <i>Florida Bar v. Went For It, Inc.</i> , 515 U.S. 618 (1995).....	35, 38, 43, 49
<i>Freeman Eng'g Assocs., Inc. v. FCC</i> , 103 F.3d 169 (D.C. Cir. 1997) .....	57

*Greater New Orleans Broadcasting Ass’n v. United States*, 527 U.S. 173 (1999)..... 33

*In re R.M.J.*, 455 U.S. 191 (1982)..... 27

*Jifry v. FAA*, 370 F.3d 1174 (D.C. Cir. 2004)..... 18

*Kovacs v. Cooper*, 336 U.S. 77 (1949) ..... 47

*Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525 (2001)..... 27

*Mainstream Marketing Services, Inc. v. FTC*, 358 F.3d 1228 (10th Cir. 2004)..... 20, 47

*Martin v. City of Struthers*, 319 U.S. 141 (1943) ..... 34

*MCI WorldCom, Inc. v. FCC*, 209 F.3d 760 (D.C. Cir. 2000) ..... 59

*Melcher v. FCC*, 134 F.3d 1143 (D.C. Cir. 1998) ..... 55

*Melody Music, Inc. v. FCC*, 345 F.2d 730 (D.C. Cir. 1965)..... 57

*Meyer v. Grant*, 486 U.S. 414 (1988) ..... 34

*Missouri ex rel. Nixon v. American Blast Fax, Inc.*, 323 F.3d 649 (8th Cir. 2003)..... 20, 33, 35

*Moser v. FCC*, 46 F.3d 970 (9th Cir. 1995)..... 21

*Motor Vehicle Mfrs. Ass’n of the United States, Inc. v. State Farm Mut. Ins. Co.*, 463 U.S. 29 (1983)..... 21, 54

*National Fuel Gas Supply Corp. v. FERC*, 468 F.3d 831 (D.C. Cir. 2006) ..... 55

*Ohralik v. Ohio State Bar Ass’n*, 436 U.S. 447 (1978)..... 26

*Reytblatt v. U.S. Nuclear Regulatory Comm’n*, 105 F.3d 715 (D.C. Cir. 1997) ..... 59

*Rubin v. Coors Brewing Co.*, 514 U.S. 476 (1995) ..... 33

*Star Wireless, LLC v. FCC*, No. 07-1190 WL 1795596 (D.C. Cir. Apr. 22, 2008) ..... 56

*Tennessee Secondary School Ass’n v. Brentwood Academy*, 127 S. Ct. 2489 (2007)..... 44

*Thompson v. Clark*, 741 F.2d 401 (D.C. Cir. 1984) ..... 59

*Thompson v. Western States Medical Center*, 535 U.S. 357 (2002)..... 19, 20, 33

*Time Warner Enm't Co. v. FCC*, 144 F.3d 75 (D.C. Cir. 1998)..... 57

*Time Warner Entertainment Co. v. FCC*, 240 F.3d 1126  
(D.C. Cir. 2001) ..... 40

\* *Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2001) ..... 15, 20, 22, 23, 27, 38, 39

\* *Trans Union Corp. v. FTC*, 267 F.3d 1138  
(D.C. Cir. 2001) ..... 15, 18, 19, 21, 22, 23, 24, 25, 26, 29, 30, 39, 49, 50

*Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002) ..... 24, 26

*Turner Broadcasting Systems, Inc. v. FCC*, 520 U.S. 180 (1997)..... 24

*U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000) ..... 5, 6, 7, 24, 35

*United States v. Albertini*, 472 U.S. 675 (1985) ..... 49

*United States v. Playboy Entertainment Group, Inc.*,  
529 U.S. 803 (2000)..... 49

*Ward v. Rock Against Racism*, 491 U.S. 781 (1989) ..... 49

**Administrative Decisions**

*AT&T*, 102 FCC 2d 655 (1985) ..... 4

*Implementation of the Telecommunications Act of 1996*, Notice of  
Proposed Rulemaking, 21 FCC Rcd 1782 (2006) ..... 10

*Implementation of the Telecommunications Act of 1996*, Second  
Report and Order, 13 FCC Rcd 8016 (1998)..... 5, 37, 51

*Implementation of the Telecommunications Act of 1996*, Third  
Report and Order, 17 FCC Rcd 14860 (2002)..... 7, 8, 9, 10, 37, 39

**Statutes and Regulations**

5 U.S.C. § 706(2)(A)..... 21

28 U.S.C. § 2342(1) ..... 2

47 U.S.C. § 217..... 40

47 U.S.C. § 222(a) ..... 1, 4

47 U.S.C. § 222(c)(1)..... 1, 21, 30

47 U.S.C. § 222(d) ..... 4

47 U.S.C. § 222(e) ..... 58

47 U.S.C. § 402(a) ..... 2

47 U.S.C. § 405(a) ..... 57

Cable Communications Policy Act, 47 U.S.C. § 551(b)(1)..... 28

Children’s Online Privacy Protection Act,  
15 U.S.C. § 6501(b)(1)(A)(ii)..... 28

Driver’s Privacy Protection Act, 18 U.S.C. § 2721(b)(13)..... 28

Family Educational Rights and Privacy Act,  
20 U.S.C. § 1232g(b)(1) ..... 28

\* Telephone Records and Privacy Protection Act of 2006,  
Pub. L. No. 109-476 § 2(1) & (2) ..... 3

\* Telephone Records and Privacy Protection Act of 2006,  
Pub. L. No. 109-476 § 2(5)..... 3

Video Privacy Protection Act, 18 U.S.C. § 2710(b)(2)(B)..... 28

47 C.F.R. § 64.2007(b)(1) (2002)..... 8, 9

47 C.F.R. § 64.2007(b)(2) (2002)..... 9

47 C.F.R. § 64.2007(b)(3) (2002)..... 8

47 C.F.R. § 64.2007(b) (2007)..... 11

**Others**

Restatement (Third) of Agency § 7.03 (2006)..... 40

Restatement (Third) of Agency § 7.08 (2006)..... 40

\* *Cases and other authorities principally relied upon are marked with asterisks.*

## **GLOSSARY**

CPNI                      Customer Proprietary Network Information. Private, personal information concerning the number called, the duration of the call, and similar information, belonging to a telephone user but disclosed to the carrier in the course of using telephone service.



IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

---

No. 07-1312

---

NATIONAL CABLE & TELECOMMUNICATIONS  
ASSOCIATION

Petitioner,

v.

FEDERAL COMMUNICATIONS COMMISSION  
AND THE UNITED STATES OF AMERICA

Respondents,

---

ON PETITION FOR REVIEW OF AN ORDER OF THE  
FEDERAL COMMUNICATIONS COMMISSION

---

BRIEF FOR RESPONDENTS

---

**QUESTIONS PRESENTED**

Section 222 of the Communications Act imposes a duty on all telecommunications carriers “to protect the confidentiality” of private information they gain about their subscribers by virtue of the subscribers’ use of telecommunications service, which is known as “customer proprietary network information” or CPNI. 47 U.S.C. § 222(a). A carrier may not use or disclose such information in most instances unless it obtains “the approval of the customer.” *Id.* § 222(c)(1).

The two methods for ascertaining customer approval are opt-in (in which approval is express) and opt-out (in which approval is inferred from silence).

The questions presented are:

1. Whether the First Amendment required the Commission to use opt-out for determining customer approval of carrier disclosure of CPNI to joint venture partners and independent contractors?
2. Whether it was arbitrary and capricious for the Commission to change its policy from opt-out approval, which it adopted in 2002, to opt-in approval for information disclosed to joint venture partners and independent contractors?

### **JURISDICTION**

The Court has jurisdiction over final FCC rulemaking orders pursuant to 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1).

### **STATUTES AND REGULATIONS**

Pertinent materials are attached in the appendix.

### **COUNTERSTATEMENT**

Every time a telephone or cell phone user – a category that includes nearly every person in the United States – makes a call, the company that provides service receives personal data about the caller, such as who was called and how long the

conversation lasted. Combined with other data the carrier knows by virtue of its business relationship with the customer, such as the user's address, call plan, and, in the case of cell phone service, location, call data can reveal substantial information about the personal lives of subscribers. One may not avoid revealing that data short of declining to use the telephone (including cell phones), which is hardly an option in modern society. The private, personal information that a telecommunications carrier obtains through the provision of telephone service is known as "customer proprietary network information" or CPNI.

Congress has found that CPNI "can be of great use to criminals because the information contained in call logs may include a wealth of personal data," such as "the names of telephone users' doctors, public and private relationships, business associates, and more." Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476 §§ 2(1) & (2). "[T]he unauthorized disclosure of telephone records 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." *Id.* § 2(5).

1. *Section 222 and the 1998 CPNI Order.*

The FCC understandably has long been concerned about the misuse of such private data. More than 20 years ago, the agency ruled that “this information belongs to the customers,” not the phone company, and it restricted phone companies’ use of CPNI. *AT&T*, 102 FCC 2d 655 (1985).

In 1996, Congress imposed a direct statutory restriction on carriers’ use and disclosure of CPNI. Congress imposed on “[e]very telecommunications carrier” a “duty to protect the confidentiality of proprietary information of ... customers.” To effectuate that mandate, Congress forbade carriers’ use or disclosure of CPNI “[e]xcept as required by law or with the approval of the customer.” 47 U.S.C. §§ 222(a), (c)(1) (the statute contains other exceptions not at issue here, *see* § 222(d)).

Congress did not, however, define how a customer was to manifest “approval” for the use or disclosure of its CPNI. There are only two basic methods of ascertaining customer assent: (1) to presume that a customer approves unless he specifies otherwise (the opt-out approach); or (2) to require a customer to affirmatively indicate approval (the opt-in approach).

In its first rulemaking order interpreting the statute, the Commission determined that opt-in best reflected Congress’s intent. The Commission reiterated that CPNI “is better understood as belonging to the customer, not the carrier.”

*Implementation of the Telecommunications Act of 1996*, Second Report and Order, 13 FCC Rcd 8016, 8093 (1998) (*1998 CPNI Order*). It then explained that the “natural, common sense understanding of the term ‘approval’ ... generally connotes an informed and deliberate response,” and “express approval [by opt-in] best insures such a knowing response.” *Id.* at 8130. By contrast, “under an opt-out approach ... because customers may not read their CPNI notices, there is no assurance that any implied consent would be truly informed. ... We therefore find it difficult to construe a customer’s failure to respond to a notice as constituting an informed approval of its contents.” *Id.* at 8130-8131. The Commission accordingly required carriers to obtain opt-in consent before they disclosed CPNI to any third party.<sup>1</sup>

## 2. *The Tenth Circuit’s U.S. West Decision.*

A divided panel of the Tenth Circuit vacated the Commission’s implementation of opt-in. *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000). The panel did not address whether opt-in was

---

<sup>1</sup> The Commission found that customer approval could be inferred from the existing carrier-customer relationship for certain uses of CPNI by the carrier itself. *1998 CPNI Order* at 8080. The Commission thus crafted what it called a “total service approach” under which a carrier could, without notice to the customer, use CPNI to market new services incidental to the service already being provided (such as caller ID marketed to an existing local service customer). *Id.* at 8081 *et seq.* The total service approach did not extend to disclosure of CPNI beyond the carrier itself.

a reasonable interpretation of the statute, but, applying the test for restrictions on commercial speech set forth in *Central Hudson Gas & Elec. Corp. v. Public Service Comm'n of New York*, 447 U.S. 557 (1980), the panel majority held that opt-in violated the First Amendment.

