

ORAL ARGUMENT NOT YET SCHEDULED

No. 24-1224 & No. 24-1225

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

SPRINT CORPORATION,
T-MOBILE USA, INC.,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION
and UNITED STATES OF AMERICA,

Respondents.

On Petitions for Review of Orders of
the Federal Communications Commission

BRIEF FOR RESPONDENTS

Doha G. Mekki
*Acting Assistant
Attorney General*

Robert B. Nicholson
Matthew A. Waring
Attorneys

U.S. DEPARTMENT OF JUSTICE
950 Pennsylvania Ave. NW
Washington, DC 20530

P. Michele Ellison
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

John R. Grimm
Counsel

FEDERAL COMMUNICATIONS
COMMISSION

45 L Street NE
Washington, DC 20554
(202) 418-1740
fcclitigation@fcc.gov

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

(A) Parties and Amici. The parties are Petitioners Sprint Corporation and T-Mobile USA, Inc., and Respondents Federal Communications Commission and the United States of America. The Chamber of Commerce for the United States of America and CTIA—The Wireless Association have filed *amicus curiae* briefs in support of Petitioners. Respondents understand that the Electronic Privacy Information Center may file an *amicus curiae* brief in their support.

(B) Rulings Under Review. The petitions for review challenge two orders (the “*Orders*”) of the Federal Communications Commission: (1) Forfeiture Order, *Sprint Corporation* (“*Sprint Order*”), 39 FCC Rcd 4305 (Apr. 29, 2024) (JA286); and (2) Forfeiture Order, *T-Mobile USA, Inc.* (“*T-Mobile Order*”), 39 FCC Rcd 4350 (Apr. 29, 2024) (JA1).

(C) Related Cases. The *Orders* have not previously been before this or any other Court. Orders assessing forfeitures against other parties for similar violations are currently on review in the United States Courts of Appeals for the Second and Fifth Circuits. *Verizon Commc’ns Inc. v. FCC*, No. 24-1733 (2d Cir.); *AT&T Inc. v. FCC*, No. 24-60223 (5th Cir.).

TABLE OF CONTENTS

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES.....	i
TABLE OF AUTHORITIES	v
GLOSSARY	x
INTRODUCTION	1
JURISDICTIONAL STATEMENT.....	2
STATEMENT OF THE ISSUES	3
PERTINENT STATUTES AND REGULATIONS	4
STATEMENT OF THE CASE.....	4
I. STATUTORY AND REGULATORY BACKGROUND.	4
A. Protecting Customer Proprietary Network Information.....	4
B. The FCC’s Forfeiture Authority.	6
II. FACTUAL BACKGROUND AND PROCEEDINGS BELOW.	7
A. The Carriers’ Location-Based Services Programs.	8
B. The Misuse of Sprint and T-Mobile Customers’ Data.....	10
C. The Carriers’ Responses to the Securus and MicroBilt News.	15
D. The <i>Orders</i> Under Review.	16
1. The Commission Finds That Location Data is CPNI.....	17
2. The Commission’s Liability Findings.	18
3. The Forfeitures.	23
STANDARDS OF REVIEW.....	24

TABLE OF CONTENTS
(continued)

	Page
SUMMARY OF THE ARGUMENT.....	25
ARGUMENT.....	29
I. THE COMMISSION DID NOT VIOLATE THE CARRIERS’ CONSTITUTIONAL RIGHTS.	29
A. The Commission’s Forfeiture Authority Does Not Violate the Seventh Amendment.	29
1. Sprint and T-Mobile Had the Right to a Trial in District Court Before Paying the Commission’s Forfeitures.....	29
2. CPNI Enforcement Actions Are Not The Type of Common-Law Claim That Requires a Jury Trial.....	33
B. The Commission Did Not Violate Separation-of-Powers or Due Process Principles.	41
II. CUSTOMER LOCATION INFORMATION IS CPNI.....	44
A. CPNI Is Not Limited to Call Location Information.....	45
B. Sprint and T-Mobile Had Access to Their Customers’ Location Data Solely by Virtue of the Carrier– Customer Relationship.	52
C. The Carriers Had Sufficient Notice That Customer Location Data is CPNI.....	55
III. THE COMMISSION’S LIABILITY FINDINGS AND THE FORFEITURES IT ASSESSED WERE LAWFUL.	56
A. Substantial Evidence Supports the Commission’s Finding of Liability.	56
B. The Commission Assessed Lawful Forfeitures.....	60