The opinion expressed considerable doubt that the government had any interest at all in protecting the privacy of telephone subscriber data: “A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest ....” 182 F.3d at 1235.

Although the panel majority ultimately decided to “assume for the sake of this appeal” that the government has a substantial interest in protecting the privacy of CPNI, it held that opt-in did not advance that interest because of a lack of “evidence showing the harm to ... privacy ... is real. Instead, the government relies on speculation that harm to privacy ... will result if carriers use CPNI.” 182 F.3d at 1237. The panel majority also held that the FCC had “fail[ed] to adequately consider an obvious and substantially less restrictive alternative, an opt-out strategy.” *Id.* at 1238.

The dissenting judge would have held that the case presented no serious constitutional question. Any restriction on speech was attributable to the statute itself and not to the FCC’s choice of opt-in – yet the statutory restriction was not

under challenge. 182 F.3d at 1243 (Briscoe, J., dissenting). Thus, “nothing warrants First Amendment scrutiny.” *Ibid.*

Applying the *Central Hudson* test for purposes of argument, however, Judge Briscoe concluded that the statute and opt-in were constitutional. In her view, “Supreme Court and circuit precedent clearly suppor[t] the conclusion that [privacy] interests are ‘substantial,’” and opt-in “directly promotes the goal of protecting consumer privacy.” 182 F.3d at 1244. Furthermore, opt-in is narrowly tailored; because “of the limited options available to the FCC, the opt-in method ... was the most reasonable solution.” Opt-out, by contrast, “did not ensure that the Congressional goal of informed customer consent would be satisfied.” *Id.* at 1246.

### 3. *The 2002 CPNI Order.*

Cognizant of the Tenth Circuit’s objections to the opt-in approach and the lack of evidence on the record at that time of concrete harms caused by disclosure of CPNI, the Commission on remand adopted the only other alternative – opt-out – for both a carrier’s own use of CPNI for marketing purposes and for disclosures of CPNI to third parties for those purposes. *Implementation of the Telecommunications Act of 1996*, Third Report and Order, 17 FCC Rcd 14860, 14874 (2002) (*2002 CPNI Order*) (“in light of *U.S. West* we now conclude that an opt-in rule ... cannot be justified based on the record”). The Commission retained

opt-in only for disclosures to third parties for purposes other than marketing communications-related services. *See* 47 C.F.R. §§ 64.2007(b)(1), (3) (2002).

The record showed that many customers remained concerned about the use and disclosure of their data. More than half the respondents in one survey “expressed some level of concern with use of CPNI” and 36 percent of customers in another study deemed it “not acceptable” for the phone company to use private data. 17 FCC Rcd at 14875. The Commission determined, however, that, with respect to a carrier’s own use of data, “a majority of customers want to be advised of service offerings from their carriers.” The agency accordingly found that opt-out “advances customers’ interests in avoiding unexpected and unwanted use and disclosure of CPNI and is sufficient to meet the ‘approval’ requirement” of section 222. *Id.* at 14877.

The Commission expressed concern about disclosure of CPNI beyond the immediate control of the carrier itself. The record showed that public concern was “most acute for disclosure to parties other than their own carrier.” 17 FCC Rcd at 14876. Nevertheless, in light of the Commission’s assessment of consumer expectations about the use of CPNI, the Commission deemed opt-out sufficiently protective of customers’ privacy interests. For purposes of marketing telecommunications-related services, the agency “extended [opt-out] treatment to all agency relationships,” to affiliates, and to third parties without agency



relationships, such as independent contractors that conduct marketing operations and joint venture partners. *Id.* at 14881; *see* 47 C.F.R. § 64.2007(b)(1) (2002).

The Commission implemented various safeguards on disclosure to joint venture partners and independent contractors, such as mandatory confidentiality agreements, in an attempt to protect CPNI “from further dissemination or uses beyond those consented to by the customer.” *Ibid.* *See* 47 C.F.R. § 64.2007(b)(2) (2002),

Notwithstanding its decision regarding disclosure to third parties for the purpose of marketing communications-related services, however, the Commission continued to require opt-in for disclosure of CPNI to third parties for other purposes. “[T]he record unequivocally demonstrates that, in contrast to intra-company use and disclosure of CPNI, there is a more substantial privacy interest with respect to third-party disclosures. The record indicates not only that consumers’ wishes are different regarding third-party disclosure, but that the privacy consequences are more significant in the case of unintended disclosure to third parties.” 17 FCC Rcd at 14883. Survey data showed that “consumers view use of CPNI by a consumer’s carrier differently than disclosure to or use by a third party,” and that 73 percent of consumers favored barring third-party disclosure. *Id.* at 14884. The Commission was further concerned that allowing entities not directly subject to section 222 and without any direct relationship with – and no

accountability to – the customer would increase the threat to privacy. *Id.* at 14884-14885.

#### 4. *The 2007 CPNI Order.*

Three years later, the Electronic Privacy Information Center (EPIC) filed a petition for rulemaking in which it reported to the Commission serious problems with the privacy of CPNI data. For example, EPIC described “data brokers” who, for a fee, could provide telephone call records and other private data, including location tracking of cell phone users, often within a few hours. *See* EPIC Petition at 5-6, 8-10 (JA - , - ).

In response to the EPIC petition, the Commission issued a notice of proposed rulemaking in which it sought comment on the matters raised by EPIC. The notice expressly asked for public input on the question whether the Commission should change the opt-out regime for disclosure to independent contractors and joint venture partners. *Implementation of the Telecommunications Act of 1996*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1788 (2006).

After receiving comments, the Commission issued the order on review, *Implementation of the Telecommunications Act of 1996*, Report and Order, 22 FCC Rcd 6972 (2007) (*2007 CPNI Order*) (JA ). The Commission concluded that “[t]he 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.” *Id.* ¶12 (JA ). Especially problematic was “pretexting,” where a data broker pretends to be a customer and obtains CPNI based on that fraudulent representation. In recent years, state Attorneys General, telephone carriers, and the Federal Trade Commission had all filed suits to block pretexters, *2007 CPNI Order* ¶12 (JA ), and Congress passed the Telephone Records And Privacy Protection Act to make the sale of CPNI records a crime.

The Commission took several steps in response to the problems. First, to combat pretexting, the Commission restricted disclosure of CPNI over the telephone and required passwords to be used in customer-initiated calls seeking CPNI information. *2007 CPNI Order* ¶¶15-17 JA - ). The Commission required passwords for on-line access to telephone account information. *Id.* ¶¶20-22 (JA - ). The Commission also adopted a number of notification requirements for changes in account status and unauthorized disclosures of CPNI. *Id.* 24, 26-32 (JA , - ).

Second, the Commission changed its rules to require opt-in for carrier disclosure for the purpose of marketing communications-related services to any third party other than “agents” and “affiliates that provide communications-related services.” 47 C.F.R. § 64.2007(b) (2007). In practical terms, the new rule requires opt-in for joint venture partners and independent marketing contractors. The Commission acknowledged that it was changing its policy and explained the

reasons for doing so. It found that “[n]ew circumstances” – the growing illicit demand for personal information, the significant harm that can result from breaches of confidentiality, and the increasing risk of disclosure – “force us to reassess our existing regulations.” *2007 CPNI Order* ¶37 (JA ).

The Commission identified several new risks that had emerged since the *2002 CPNI Order*. “The black market for CPNI has grown exponentially with an increased market value placed on obtaining this data,” the Commission found. *2007 CPNI Order* ¶39 (JA ). Moreover, “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 data to assume a customer’s identity.” *Ibid.* Indeed, Congress had made express legislative findings of such harm, *see p.3 supra*, and the administrative record told of an information broker who sold a detective’s pager number to a mafia member who was trying to determine the identity of an informant. *Id.* n.31 (JA ).

The Commission also expressed concern with the efficacy of opt-out notices. “[C]urrent opt-out notices ... are often vague and not comprehensible to the average customer.” *2007 CPNI Order* ¶40 (JA ). Studies revealed “consumer confusion” on the matter, *ibid.*, demonstrating, according to comments submitted by a coalition of state Attorneys General, that “customers are unlikely to read opt-

out notices and therefore [do] not know that they are giving affirmative consent to share their information,” *id.* n.128 (JA ).

The Commission reiterated its concerns about the disclosure of data to third parties, first articulated in the *2002 CPNI Order*. “It stands to reason that placing customers’ personal data in the hand of companies outside the carrier-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.” *2007 CPNI Order* ¶41 (JA ). “[I]t is axiomatic that the more companies that have access to CPNI, the greater the risk of unauthorized disclosure .... 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.” *Id.* ¶46 (JA ).

The Commission found that neither contracts between carriers and third parties governing use of CPNI nor market forces reduced to a tolerable degree the risk and consequences of disclosure. “[I]n the event of a breach,” the Commission determined, “the damage is already inflicted upon the customer.” *2007 CPNI Order* ¶42 (JA ). “[T]he 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.” *Ibid.*

The combination of those increased risks and consequences led the Commission to reevaluate the need to protect consumers' private information given consumers' expectations of privacy with respect to disclosure of private data to independent contractors and joint venture partners 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." *2007 CPNI Order* ¶45 (JA ). Put another way, "before the chances of unauthorized disclosure are increased, a customer's explicit consent should be required." *Id.* ¶46 (JA ). The Commission accordingly adopted an opt-in rule for carrier disclosure of CPNI to independent contractors and joint venture partners for marketing purposes.

### **SUMMARY OF ARGUMENT**

The disclosure of a telephone subscriber's personal private calling information can cause substantial harm, ranging from invasion of privacy, to harassment, to interference with police investigations. There is a vigorous black market for such information, and the consequences for those whose data security is breached can be severe. In section 222, Congress accordingly has undertaken to

protect the privacy of CPNI by directing that consumers, to whom the data belong, must give their approval before a carrier uses or discloses CPNI data.

1. This Court's decision in *Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2001), and its opinion denying rehearing in that case, 267 F.3d 1138 (D.C. Cir. 2001), control the analysis of this case. There, the Court confronted a statutory scheme to protect the confidentiality of private consumer data through opt-in that was functionally identical to the one at issue here for purposes of constitutional examination. The Court easily held the arrangement to be consistent with the First Amendment. The protection of private financial data "unquestionably advances" the government's substantial interest in protecting privacy, the Court held, and that interest cannot be promoted "except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent." 267 F.3d at 1142. Congress was not required to use opt-out rather than opt-in because intermediate scrutiny – the applicable constitutional standard – does mandate an alternative solution that "is marginally less intrusive on a speaker's First Amendment interests." *Id.* at 1143. The *Trans Union* analysis applies foursquare here. Petitioner has failed utterly to distinguish the case; intervenors have not even tried.

2. Even if *Trans Union* did not control the outcome here, the FCC's use of opt-in was constitutional under intermediate scrutiny. Opt-in satisfies all of the

intermediate scrutiny factors. The government obviously has a substantial interest in both the protection of CPNI and in ensuring that consumers knowingly consent to the disclosure of their private information. Opt-in also directly furthers those interests. As with the credit information at issue in *Trans Union*, the government cannot protect the privacy of information except by regulating its disclosure. Opt-in also directly ensures that a customer is aware of the potential disclosure of private information and consents to its release. Opt-out, the only other possibility, does not ensure that a consumer has knowingly chosen to assume the risks. The Commission's opt-in regime is proportional to the interests it serves in light of its limited scope and the multiple means by which carriers may reach customers.

Petitioner's arguments to the contrary are not well founded. Its principal claim – that opt-in does nothing to further the government's interest in preventing breaches of data security – misses the mark. The Commission's interest in opt-in is not only reducing data breaches, but also ensuring that consumers accept the increased risk of a breach that results when data is shared beyond the carrier. Petitioner's claim that no additional risk accrues from sharing CPNI with third parties is also wrong. It is a matter of common sense that increasing the number of companies that have access to data increases the vulnerability of the data to disclosure – whether by accident, such as a laptop left on the subway; on purpose, by a corrupt employee; or by other means, such as computer hacking or pretexting.



Private contracts between carriers and their independent contractors and joint venture partners are not sufficient to eliminate the risk. They can be enforced only after a breach, and then it is too late. Indeed, the carriers themselves, who are directly accountable to customers and directly subject to section 222, have had trouble protecting the security of data.

This case is fundamentally different from the precedents relied on by petitioner. Most of those cases involved flat prohibitions on speech, in some cases core political speech, and in most instances with no alternative avenues of communication; none of them involved the commercial use of private data. In many of the commercial speech cases on which petitioner relies, the speech bans served to keep consumers in the dark by withholding relevant information. Such cases plainly have no bearing here. Other cases, not cited by petitioner, show that where commercial speech conflicts with consumer privacy interests, privacy typically prevails.

Petitioner is also wrong that opt-in is insufficiently tailored. Opt-in imposes a minimal burden on petitioner's communications. It does not regulate the content of carriers' marketing messages, and carriers have multiple means to market services to all their customers, including those customers who choose not to permit disclosure of their private data. The small burden on speech is proportional to the significant interests furthered by the limited opt-in approach. As this Court held in

*Trans Union*, opt-out is only “marginally less intrusive” than opt-in. 267 F.3d at 1143. More informative opt-out notices, petitioner’s proposed solution, are no cure for the problem because even the best opt-out notice is of no use to the consumer who fails to read it, a common occurrence given most people’s busy lives.

4. Petitioner’s administrative law claims also fail. The FCC reasonably changed its regulatory approach in light of new information that demonstrated the existence of a black market in CPNI data and the severe consequences of a data breach. Petitioner’s claim that the Commission failed to respond to comments that opt-in would impose competitive harm on small carriers lacks merit. Petitioner has waived that argument by failing to raise it before the agency. On the merits, the claim fails because (as petitioner’s own intervenors agree) the opt-in requirement applies equally to all companies, and no company is treated differently. Moreover, an agency is required to respond only to the most important and fundamental comments, which on the record here did not include those regarding competitive harm.

## **ARGUMENT**

### **I. STANDARD OF REVIEW.**

The constitutionality of the Commission’s decision is reviewed *de novo*. *Jifry v. FAA*, 370 F.3d 1174, 1182 (D.C. Cir. 2004). Under intermediate scrutiny, a

regulation of commercial speech is valid as long as it implements a substantial governmental interest, directly advances that interest, and is narrowly tailored to serve that interest. *Central Hudson*, 447 U.S. at 563-566. In addition, this Court has held that “private speech” – such as that between petitioners and their joint venture partners – “warrant[s] only the qualified constitutional protection” of intermediate scrutiny. *Trans Union Corp. v. FTC*, 267 F.3d 1138, 1141 (D.C. Cir. 2001).

Petitioner makes a passing attempt to claim that this case presents a content-based restriction subject to strict scrutiny, Br. 25-26, but it ultimately does not actually argue as much, and, as petitioner acknowledges, the Court need not take up the issue. Br. 26 (“The Court need not resolve that issue”); *see Carducci v. Regan*, 714 F.2d 171, 177 (D.C. Cir. 1983) (Court will not address an “asserted but unanalyzed” argument). Even if section 222 were content-based, however, intermediate scrutiny would still apply. *See Trans Union*, 267 F.3d at 1141 (“[G]iven the Supreme Court’s commercial speech doctrine, which creates a category of speech defined by content but afforded only qualified protection, the fact that a restriction is content-based cannot alone trigger strict scrutiny.”); *Thompson v. Western States Medical Center*, 535 U.S. 357 (2002) (applying *Central Hudson* to a content-based restriction on commercial speech).

Petitioner also implies that restrictions on commercial speech are never upheld and argues that “a majority of Justices presently on the Court has now suggested ... that truthful and non-misleading commercial speech may be entitled to greater protection than afforded under intermediate scrutiny.” Br. 27. But petitioner then immediately backs off the subject. Br. 28 (“this Court need not decide the issue”). The Supreme Court has not, however, overruled *Central Hudson*; to the contrary, in *Thompson*, the Supreme Court acknowledged the various views of individual justices and found “no need ... to break new ground.” 535 U.S. at 367-368.

Furthermore, notwithstanding petitioner’s string cite of Supreme Court cases striking down commercial speech restrictions, none of which involved the protection of personal privacy from commercial exploitation, numerous courts of appeals, including this Court, recently have upheld such restrictions against First Amendment challenges where personal privacy is at stake. *See, e.g., Mainstream Marketing Services, Inc. v. FTC*, 358 F.3d 1228 (10th Cir. 2004) (upholding do-not-call list); *Missouri ex rel. Nixon v. American Blast Fax, Inc.*, 323 F.3d 649 (8th Cir. 2003) (upholding ban on unsolicited faxes); *Anderson v. Treadwell*, 294 F.3d 453 (2d Cir. 2002) (upholding ban on real estate solicitation); *Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2001); *Trans Union Corp. v. FTC*, 267 F.3d 1138

(D.C. Cir. 2001) (upholding ban on sharing of financial data); *Moser v. FCC*, 46 F.3d 970, 975 (9th Cir. 1995) (upholding ban on telemarketing calls).

Petitioner’s administrative law claim is subject to the traditional highly deferential standard of review for such claims. The Court “presume[s] the validity of the Commission’s action and will not intervene unless the Commission failed to consider relevant factors or made a manifest error in judgment.” *Consumer Electronics Ass’n v. FCC*, 347 F.3d 291, 300 (D.C. Cir. 2003). It may reverse only if the agency’s decision is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law,” 5 U.S.C. § 706(2)(A). The agency may change its regulatory approach “with or without a change in circumstances,” as long as it provides “a reasoned analysis” for doing so. *Motor Vehicle Mfrs. Ass’n of the United States, Inc. v. State Farm Mut. Ins. Co.*, 463 U.S. 29, 57 (1983) (quotation marks omitted). The Court may not “substitute its judgment for that of the agency.” *State Farm*, 463 U.S. at 43.

## **II. THE FIRST AMENDMENT DOES NOT FORBID OPT-IN.**

The First Amendment challenge here is highly limited. Petitioner does not claim that section 222 is unconstitutional, and it therefore must be taken as a given that the First Amendment allows the government to forbid a telecommunications carrier to “use, disclose, or permit access to” a customer’s CPNI without the “approval of the customer.” 47 U.S.C. § 222(c)(1). Petitioner challenges only the

Commission's determination of what type of customer "approval" best effectuates the statute when a carrier wants to share a customer's private information with an independent contractor or joint venture partner. As this Court has recently ruled, however, the difference between opt-in and opt-out is not significant under the First Amendment.

**A. The *Trans Union* Cases Compel The Conclusion That Opt-In Is Constitutional.**

In circumstances very similar to those here, this Court has recently held that the First Amendment did not prohibit Congress from requiring a financial reporting company to obtain customer opt-in approval before it could disclose the customer's personal financial information for marketing purposes. The Court's decision in *Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2001), and its opinion denying rehearing, *Trans Union Corp. v. FTC*, 267 F.3d 1138 (D.C. Cir. 2001), considered a statutory scheme functionally identical for purposes of the constitutional analysis to the one at issue here and compel the conclusion that the FCC's adoption of opt-in is constitutional.

*Trans Union* involved a challenge to the Fair Credit Reporting Act, which bars consumer reporting agencies from selling reports, compiled from confidential financial information and listing the names and addresses of individuals who met certain financial profiles, unless the subject of the information opted in to its release. *Trans Union*, a consumer reporting agency, wanted to sell such reports to

outside entities so that they could engage in targeted marketing very similar to the marketing at issue here. It challenged the statute, arguing that it “violates the free speech guarantee of the First Amendment because it restricts the company’s ability to disseminate information.” 245 F.3d at 817.

Applying intermediate scrutiny, the Court disposed easily of Trans Union’s claim that the restriction on the sale of targeted marketing lists violated the First Amendment. The Court “had no doubt that [the government’s] interest – protecting the privacy of consumer credit information – is substantial,” and that the ban furthered that interest. 245 F.3d at 818. The Court next rejected the claim that Congress was required to use an opt-out approach as a less restrictive alternative. “Because the FCRA is not subject to strict First Amendment scrutiny, ... Congress had no obligation to choose the least restrictive means of accomplishing its goal.” *Id.* at 819. The Court also rejected Trans Union’s claim that the statute is underinclusive because it applies only to some companies that sell consumer information and not to others that also sell such information. *Ibid.*

Disposing of a petition for panel rehearing, the Court strongly affirmed its earlier conclusions. It noted that “private speech,” such as the transmittal of personal financial data, is entitled to “only qualified constitutional protection” and “merits only intermediate scrutiny.” 267 F.3d at 1141. Again applying that test, the Court held that the prohibition of the sale of personal financial data

“unquestionably advances the identified state interest” in protecting citizens’ privacy. *Id.* at 1142. “[T]he government cannot promote its interest (protection of personal financial data) except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent.” *Ibid.*

The Court also addressed again the question of opt-in versus opt-out:

“Although the opt-in scheme may limit more Trans Union speech than would the opt-out scheme the company prefers, intermediate scrutiny does not obligate courts to invalidate a ‘remedial scheme because some alternative solution is marginally less intrusive on a speaker’s First Amendment interests.’” 267 F.3d at 1143, quoting *Turner Broadcasting Systems, Inc. v. FCC*, 520 U.S. 180, 217-218 (1997). “A regulation is not ... invalid simply because a court concludes that the government’s interest could be adequately served by some less-speech-restrictive alternative.” 267 F.3d at 1143, quoting *Turner*, 520 U.S. at 218.

In a subsequent case, also involving Trans Union, but arising under a different statute, the Court again confronted the question of opt-in versus opt-out, and held that opt-out “is not significantly narrower” than opt-in. *Trans Union LLC v. FTC*, 295 F.3d 42, 53 (D.C. Cir. 2002).<sup>2</sup>

---

<sup>2</sup> In that sense, the *Trans Union* cases are consistent with the view of the dissenting Judge in *U.S. West*, who would have held that opt-in “does not ... directly impact a carrier’s expressive activity.” 182 F.3d at 1244 (Briscoe, J., dissenting).



The *Trans Union* decisions control the outcome here. The governmental programs at issue in both cases involve a statute and regulations designed to protect the privacy of sensitive personal information by restricting the disclosure of that information to third parties for marketing purposes. Both programs allow disclosure only if the owner of the information affirmatively acts to authorize its release.<sup>3</sup> Accordingly, under *Trans Union*, the CPNI rules clearly survive intermediate scrutiny.

Petitioner makes a cursory attempt in a footnote to distinguish *Trans Union*, but it fails (intervenors do not even try). Footnote 19 of petitioner's brief asserts that the statute at issue in *Trans Union* is "entirely different" from section 222, but petitioner omits completely an explanation of any material difference – of which for purposes of the constitutional analysis there is none. It also asserts that the Court did not apply *Central Hudson*, Br. 61 n.19, but it is obvious, particularly from the rehearing opinion (which petitioner ignores) that the Court treated the matter as a commercial speech case and correctly applied intermediate scrutiny; the Court cited numerous commercial speech decisions. *See* 267 F.3d at 1142.

Finally, petitioner claims that the Court lacked "the benefit of [the Supreme

---

<sup>3</sup> Indeed, the FCRA's restriction is broader than section 222 because *Trans Union* had no other way of engaging in its desired speech, whereas telecommunications carriers may continue to communicate with their customers in multiple ways, and may engage in targeted marketing using customer CPNI as long as the information is not disclosed to joint venture partners or independent contractors.

Court's decision in] *Thompson*," but *Thompson* did not involve the disclosure of private consumer information and has little bearing here. Moreover, petitioner fails to note that the *Trans Union* rehearing opinion was issued after *Thompson*, as was the subsequent *Trans Union* case, which followed the same analysis and cited *Thompson*, *Trans Union, LLC*, 295 F.3d at 53.

**B. The Opt-In Requirement Survives Intermediate Scrutiny.**

Because *Trans Union* controls the outcome of this case, the Court need not proceed further. But even if the *Trans Union* opinions did not dictate the result here, the opt-in requirement for CPNI data disclosed to third parties would be constitutional under intermediate scrutiny.

"[P]rivate speech," such as that between petitioners and their joint venture partners, "warrant[s] only qualified constitutional protection." *Trans Union*, 267 F.3d at 1141. Commercial speech, such as petitioner's members' marketing messages to customers, likewise occupies a "subordinate position ... in the scale of First Amendment values." *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 456 (1978). As a result, the First Amendment permits regulation of commercial speech as long as the restriction directly advances a substantial government interest and is narrowly tailored to serve that interest. *Central Hudson*, 447 U.S. at 563-566. That test does not require the government to employ "the least restrictive means" of regulation or to achieve a perfect fit between means and ends. *Board of*

*Trustees v. Fox*, 492 U.S. 469, 480 (1989). Rather, it is sufficient that there be a “reasonable” fit that is “in proportion to the interest served.” *Ibid.* (quoting *In re R.M.J.*, 455 U.S. 191, 203 (1982)); accord *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 556 (2001). Opt-in, to the degree it restricts speech at all, meets that test.

**1. The Government Has Substantial Interests In Privacy And In Ensuring That Consumers Knowingly Assume The Risks Of Data Sharing.**

The protection of private CPNI data obviously is a substantial governmental interest, *cf. Trans Union*, 245 F.3d at 818 (“we have no doubt that this interest – protecting the privacy of consumer credit information – is substantial”), and petitioner does not seriously contend otherwise.<sup>4</sup> As a corollary to the interest in privacy, the government also plainly has a substantial interest in ensuring that telecommunications customers knowingly accept the risks entailed by disclosure of their CPNI data in the current environment. Knowing consent to the sharing of

---

<sup>4</sup> Petitioner intimates that “there is good reason to question” the substantiality of the privacy interest, but then “does not argue otherwise.” Br. 28-29. Petitioner’s suggestion that consumers lose any privacy interest in their telephone call records because they “voluntarily disclosed” that information (Br. 29) is quite wrong. Citizens “voluntarily disclose” medical information to their doctors, financial information to their banks, and other deeply personal information to their therapists and clergymen, but there is a societal consensus that such matters deserve government protection from commercial disclosure and usage. That information is “lawfully acquired” does not mean that it is entitled to no protection.

data was the very point of Congress's requirement in section 222 that carriers obtain customer approval before using or sharing their data.

The substantiality of the government's interest in preserving the privacy of personal data through knowing consent has been demonstrated repeatedly in congressional attempts to protect the private information of citizens. In recent years, opt-in prior to the release of personal information has been adopted by Congress in the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(b)(1); the Cable Communications Policy Act, 47 U.S.C. § 551(b)(1); the Video Privacy Protection Act, 18 U.S.C. § 2710(b)(2)(B); the Driver's Privacy Protection Act, 18 U.S.C. § 2721(b)(13); and the Children's Online Privacy Protection Act, 15 U.S.C. § 6501(b)(1)(A)(ii). Those statutes reflect Congress's repeated recognition of the government's powerful interest in ensuring that consumers knowingly and affirmatively approve of the disclosure of their private information. Petitioner seemingly would have all such statutes declared unconstitutional. Br. 39 n.12.<sup>5</sup>

---

<sup>5</sup> The number of statutes requiring opt-in, along with section 222 itself, demonstrate that opt-in is not, as petitioner wrongly asserts, an instance of "the agency's paternalism." Br. 47. To the contrary, opt-in ensures that citizens freely choose to forego protection of their private data, and such an enhancement of individual autonomy is hardly "paternalistic."

## 2. Opt-In Furthers The Government's Interest In Knowing Consent.

The statutory restriction on disclosure of CPNI and the opt-in approach directly advance the governmental interests in privacy and knowing consent. As with the credit information at issue in *Trans Union*, the government cannot protect personal, private CPNI data except by regulating its disclosure, because the disclosure itself violates the privacy the government seeks to protect. *See Trans Union*, 267 F.3d at 1142. Opt-in directly ensures that a customer is aware of the potential disclosure of private personal information to the phone company's independent contractor or joint venture partner and consents to such release. Moreover, “[i]n 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.” *2007 CPNI Order* ¶45 (JA ). Opt-in also will “force carriers to provide clear and comprehensible notices to their customers in order to gain their express authorization.” *Id.* ¶41 (JA ). Opt-out, the only other practical possibility, does not ensure to the same degree that a consumer has knowingly chosen to assume the risks.

Petitioner argues that opt-in does not further the government's interests for two reasons: first, because opt-in will not directly protect against disclosure of

CPNI (Br. 33-36); and second, because the government has not proven that its concerns about data security are real (Br. 36-44).

a. *Opt-In Directly Advances The Government's Interests.*

Petitioner's argument that the government's interests are not advanced by opt-in boils down largely to its contention that opt-in "is not a sufficiently direct way to pursue the Commission's objective of protecting consumers from unauthorized disclosure." Br. 34. *See* Br. 36 (FCC "fail[ed] to provide any evidence that [opt-in] will have any effect on the incidence of unauthorized disclosure"); Int. Br. 20 (FCC action will not "materially advance[e] its legitimate effort to thwart pretexters"). The argument fails for two reasons.

First, the argument fails because it overlooks a disclosure that unquestionably takes place: that by the telecommunications carrier to its joint venture partner or independent contractor. The statute prohibits such "disclos[ure]" without "the approval of the customer." 47 U.S.C. § 222(c)(1). A rule requiring that a customer explicitly consent to such disclosure is an obvious and direct advancement of the government's interest in preventing the unapproved dissemination of private information. *See Trans Union*, 267 F.3d at 1142 ("the government cannot promote its interest (protection of personal financial data) except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent. Thus, the FCRA

unquestionably advances the identified state interest.”). That interest is advanced even if there were no risk of further disclosure or data breach by the independent contractor or joint venture partner.

Second, petitioner’s contention that opt-in does not directly advance the interest in preventing (other) unauthorized disclosures addresses the wrong issue. In switching from opt-out to opt-in, the Commission’s main concern was not only reducing the incidence of data breaches, but also ensuring that consumers were affirmatively agreeing to accept the risk of a breach by a third party. *2007 CPNI Order* ¶45 (“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”) (JA ); *id.* ¶48 (“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”) (JA ). Requiring affirmative consumer assent directly achieves that goal – and does so more effectively than presuming that consumers consent unless they take the initiative to indicate otherwise.

Moreover, even if the only point of opt-in had been to reduce unauthorized data disclosures, the risks identified by the Commission were not limited to pretexters. Rather, “the rules we are adopting are designed to curtail *all* forms of unauthorized disclosure of CPNI, not just pretexting.” *2007 CPNI Order* ¶46 (JA

). That category includes not only “inappropriate handling” of CPNI but also “innocent mishandling or loss.” *Id.* ¶41 (JA ).

None of petitioner’s cases addresses a situation remotely akin to this one. *Edenfield v. Fane*, 507 U.S. 761 (1993), one of petitioner’s principal citations, involved a state rule that forbade accountants from soliciting new clients in person. The asserted reason for the regulation was to reduce fraud and other forms of deception. 507 U.S. at 768. The Court held that the state had failed to show that the rule would in fact help reduce fraud; therefore, the rule would not directly promote the state’s interest. 507 U.S. at 771-772. Here, by contrast, the government’s interest in ensuring that customers knowingly assume the risk involving in disclosing private data is directly advanced by opt-in – and opt-out, the only other option, would not advance that interest as effectively because it does not ensure that customers knowingly accept an increase in risk. Moreover, also unlike *Edenfield*, carriers are free to market their services to consumers by any method they see fit (including targeted marketing if customers consent). They simply may not disclose to certain third parties private information owned by the customer in the absence of consent. *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410 (1993), is similarly inapposite because the regulation on commercial speech at issue failed to achieve the government’s objectives. *Id.* 425-426.



Intervenors cite *Board of Education v. Pico*, 457 U.S. 853 (1982), for the proposition that opt-in raises significant constitutional problems. But that case involved banning books from public school libraries and had nothing to do with the commercial use of private information. Moreover, *Pico* and similar cases involve “opt-in” schemes very different from those at issue here, in which all speech, such as the availability of a book, was banned unless a person expressly requested it.

Petitioner’s other principal cases, *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484 (1996); *Rubin v. Coors Brewing Co.*, 514 U.S. 476 (1995); and *Greater New Orleans Broadcasting Ass’n v. United States*, 527 U.S. 173 (1999), are likewise inapposite. Those cases involved statutes that “banned dissemination of truthful commercial information, either to prevent members of the public from making bad decisions with the information . . . or to advance a governmental interest that could be furthered without regulating speech.” *American Blast Fax*, 323 F.3d at 659 (citations and quotation marks omitted). *See, e.g., Thompson*, 535 U.S. at 377 (Thomas, J., concurring) (“the asserted [government] interest is one that is to be achieved through keeping would-be recipients of the speech in the dark”); *44 Liquormart*, 517 U.S. 484, 503 (1996) (opinion of Stevens, J.) (“The First Amendment directs us to be especially skeptical of regulations that seek to keep people in the dark for what the government perceives to be their own good.”). The government interest here is in securing knowing and adequate customer

consent to the use of their own private data in an environment of increased threats to privacy. That interest cannot be fully achieved without presuming that consumers do not consent unless they affirmatively indicate otherwise. Carriers remain free to convey any marketing information of their choice to their customers, and no consumer is “kept in the dark” by the Commission’s order.<sup>6</sup>

Indeed, if the cases show anything, it is not that, as petitioner claims, commercial speech restrictions are typically struck down, but that when commercial speech impinges on privacy, privacy wins. *See, e.g., Curtis v. Thompson*, 840 F.2d 1291, 1300 (7th Cir. 1988) (“When the fundamental right to privacy clashes with the right of free expression, the interest in privacy does not play second fiddle when the speech is merely intended to propose a commercial transaction.”). In that respect, this case more closely resembles *American Blast Fax*, which upheld a statute that prohibited unsolicited facsimile transmissions unless the recipient had opted in to receipt. “While it is true that the effect of [the

---

<sup>6</sup> Indeed, even the cases petitioner cites in support of its claims of First Amendment injury (Br. 24-25) have no bearing here. *Bartnicki v. Vopper*, 532 U.S. 514 (2001), involved a statute that “implicate[d] the core purposes of the First Amendment” by restricting “information of public concern” broadcast over a radio station by a political commentator. *Id.* at 533-534. This case concerns speech of no concern to the general public. *Meyer v. Grant*, 486 U.S. 414 (1988), involved “a limitation on political expression.” *Id.* at 420. The Court did not address, and the case has no bearing on, the First Amendment implications of targeted marketing that requires use of private data that does not belong to the speaker. *Bolger v. Young Drugs Corp.*, 463 U.S. 60 (1983), involved an explicitly content-based restriction on the mailing of flyers advertising contraceptive devices. *Martin v. City of Struthers*, 319 U.S. 141 (1943), considered a flat ban on door-to-door religious proselytizing.

fax restriction] will be that some consumers will not receive unsolicited advertisements they might have appreciated,” the Court held, under an opt-out approach, “there would always be individuals suffering costs and interference from unwanted advertisements. It was not unreasonable ... to choose a system that protects those who would otherwise be forced to bear unwanted burdens over those who wish to send and receive unsolicited fax advertising.” 323 F.3d at 659. The Ninth Circuit similarly upheld a restriction on faxes in *Destination Ventures, Ltd. v. FCC*, 46 F.3d 54 (9th Cir. 1995). As discussed above, this Court in *Trans Union* strongly affirmed the primacy of privacy rights over commercial speech using personal consumer data. *See also Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 625 (1995) (upholding restriction on targeted marketing of legal services to accident victims in part because such solicitations “are perceived by the public as intrusive”).<sup>7</sup>

Opt-in also furthers a Commission interest in conforming commercial practices to consumers’ expectations about how carriers will use their personal

---

<sup>7</sup> The Tenth Circuit’s decision in *U.S. West* diverged from such cases, but there is no good reason for this Court to follow that decision. For example, the Tenth Circuit held that opt-in failed to advance an interest in privacy because the FCC “presents no evidence showing the harm to ... privacy ... is real.” 182 F.3d at 1237. But both the current administrative record and recent findings of fact made by Congress, neither of which was before the Tenth Circuit, now show conclusively that there is a quite substantial government interest in protecting CPNI data and that the consequences of the release of such data can be severe.

data. Knowing consumer authorization for disclosure is important because “there is less customer willingness for their information to be shared without their express authorization with others outside the carrier-customer relationship.” *2007 CPNI Order* ¶40 (JA ). The government has a direct interest in protecting such expectations and ensuring that information will be shared only with respect to those customers who truly wish to authorize such sharing.

Petitioner claims that the Commission improperly relied on consumer expectations (Br. 34-36), arguing that such expectations are both “immaterial” and “unsubstantiated” (Br. 35). In fact, consumer expectations are highly material when assessing the scope of privacy interests. *Cf. Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (considering patient’s “reasonable expectation of privacy” in her medical records in assessing Fourth Amendment claim). The requisite type of customer consent to the use and sharing of CPNI depends to a large degree on how consumers expect their private data to be used; for that reason, consumer expectations have been a principal factor in the Commission’s analysis throughout its implementation of section 222. For example, under the “total service approach” (described in note 1, *supra*) adopted in the *1998 CPNI Order*, a carrier may freely use CPNI data to market services incidental to those already offered. The Commission concluded that such use without express approval was permissible, in part, because of its assessment of consumer expectations about the use of CPNI

data. *1998 CPNI Order*, 13 FCC Rcd at 8080 (“customer approval for carriers to use, disclose, and permit access to CPNI can be inferred in the context of an existing customer-carrier relationship ... 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”). Likewise, the Commission’s decision in the *2002 CPNI Order* to require opt-in for disclosure of CPNI to third parties that do not provide telecommunications services was also driven by consumer expectations. 17 FCC Rcd at 14884 (record “vividly demonstrate[s] that consumers view use of CPNI by a consumer’s carrier differently than disclosure to or use by a third party”).

Commission concern about consumer expectations regarding data sharing is also substantiated. The record at the time of the *2002 CPNI Order* showed that consumer concern was “most acute for disclosure to parties other than their own carrier,” 17 FCC Rcd at 14876, and that 73 percent of consumers favored barring third-party disclosure entirely, *id.* at 14884. At the time, the Commission weighed that evidence against other considerations and found that, on balance, opt-out was appropriate for disclosures to third parties that provide telecommunications services, but opt-in was appropriate for third parties that did not provide such services. Comments submitted in the current record also express consumer discomfort with use and disclosure of data. *2007 CPNI Order* n.129 (JA ).

Given the increased risks and consequences of security breaches, the balance has shifted and the FCC can no longer presume that consumers will consent to all third-party disclosures for marketing purposes. Rather, in the current climate, 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. *2007 CPNI Order* ¶45 (JA ). An opt-in program based on an understanding of consumer expectations reflects the type of “consensus” the Supreme Court has found relevant to the question whether the government’s interests are advanced. *Florida Bar*, 515 U.S. at 628.

Finally, petitioners claim that “[w]hether CPNI is shared with independent contractors or joint venture partners ... or agents or affiliates of the carrier ... seems quite unlikely to affect consumer preferences.” Br. 35, 38-39. In effect, petitioner is claiming that the Commission’s approach is underinclusive because it allows opt-out for a category of disclosures (to affiliates and agents) that resembles another category subject to opt-in (independent contractors and joint venture partners).

As this Court held in *Trans Union*, however, “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.” 245 F.3d at 819 (quoting *Blount v. SEC*, 61 F.3d 938, 946 (D.C. Cir. 1995)). To win on an

underinclusiveness claim, a party must show that “it cannot fairly be said to advance any genuinely substantial governmental interest because it provides only ineffective or remote support for the asserted goals or limited incremental support.” *Trans Union*, 245 F.3d at 819 (quoting *Blount*, 61 F.3d at 946); *see also Trans Union*, 267 F.3d at 1143.

The line drawn by the Commission was reasonable and provides effective support for its goals. Requiring affirmative customer consent to disclosing CPNI to independent contractors and joint venture partners fulfills the government’s interests whether or not disclosures to affiliates and agents are governed by the same consent standard. Thus, the Commission’s distinction between the two different types of third parties does not undermine the policies at stake. Indeed, “it would be odd to strike down a statute because Congress failed to restrict as much expression as it could have.” *Bell South Corp. v. FCC*, 144 F.3d 58, 70 (D.C. Cir. 1998).

Furthermore, the Commission has consistently treated disclosures to joint venture partners and independent contractors more strictly than those made to affiliates and agents. In the *2002 CPNI Order* for example, the Commission placed special protective restrictions on carrier/independent contractor and carrier/joint venture partner relationships that it did not place on affiliate and agency relationships (and no one challenged that distinction). 17 FCC Rcd 14881.

Here, the Commission found that 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,” disclosure to such third parties posed a particular risk, which thus called for a more explicit form of customer consent than for affiliates and agents. Indeed, the affiliate rules attribute ownership to a stakeholder precisely because of the influence and control over operations – and thus the ability to protect information directly – that ownership gives. *E.g.*, *Time Warner Entertainment Co. v. FCC*, 240 F.3d 1126, 1140-1141 (D.C. Cir. 2001). An agency relationship also places liability on the carrier for improper acts of the agent, thus giving the carrier a strong incentive to ensure that all information is handled properly. *See* Restatement (Third) of Agency §§ 7.03, 7.08 (2006). Non-agency, non-affiliate relationships, by contrast, are one step further removed, without direct control by the carrier, and possibly without recourse against the carrier by a victim of a data breach.<sup>8</sup>

---

<sup>8</sup> Intervenors rely (Int. Br. 35) on 47 U.S.C. § 217 for the proposition that independent contractors are in the same position as agents, but while that may be true for FCC enforcement purposes, intervenors have not shown that it is true in private party litigation against a carrier for damages.



b. *The Government's Interest Is Real.*

Opt-in ensures that consumers knowingly consent to the disclosure of their private data to a joint venture partner or independent contractor and also that consumers accept the increased risk associated with such disclosure. Petitioner again ignores the first interest, and this omission is, by itself, fatal to its argument. The argument that petitioner does make – that opt-in does not advance the interest in knowing consent to increased risk because there is no increased risk – fails as well.

The Commission concluded that “the more companies that have access to CPNI, the greater the risk of unauthorized disclosure,” *2007 CPNI Order* ¶46 (JA ); *see ibid.* (“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”). In light of the increased risk, the Commission determined that the threshold for consumer consent also should increase.

That finding of increased risk was a matter of simple common sense – as the Commission termed it, “axiomatic.” *Id.* ¶46 (JA ). As more companies have access to data, the data become more vulnerable to disclosure. More companies means greater numbers of employees who might seek to profit from the sale of data. *See id.* ¶46 (JA ) (majority of identity theft incidents arise from insider conduct). It also means more data on laptops and data disks that can be lost or

stolen. *Id.* ¶41 (JA ) (Commission concerned not only with “inappropriate handling” of CPNI but with “innocent mishandling or loss” as well).

Indeed, as the Commission pointed out, the carriers themselves have had difficulty protecting CPNI data, which leads naturally to the conclusion that the data are less safe in the hands of a third party. *Id.* ¶49 (JA ). Carriers themselves “have failed to adequately protect CPNI” in the past by engaging in improper practices, and the Commission has had to take enforcement action against those carriers. *Id.* ¶12 & n.31 (JA ). If carriers themselves, with direct customer relationships at stake and directly subject to both section 222 and the Commission’s enforcement authority, cannot or will not properly protect CPNI, it is foolhardy to assume that independent contractors and joint venture partners will have any greater incentive to do so. Moreover, as one large carrier informed the Commission, “pretexters persist without regard” to the holder of the data. *Id.* ¶46

(JA ).<sup>9</sup> And the development of a black market in CPNI data ratchets up the likelihood and consequences of disclosure, thus increasing the overall level of risk.

That is true whether or not there have been incidents of data disclosure from independent contractors and joint venture partners. The Commission was concerned about *risk*, and the risk is higher when more entities have access to the data. It would make no sense for the Court to rule, as petitioner and its intervenor urge, that the Commission is prohibited from taking any regulatory action until after the damage is done.

That type of “simple common sense” conclusion is sufficient under intermediate scrutiny to support the Commission’s conclusion that opt-in is necessary to ensure knowing customer consent as risks increase. *Florida Bar*, 515 U.S. at 628. Petitioner’s reliance (Br. 38) on *Century Communications Corp. v. FCC*, 835 F.2d 292 (D.C. Cir. 1987), for the proposition that common sense has no place in the constitutional analysis is misplaced. That case held only that the Court

---

<sup>9</sup> Intervenors claim that there is no risk because independent marketing companies do not have access to call detail data. Int. Br. 22. But the Commission found, and Intervenors do not dispute, that Congress intended to protect *all* CPNI, not just call details. *2007 CPNI Order* ¶48 (JA ). Furthermore, non-call-detail data can be used as a springboard to obtaining other personal information. *Id.* n.73 (JA ). The Commission also provided specific examples of non-call detail data that nevertheless can be highly personal, such as the names and numbers contained in calling lists. *Id.* ¶48 (JA ). Intervenors also claim that attempting to obtain CPNI from contractors “is an obviously fruitless practice,” Int. Br. 22, but in *ex parte* comments Sprint stated that pretexters do attack contractors. *2007 CPNI Order* ¶46 (JA ).

does not defer to agency judgments in constitutional cases the way it does in APA cases (and the Court did not use the term “common sense”). Indeed, in rejecting a First Amendment claim just last year, the Supreme Court held that it did not need “empirical data to credit [a] common-sense conclusion” advanced in support of the restriction at issue. *Tennessee Secondary School Ass’n v. Brentwood Academy*, 127 S. Ct. 2489, 2495-2496 (2007).

Petitioner is incorrect that the various safeguards that protect CPNI shared with joint venture partners and independent contractors eliminate any risk of disclosure. Br. 41-44; *see* Int. Br. 34-36. The Commission found that data safeguards “do not adequately protect a customer’s CPNI in today’s environment” in the wake of an “increased market value ... on obtaining [CPNI] data,” and “concrete evidence that the dissemination of this private information does inflict specific and significant harm on individuals.” *2007 CPNI Order* ¶39 (JA ). “[O]nce 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.” *Ibid.* Indeed, as discussed above, the carriers themselves have been unable to prevent security breaches, and it stands to reason that third parties are even more vulnerable. *Id.* ¶49 (JA ).

Third parties such as telemarketers that do not provide communications services are not directly subject to section 222. Private contracts may attempt to

protect consumers' data in such relationships, but they can be enforced – by the carrier, but not necessarily by the customer – only after a breach. That is too little, too late: “in the event of a breach of CPNI security, the damage is already inflicted upon the customer.” *Id.* ¶42 (JA ). Nor is an after-the-fact FCC enforcement proceeding adequately protective because enforcement actions “cannot undo the harm to a customer after a breach.” *Id.* n.134 (JA ). Thus, while data safeguards may reduce the risk of disclosure somewhat, they do not eliminate it entirely, and the risk posed to consumers is real. In deciding between opt-in and opt-out, the Commission properly determined that the risk was sufficient to require affirmative customer approval before a carrier may increase the risk of a data breach.

### **3. Opt-In Is Sufficiently Tailored.**

Given the significant risks and consequences of data theft and accidental disclosure, and the concomitant need for genuine and knowing consumer acceptance of the risks inherent in using the information, the Commission would have been justified in adopting an opt-in approach for all CPNI disclosure for marketing purposes. Instead, the Commission judiciously chose to use a substantially limited opt-in approach that applies only to disclosure to joint venture partners and independent contractors. That approach is proportional to the government's interests in protecting the privacy of CPNI.

The “burden” imposed by opt-in on carriers’ speech is minimal. Opt-in does not regulate the content of carriers’ marketing messages. Carriers have multiple means to market services to all their customers, including those customers who choose not to permit disclosure of their private data, and no carrier is prohibited from speaking to its customers in any way.

Nor does the limited opt-in measure at issue here prohibit targeted marketing. *See* Br. 4-5; Int. Br. 3. Indeed, the Commission found that many carriers use opt-in voluntarily, *2007 CPNI Order* n.148 (JA ), which demonstrates that opt-in does not seriously interfere with carriers’ ability to engage in marketing. Even if most customers do not opt in, petitioner’s members may continue to engage in targeted marketing by using in-house personnel or agents and affiliates.

The true stakes here thus are not a prohibition on speech, but a possible increase in marketing costs: petitioner’s members may have to spend more time or money to convince their customers to permit disclosure of private information for marketing purposes or may have to make some sales calls in-house. The Commission found that increased marketing costs were “outweighed by the carriers’ duty to protect their customers’ private information, and more importantly, customers’ interest in maintaining control over their private information.” *2007 CPNI Order* ¶43 (JA ). “That more people may be more easily and cheaply reached ... is not enough to call forth constitutional protection

for what those charged with public welfare reasonably think is a nuisance when easy means of publicity are open.” *Kovacs v. Cooper*, 336 U.S. 77, 88-89 (1949).

The limited opt-in approach for independent contractors and joint venture partners is proportional to the interest it serves. *See Florida Bar*, 515 U.S. at 633 (upholding restriction on targeted marketing where there were “many other ways ... to learn about the availability of legal representation”); *Bell South*, 144 F.3d at 70 (“the fact that § 274 leaves ... BellSouth free to pursue [other avenues of speech] strengthens our conclusion that § 274 does not restrict substantially more speech than necessary”); *Mainstream Marketing*, 358 F.3d at 1243 (narrow tailoring demonstrated by “the fact that [government do-not-call program] presents both sellers and consumers with a number of options to make and receive sales offers”). *Compare 44 Liquormart*, 517 U.S. at 530-531 (O’Connor, J.) (“No channels exist at all to permit [liquor stores] to publicize the price of their products.”).

Opt-out, the only other possibility, would not achieve the Commission’s goal of ensuring that consumers knowingly accept the increased risk that results from the sharing of private CPNI data with independent contractors and joint venture partners. Given that this information is owned by the consumer, not the telecommunications carrier, it was entirely logical and consistent with basic

concepts of property law to require the consumer's affirmative consent before the information could be disclosed to a third party.

Whereas opt-in requires an affirmative act by the consumer, and thus a conscious decision to allow data sharing, opt-out leaves unprotected the consumer who does not wish to have data shared with third parties but who did not read or could not understand the opt-out notice, or simply did not get around to taking the effort required to opt out.<sup>10</sup> In that vein, the Commission expressed concern that opt-out notices do not truly inform consumers of the stakes at issue. The notices “are often vague and not comprehensible to an average customer,” *2007 CPNI Order* ¶40 (JA )<sup>11</sup>; more importantly, a customer “may not have read” it in the first place, *ibid.* Finally, the Commission noted that opt-in “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.” *Id.* ¶41 (JA ).

---

<sup>10</sup> Intervenors argue, for example, that “customers routinely fail to return opt-in forms” even if they want to receive targeted marketing. Int. Br. 4. It stands to reason that at least as many customers fail to pursue opt-out even when they do not want their information shared.

<sup>11</sup> That conclusion was supported by an example in the record of a current opt-out notice that is largely incomprehensible to the average person, even if it is technically accurate. EPIC Comments at 17 (JA ). EPIC also described the “cumbersome and confusing” – as well as misleading – process customers were forced to navigate if they understood the notice and decided to opt-out. *Ibid.*



Because opt-in “promotes a substantial government interest that would be achieved less effectively absent the regulation,” its use is constitutional whether or not it is the “least intrusive” means imaginable. *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989) (quoting *United States v. Albertini*, 472 U.S. 675, 689 (1985)); accord *Florida Bar*, 515 U.S. at 632 (“the ‘least restrictive means’ test has no role in the commercial speech context”). As the Court put it in *Trans Union*, “[a]lthough the opt-in scheme may limit more ... speech than would the opt-out scheme ..., intermediate scrutiny does not obligate courts to invalidate a remedial scheme because some alternative solution is marginally less intrusive on a speaker’s First Amendment interests.” 267 U.S. at 1143 (quotation marks and citation omitted).

Petitioner’s counterargument ignores the obviously relevant discussion in *Trans Union* and instead seems to rest on the premise that this case is subject to strict scrutiny. Under that standard, opt-in must be struck down unless it is the least restrictive alternative. Petitioner relies on *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803 (2000) (Br. 58), a strict scrutiny case that involved a statute that suppressed particular types of sexually oriented video programming and constituted “the essence of content-based regulation” that effectively “silence[d] the protected speech.” 529 U.S. at 812. On the basis of that case, petitioner argues (Br. 54-55) that because there are theoretical

“prototype” opt-out notices that can inform consumers of their rights, the Commission is required to use such notices rather than opt-in.

But this is not a strict scrutiny case, and the FCC does not have to show that opt-in is the least restrictive possible alternative; rather, it must show only that opt-in is a “reasonable” means that is “in proportion to the interest served.” *Fox*, 492 U.S. at 480; *see Trans Union*, 267 F.3d at 1143 (describing opt out as “marginally less intrusive on a speaker’s First Amendment interests” than opt-in). Thus, much of petitioner’s argument is simply irrelevant. To the degree it is relevant, the argument is wrong.

Petitioner argues at length that opt-in is more restrictive than necessary because the Commission’s concerns would be addressed by requiring better opt-out notices. Br. 49-61. The claim is not well founded for two principal reasons. First, the deficiencies in opt-out notices referred to by the Commission were not the only, or even the principal, reason the Commission adopted an opt-in regime for third party disclosures. In light of the extensive discussion in the order of the need for affirmative customer assumption of risk, it is clear that even if the Commission had not found that current opt-out notices are deficient, it would have adopted opt-in for joint venture and independent contractor use anyway.

Second, the most informative, easiest-to-understand opt-out notice makes no difference to the consumer who fails to read it. The Commission was

concerned not only about notices that are “vague and not comprehensible,” but also about customers who “may not have read” it in the first place. *2007 CPNI Order* ¶40 (JA ). As the Attorneys General of 48 states put it in their comments, “common sense tell us” that “in this harried country of multitaskers, most consumers are unlikely to read the extra notices that arrived in today’s or last week’s mail.” Attorney General Comments at 6 (JA ), cited at *2007 CPNI Order* ¶44 (JA ). The Commission has been concerned since its initial implementation of section 222 about the consumer who fails to read an opt-out notice: “under an opt-out approach ... because customers may not read their CPNI notices, there is no assurance that any implied consent would be truly informed.” *1998 CPNI Order* at 8130-8131. Better opt-out notices are not a less restrictive alternative because they would fail to achieve the Commission’s goals.

Petitioner also claims that opt-in restricts more speech than necessary because in the *2002 CPNI Order* the Commission found that opt-out would adequately protect the government’s interests. Br. 45-46. Since then, petitioner argues, “[n]othing has changed,” and therefore opt-in is not a narrowly tailored solution. Br. 46.

As the Commission explained, its understanding of the risks and consequences of CPNI disclosure changed substantially since the *2002 CPNI Order* in 2002. The Commission learned of the black market in CPNI data and the

corresponding serious risk that CPNI could be disclosed, and of the serious consequences that disclosure can entail, from embarrassment to domestic violence to interference with police investigations. *2007 CPNI Order* ¶¶12, 39 (JA , ). Since that time, Congress has also made explicit findings about the seriousness of CPNI breaches in the Telephone Records and Privacy Protection Act of 2006. The balance of interests has changed substantially since 2002, thus making imperative express consent to certain risks posed by CPNI usage. In those circumstances “customers’ interests in maintaining control over their private information” outweighs the small burden placed on the carrier. *2007 CPNI Order* ¶43 (JA ).

Finally, petitioner argues that “there are obvious means available” short of opt-in to alleviate the Commission’s concern about the risk of disclosure of CPNI data in the hands of independent contractors and joint venture partners. Br. 61-64. Petitioner’s suggestion is for the Commission “to impose additional contractual and regulatory safeguards” to reduce the risk of disclosure. Br. 62. But as we have explained at pages 41-42 above, the Commission concluded that it is a commonsense proposition that increasing the number of companies that have access to data increases the chance that the data will be disclosed. Petitioner has not come to grips with the Commission’s observation that if the carriers themselves have had difficulty protecting the secrecy of data, it is clear that data is even less safe in the hands of a third party. *Id.* ¶49 (JA ).

It is not enough to answer that “if the Commission thought the restrictions applicable to carriers and their affiliates/agents were sufficient to permit sharing under an opt-out regime,” then those restrictions should be sufficient for independent contractors and joint venture partners as well. Br. 62; *see* Int. Br. 33-34. That argument is just one more variant on the underinclusiveness claim, and it fails for the reasons discussed above. The Commission would have been justified in requiring opt-in for all third party disclosures; there is no constitutional infirmity in its having allowed opt-out for some. Disclosure to affiliates and agents can be expected to take place in a framework of greater accountability and a higher degree of carrier control than other third parties. *See 2007 CPNI Order* ¶39 (JA ) (“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”); *see also supra* pp.39-40. The Commission was entitled to address what it deemed the most significant problem, while letting other potential problems be.

### **III. THE COMMISSION REASONABLY CHANGED FROM AN OPT-OUT TO A LIMITED OPT-IN APPROACH.**

Petitioner makes a token argument that, for the same reasons that the change from opt-out to opt-in is allegedly unconstitutional, it is also arbitrary and

capricious. The claims lack merit in the administrative law context for the same reasons they fail in the constitutional context.

Under basic principles of administrative law, “regulatory agencies do not establish rules of conduct to last forever,” and “an agency must be given ample latitude to adapt [its] rules and policies to the demands of changing circumstances.” *State Farm*, 463 U.S. at 42 (quotation marks and citations omitted). So too here. In the rulemaking before the Court, the Commission faced a landscape very different from the one it had examined at the time of the *2002 CPNI Order*. As we have explained, the risks and consequences of data disclosure were revealed to be far more significant and severe than they had appeared in the earlier proceeding, and the Commission adapted its approach accordingly in order to protect the public and fulfill the mandate of section 222. We have explained fully above the reasoning and record supporting the Commission’s decision to limit opt-in to independent contractors and joint venture partners, and we have likewise explained why the Commission’s policy determination will accomplish its goals.

Indeed, the APA gives the Commission considerable latitude to regulate in areas of uncertainty. “When . . . an agency is obliged to make policy judgments where no factual certainties exist . . . we require only that the agency ‘so state and go on to identify the considerations it found persuasive.’” *AT&T v. FCC*, 832 F.2d 1285, 1291 (D.C. Cir. 1987); accord *Melcher v. FCC*, 134 F.3d 1143, 1152 (D.C.

Cir. 1998). The Commission drew just such a predictive judgment when it determined that affirmative customer consent should be required for disclosures of CPNI to independent contractors and joint venture partners.

Intervenors rely heavily on *National Fuel Gas Supply Corp. v. FERC*, 468 F.3d 831 (D.C. Cir. 2006), for the proposition that it was arbitrary for the Commission to require opt-in for joint venture partners and independent contractors in the absence of examples in the record of data breaches at the hands of such entities. That reliance is misplaced. In *National Fuel*, FERC extended the coverage of rules that were intended to prevent anti-competitive discriminatory treatment. The rules initially imposed structural separation requirements on gas pipelines' "marketing affiliates," in order to restrict the abuse of the pipelines' monopoly power. FERC later expanded the rules to cover non-marketing affiliates as well. The Court vacated the order extending coverage because there was no evidence that the pipelines had exploited their monopoly power through their relationships with non-marketing affiliates. 468 F.3d at 843. In other words, the Court held that FERC could not regulate one set of relationships (those with non-marketing affiliates) on the basis of abuses that occurred through a different set of relationships (those with marketing affiliates) in the absence of evidence that the abuses could occur with non-marketing affiliates.

Here, by contrast, the problem of the growing black market for CPNI information and the severe consequences that can result from the disclosure of that data pertains to *any* company that has access to CPNI. Unlike in *National Fuel*, the Commission and the public face a genuine threat of the release of confidential data by all third party recipients of that data. It is of no moment that the record did not tell of specific instances of breaches of data security stemming from independent contractors or joint venture partners because there is no question that such parties have access to CPNI data and are, for the reasons set forth by the Commission, vulnerable to data breaches. On that record, *National Fuel* has no bearing here. Under intervenors' reading of that case, agencies may not make rules intended to fight foreseeable problems prophylactically, but may remedy problems only after it is too late. *Cf. Star Wireless, LLC v. FCC*, No. 07-1190, 2008 WL 1795596, at \*4 (D.C. Cir. Apr. 22, 2008) (“general bright-line prophylactic measures ... are appropriate when ‘the probability of abuse in transactions between related organizations is significant enough that it is more efficient to prevent the opportunity for abuse from arising than it is to try to detect actual incidents of abuse.’” (quoting *Biloxi Reg'l Med. Ctr. v. Bowen*, 835 F.2d 345, 350 (D.C. Cir. 1987))).

Petitioner makes one new argument that is not just a reprise of its constitutional claims in APA garb: it complains that the Commission failed to



address comments raising the issue of an alleged competitive harm to “new entrants and smaller carriers” that opt-in will cause. Br. 69.

At the outset, the argument is barred by 47 U.S.C. § 405(a) because petitioner did not raise it before the Commission in a petition for reconsideration. “If a party to an FCC proceeding believes that the Commission has failed to address certain record evidence, § 405(a) requires that the party bring the matter to the attention of the agency before proceeding to court.” *Freeman Eng’g Assocs., Inc. v. FCC*, 103 F.3d 169, 182 (D.C. Cir. 1997). If the party does not raise the oversight claim with the agency by means of a petition for reconsideration, its claim is waived. *See id.*; accord *Time Warner Entertainment Co. v. FCC*, 144 F.3d 75, 80-81 (D.C. Cir. 1998) (when petitioner alleges “procedural oversight,” such as claim that FCC “ignored certain record evidence,” it must seek agency reconsideration as a prerequisite to judicial review of its oversight claim).

On its merits, the argument fails because the limited opt-in program applies equally to all companies that have access to CPNI data; no company is treated differently – consistent with the general rule that similarly situated parties must be treated similarly. *E.g., Melody Music, Inc. v. FCC*, 345 F.2d 730 (D.C. Cir. 1965). Petitioner has not cited any case where it was held unlawful to apply a general rule to all parties subject to the regulation. Indeed, even intervenors refuse to support the argument. Int. Br. 29 n.4. To the degree that petitioner is arguing that some

companies must be exempt from the general rule, it gives no indication what the criteria for exemption should be, and its challenge is not well founded.

Moreover, it is clear from the text of section 222 that the protection of privacy was Congress's principal concern in enacting that statute. The provision is entitled "Privacy of Customer Information" and fundamentally imposes the duty to "protect" the "confidentiality" of "proprietary" information that the FCC has long regarded as belonging to the customer. The statute also protects information that is personal to the customer (and allows release of other information that is less personal, § 222(e)). Privacy thus takes precedence over competitive effects.

Given the record presented, the Commission properly focused on the compelling privacy concerns at stake in this matter. So did the commenters. The four sets of comments relied on by petitioner make at most passing mention of any competitive issue. For example, Charter Communications referred in passing to competitive effects (and it is not clear that they pertained to opt-in/opt-out) at page 2 of its comments (JA ), but in a 7-page discussion of opt-in, Charter did not mention competition once. Comments of Charter Communications at 14-20 (JA - ). Alltel devoted two sentences to competition, Comments of Alltel Corp. at 4 (JA ); Comcast only a single sentence, Comments of Comcast Corp. at 1 (JA ). Sprint gave the matter one paragraph of a 17-page ex parte presentation. Sprint Nextel Feb. 12, 2007, ex parte (JA ).

Even if such comments were sufficient to preserve the matter for appellate review, they hardly raised a serious consideration, and the FCC accordingly was not obligated to respond. “[I]t is one thing to preserve a point for judicial review and quite another to raise the issue with sufficient force to require an agency to formally respond. An agency is not obliged to respond to every comment, only those that can be thought to challenge a fundamental premise.” *MCI WorldCom, Inc. v. FCC*, 209 F.3d 760, 765 (D.C. Cir. 2000). *Accord Reytblatt v. U.S. Nuclear Regulatory Comm’n*, 105 F.3d 715, 722 (D.C. Cir. 1997) (“An agency need not address every comment, but it must respond in a reasoned manner to those that raise significant problems.”); *Thompson v. Clark*, 741 F.2d 401, 408 (D.C. Cir. 1984). Petitioner has not shown any error.

**CONCLUSION**

For the foregoing reasons, the petition for review should be denied.

Respectfully submitted,

THOMAS O. BARNETT  
ASSISTANT ATTORNEY GENERAL

MATTHEW B. BERRY  
GENERAL COUNSEL

JAMES J. O'CONNELL, JR.  
DEPUTY ASSISTANT ATTORNEY GENERAL

JOSEPH R. PALMORE  
DEPUTY GENERAL COUNSEL

CATHERINE G. O'SULLIVAN  
NANCY C. GARRISON  
ATTORNEYS

RICHARD K. WELCH  
ACTING DEPUTY ASSOCIATE GENERAL  
COUNSEL

UNITED STATES DEPARTMENT OF JUSTICE  
WASHINGTON, D.C. 20530



JOEL MARCUS  
COUNSEL

FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554  
(202) 418-1740 (TELEPHONE)  
(202) 418-2819 (FAX)

April 30, 2008

IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

NATIONAL CABLE & TELECOMMUNICATIONS )  
Association )

PETITIONER, )

v. )


FEDERAL COMMUNICATIONS COMMISSION )  
AND THE UNITED STATES OF AMERICA )

RESPONDENTS, )

No. 07-1312

CERTIFICATE OF COMPLIANCE

Pursuant to the requirements of Fed. R. App. P. 32(a)(7), I hereby certify that the accompanying "Brief for Respondents" in the captioned case contains 13693 words.



Joel Marcus  
Counsel

FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554  
(202) 418-1740 (TELEPHONE)  
(202) 418-2819 (FAX)

April 30, 2008

# STATUTORY APPENDIX

47 U.S.C. § 222  
47 U.S.C. § 405(a)

Pub. L. No. 109-476

47 C.F.R. § 64.2007 (2002)  
47 C.F.R. § 64.2007 (2007)

UNITED STATES CODE ANNOTATED  
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS  
CHAPTER 5. WIRE OR RADIO COMMUNICATION  
SUBCHAPTER II. COMMON CARRIERS  
PART I. COMMON CARRIER REGULATION

§ 222. Privacy of customer information

(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

## 47 U.S.C. § 222 (cont'd)

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)--

(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) 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.



## 47 U.S.C. § 222 (cont'd)

## (f) Authority to use wireless location information

For purposes of subsection (c)(1) of this section, 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), other than in accordance with subsection (d)(4) of this section; 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) of this section, a telecommunications carrier that provides telephone exchange service shall provide information described in subsection (i)(3)(A) [FN1] of this section (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

## 47 U.S.C. § 222 (cont'd)

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.

[FN1] So in original. Probably should be “(h)(3)(A)”.

UNITED STATES CODE ANNOTATED  
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS  
CHAPTER 5--WIRE OR RADIO COMMUNICATION  
SUBCHAPTER IV--PROCEDURAL AND ADMINISTRATIVE PROVISIONS

§ 405. Petition for reconsideration; procedure; disposition; time of filing; additional evidence; time for disposition of petition for reconsideration of order concluding hearing or investigation; appeal of order

(a) After an order, decision, report, or action has been made or taken in any proceeding by the Commission, or by any designated authority within the Commission pursuant to a delegation under section 155(c)(1) of this title, any party thereto, or any other person aggrieved or whose interests are adversely affected thereby, may petition for reconsideration only to the authority making or taking the order, decision, report, or action; and it shall be lawful for such authority, whether it be the Commission or other authority designated under section 155(c)(1) of this title, in its discretion, to grant such a reconsideration if sufficient reason therefor be made to appear. A petition for reconsideration must be filed within thirty days from the date upon which public notice is given of the order, decision, report, or action complained of. No such application shall excuse any person from complying with or obeying any order, decision, report, or action of the Commission, or operate in any manner to stay or postpone the enforcement thereof, without the special order of the Commission. The filing of a petition for reconsideration shall not be a condition precedent to judicial review of any such order, decision, report, or action, except where the party seeking such review (1) was not a party to the proceedings resulting in such order, decision, report, or action, or (2) relies on questions of fact or law upon which the Commission, or designated authority within the Commission, has been afforded no opportunity to pass. The Commission, or designated authority within the Commission, shall enter an order, with a concise statement of the reasons therefor, denying a petition for reconsideration or granting such petition, in whole or in part, and ordering such further proceedings as may be appropriate: *Provided*, That in any case where such petition relates to an instrument of authorization granted without a hearing, the Commission, or designated authority within the Commission, shall take such action within ninety days of the filing of such petition. Reconsiderations shall be governed by such general rules as the Commission may establish, except that no evidence other than newly discovered evidence, evidence which has become available only since the original taking of evidence, or evidence which the Commission or designated authority within the Commission believes should have been taken in the original proceeding shall be taken on any reconsideration. The time within which a petition for review must be filed in a proceeding to which section 402(a) of this title applies, or within which an appeal must be taken under section 402(b) of this title in any case, shall be computed from the date upon which the Commission gives public notice of the order, decision, report, or action complained of.

47 U.S.C. § 405 (continued)

**(b)(1)** Within 90 days after receiving a petition for reconsideration of an order concluding a hearing under section 204(a) of this title or concluding an investigation under section 208(b) of this title, the Commission shall issue an order granting or denying such petition.

**(2)** Any order issued under paragraph (1) shall be a final order and may be appealed under section 402(a) of this title.

**UNITED STATES PUBLIC LAWS  
109th Congress - Second Session  
Convening January 7, 2005**

Copr. © 2007 Thomson/West. No Claim to Orig. U.S. Govt. Works

Additions and Deletions are not identified in this database.  
Vetoed provisions within tabular material are not displayed

PL 109-476 (HR 4709)

January 12, 2007

**TELEPHONE RECORDS AND PRIVACY PROTECTION ACT OF 2006**

An Act To amend title 18, United States Code, to strengthen protections for law enforcement officers and the public by providing criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records.

Be it enacted by the Senate and House of Representatives of the United States  
of America in Congress assembled,

<< 18 USCA § 1 NOTE >>

**SECTION 1. SHORT TITLE.**

This Act may be cited as the "Telephone Records and Privacy Protection Act of 2006".

<< 18 USCA § 1039 NOTE >>

**SEC. 2. FINDINGS.**

Congress finds that--

- (1) telephone records can be of great use to criminals because the information contained in call logs may include a wealth of personal data;
- (2) call logs may reveal the names of telephone users' doctors, public and private relationships, business associates, and more;
- (3) call logs are typically maintained for the exclusive use of phone companies, their authorized agents, and authorized consumers;

PL 109-476 (cont'd)

(4) telephone records have been obtained without the knowledge or consent of consumers through the use of a number of fraudulent methods and devices that include--

(A) telephone company employees selling data to unauthorized data brokers;

(B) "pretexting", whereby a data broker or other person represents that they are an authorized consumer and convinces an agent of the telephone company to release the data; or

(C) gaining unauthorized Internet access to account data by improperly activating a consumer's account management features on a phone company's webpage or contracting with an Internet-based data broker who trafficks in such records; and

(5) the unauthorized disclosure of telephone records 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.

### SEC. 3. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH OBTAINING CONFIDENTIAL PHONE RECORDS INFORMATION OF A COVERED ENTITY.

<< 18 USCA § 1039 >>

(a) OFFENSE.--Chapter 47 of title 18, United States Code, is amended by inserting after section 1038 the following:

"§ 1039. Fraud and related activity in connection with obtaining confidential phone records information of a covered entity

"(a) CRIMINAL VIOLATION.--Whoever, in interstate or foreign commerce, knowingly and intentionally obtains, or attempts to obtain, confidential phone records information of a covered entity, by--

"(1) making false or fraudulent statements or representations to an employee of a covered entity;

"(2) making such false or fraudulent statements or representations to a customer of a covered entity;

"(3) providing a document to a covered entity knowing that such document is false or fraudulent; or

PL 109-476 (cont'd)

"(4) accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates section 1030 of this title, without prior authorization from the customer to whom such confidential phone records information relates; shall be fined under this title, imprisoned for not more than 10 years, or both.

**"(b) PROHIBITION ON SALE OR TRANSFER OF CONFIDENTIAL PHONE RECORDS INFORMATION.--**

"(1) Except as otherwise permitted by applicable law, whoever, in interstate or foreign commerce, knowingly and intentionally sells or transfers, or attempts to sell or transfer, confidential phone records information of a covered entity, without prior authorization from the customer to whom such confidential phone records information relates, or knowing or having reason to know such information was obtained fraudulently, shall be fined under this title, imprisoned not more than 10 years, or both.

"(2) For purposes of this subsection, the exceptions specified in section 222(d) of the Communications Act of 1934 shall apply for the use of confidential phone records information by any covered entity, as defined in subsection (h).

**"(c) PROHIBITION ON PURCHASE OR RECEIPT OF CONFIDENTIAL PHONE RECORDS INFORMATION.--**

"(1) Except as otherwise permitted by applicable law, whoever, in interstate or foreign commerce, knowingly and intentionally purchases or receives, or attempts to purchase or receive, confidential phone records information of a covered entity, without prior authorization from the customer to whom such confidential phone records information relates, or knowing or having reason to know such information was obtained fraudulently, shall be fined under this title, imprisoned not more than 10 years, or both.

"(2) For purposes of this subsection, the exceptions specified in section 222(d) of the Communications Act of 1934 shall apply for the use of confidential phone records information by any covered entity, as defined in subsection (h).

**"(d) ENHANCED PENALTIES FOR AGGRAVATED CASES.--**Whoever violates, or attempts to violate, subsection (a), (b), or (c) while violating another law of the United States or as part of a pattern of any illegal activity involving more than \$100,000, or more than 50 customers of a covered entity, in a 12- month period shall, in addition to the penalties provided for in such subsection, be fined twice the amount provided in subsection (b)(3) or (c)(3) (as the case may be) of section 3571 of this title, imprisoned for not more than 5 years, or both.

PL 109-476 (cont'd)

"(e) ENHANCED PENALTIES FOR USE OF INFORMATION IN FURTHERANCE OF CERTAIN CRIMINAL OFFENSES.--

"(1) Whoever, violates, or attempts to violate, subsection (a), (b), or (c) knowing that such information may be used in furtherance of, or with the intent to commit, an offense described in section 2261, 2261A, 2262, or any other crime of violence shall, in addition to the penalties provided for in such subsection, be fined under this title and imprisoned not more than 5 years.

"(2) Whoever, violates, or attempts to violate, subsection (a), (b), or (c) knowing that such information may be used in furtherance of, or with the intent to commit, an offense under section 111, 115, 1114, 1503, 1512, 1513, or to intimidate, threaten, harass, injure, or kill any Federal, State, or local law enforcement officer shall, in addition to the penalties provided for in such subsection, be fined under this title and imprisoned not more than 5 years.

"(f) EXTRATERRITORIAL JURISDICTION.--There is extraterritorial jurisdiction over an offense under this section.

"(g) NONAPPLICABILITY TO LAW ENFORCEMENT AGENCIES.--This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or political subdivision of a State, or of an intelligence agency of the United States.

"(h) DEFINITIONS.--In this section:

"(1) CONFIDENTIAL PHONE RECORDS INFORMATION.--The term 'confidential phone records information' means information that--

"(A) relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, subscribed to by any customer of that covered entity, and kept by or on behalf of that covered entity solely by virtue of the relationship between that covered entity and the customer;

"(B) is made available to a covered entity by a customer solely by virtue of the relationship between that covered entity and the customer; or

"(C) is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer.



PL 109-476 (cont'd)

"(2) COVERED ENTITY.--The term 'covered entity'--

"(A) has the same meaning given the term 'telecommunications carrier' in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and

"(B) includes any provider of IP-enabled voice service.

"(3) CUSTOMER.--The term 'customer' means, with respect to a covered entity, any individual, partnership, association, joint stock company, trust, or corporation, or authorized representative of such customer, to whom the covered entity provides a product or service.

"(4) IP-ENABLED VOICE SERVICE.--The term 'IP-enabled voice service' means the provision of real-time voice communications offered to the public, or such class of users as to be effectively available to the public, transmitted through customer premises equipment using TCP/IP protocol, or a successor protocol, (whether part of a bundle of services or separately) with interconnection capability such that the service can originate traffic to, or terminate traffic from, the public switched telephone network, or a successor network."

<< 18 USCA prec. § 1001 >>

(b) CHAPTER ANALYSIS.--The table of sections for chapter 47 of title 18, United States Code, is amended by adding after the item relating to section 1038 the following:

"1039. Fraud and related activity in connection with obtaining confidential phone records information of a covered entity."

<< 28 USCA § 994 NOTE >>

#### SEC. 4. SENTENCING GUIDELINES.

(a) REVIEW AND AMENDMENT.--Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of any offense under section 1039 of title 18, United States Code.

(b) AUTHORIZATION.--The United States Sentencing Commission may amend the Federal sentencing guidelines in accordance with the procedures set forth in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that section had not expired.

**CODE OF FEDERAL REGULATIONS**  
**TITLE 47--TELECOMMUNICATION**  
**CHAPTER I--FEDERAL COMMUNICATIONS COMMISSION**  
**SUBCHAPTER B--COMMON CARRIER SERVICES**  
**PART 64--MISCELLANEOUS RULES RELATING TO COMMON CARRIERS**  
**SUBPART U--CUSTOMER PROPRIETARY NETWORK INFORMATION**

Current through October 1, 2002, 67 FR 61757

§ 64.2007. Notice and approval required for use of customer proprietary network information.

<Text of section effective until Oct. 21, 2002.>

(a) A telecommunications carrier must obtain customer approval to use, disclose, or permit access to CPNI to market to a customer service to which the customer does not already subscribe to from that carrier.

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

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

(d) Approval obtained by a telecommunications carrier for the use of CPNI outside of the customer's total service relationship with the carrier must remain in effect until the customer revokes or limits such approval.

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

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

(1) A telecommunications carrier may provide notification through oral or written methods.

(2) 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.

## 47 C.F.R. § 64.2007 (2002) (cont'd)

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

(ii) 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.

(iii) 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.

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

(v) 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.

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

(vii) 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.

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

(ix) 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 to from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

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

**Effective: December 08, 2007**

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

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

(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 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.

IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

National Cable & Telecommunications Association, Petitioner,

v.

Federal Communications Commission and USA, Respondents.

Certificate Of Service

I, Sharon D. Freeman, hereby certify that the foregoing typewritten "Brief For Respondents" was served this 30th day of April, 2008, by mailing true copies thereof, postage prepaid, to the following persons at the addresses listed below:

Daniel L. Brenner  
National Cable & Telecommunications Association  
25 Massachusetts Ave., N.W.  
Suite 100  
Washington DC 20001-1431

Matthew A. Brill  
Latham & Watkins LLP  
555 11th Street., N.W.  
Suite 1000  
Washington DC 20004-1304

Counsel For: National Cable & Telecommunications  
Association

Counsel For: National Cable & Telecommunications  
Association

Nancy C. Garrison  
U.S. Dept. of Justice  
Antitrust Div., Appellate Section  
950 Pennsylvania Avenue, N.W., Room 3224  
Washington DC 20530-0001

Michael E. Glover  
Verizon  
1515 North Courthouse Road  
Suite 500  
Arlington VA 22201-2909

Counsel For: USA

Counsel For: Verizon

Andrew G. McBride  
Wiley Rein LLP  
1776 K Street, N.W.  
11th Floor  
Washington DC 20006-2359

Robert B. McKenna  
Qwest Communications International, Inc.  
607 14th Street, N.W.  
Suite 950  
Washington DC 20005

Counsel For: Verizon

Counsel For: Qwest Communications International Inc.

  
Sharon D. Freeman