TABLE OF CONTENTS
(continued)

	Page
CONCLUSION	65
CERTIFICATE OF COMPLIANCE	66

TABLE OF AUTHORITIES*

Cases

<i>Abdelfattah v. U.S. Dep't of Homeland Sec.</i> , 787 F.3d 524 (D.C. Cir. 2015)	32
* <i>Action for Children's Television v. FCC</i> , 59 F.3d 1249 (D.C. Cir. 1995)	31
<i>Air Transp. Ass'n v. U.S. Dep't of Agric.</i> , 37 F.4th 667 (D.C. Cir. 2022)	52
<i>Archer W. Contractors, LLC v. U.S. Dep't of Transp.</i> , 45 F.4th 1 (D.C. Cir. 2022)	25
<i>Art Metal-U.S.A., Inc. v. United States</i> , 753 F.2d 1151 (D.C. Cir. 1985)	37
<i>AT&T Corp. v. FCC</i> , 323 F.3d 1081 (D.C. Cir. 2003)	2, 7, 30
<i>Atlas Roofing Co., Inc. v. OSHA</i> , 430 U.S. 442 (1977)	38
<i>Burlington N. & Santa Fey Ry. Co. v. Whyte</i> , 548 U.S. 53 (2006)	48
<i>Cellco P'Ship v. FCC</i> , 357 F.3d 88 (D.C. Cir. 2004)	25
<i>Concrete Pipe and Prods. of Cal., Inc. v. Constr. Laborers Pension Tr. for So. Cal.</i> , 508 U.S. 602 (1993)	42
<i>Crooks v. Mabus</i> , 845 F.3d 412 (D.C. Cir. 2016)	25

* *Authorities upon which we chiefly rely are marked with asterisks.*

TABLE OF AUTHORITIES
(continued)

	Page(s)
<i>Crowell v. Benson</i> , 285 U.S. 22 (1932)	39
<i>Facebook, Inc. v. Duguid</i> , 592 U.S. 395 (2021)	50, 51
<i>Fogo De Chao (Holdings) Inc. v. U.S. Dep’t of Homeland Sec.</i> , 769 F.3d 1127 (D.C. Cir. 2014)	42
<i>Grid Radio v. FCC</i> , 278 F.3d 1314 (D.C. Cir. 2002)	25
<i>Ill. Citizens Comm. for Broad. v. FCC</i> , 515 F.2d 397 (D.C. Cir. 1974)	30
<i>In re Zdravkovich</i> , 634 F.3d 574 (D.C. Cir. 2011)	42
<i>Landry v. New Amsterdam Cas. Co.</i> , 279 F.2d 214 (5th Cir. 1960) (per curiam)	32
* <i>Lockhart v. United States</i> , 577 U.S. 347 (2016)	50, 51
<i>Loper Bright Enters. v. Raimondo</i> , 603 U.S. 369 (2024)	24
<i>Meta Platforms, Inc. v. FTC</i> , 723 F. Supp. 3d 64 (D.D.C. 2024)	32
<i>Miss. Comm’n on Env’t Quality v. EPA</i> , 790 F.3d 138 (D.C. Cir. 2015)	55
<i>Munn v. Illinois</i> , 94 U.S. 113 (1877)	38, 39
<i>Nat’l Broad. Co. v. FCC</i> , 516 F.2d 1101 (D.C. Cir. 1974)	40

TABLE OF AUTHORITIES
(continued)

	Page(s)
<i>Nat’l Lifeline Ass’n v. FCC</i> , 983 F.3d 498 (D.C. Cir. 2020)	24
<i>NetworkIP, LLC v. FCC</i> , 548 F.3d 116 (D.C. Cir. 2008)	56
<i>Neustar, Inc. v. FCC</i> , 857 F.3d 886 (D.C. Cir. 2017)	55
<i>Oil States Energy Servs. v. Greene’s Energy Grp.</i> , 584 U.S. 325 (2018)	40, 41
<i>Qassim v. Trump</i> , 927 F.3d 522 (D.C. Cir. 2019)	33
<i>Rodriguez de Quijas v. Shearson/American Express, Inc.</i> , 490 U.S. 477 (1989)	41
<i>Sanchez v. Office of State Superintendent of Ed.</i> , 45 F.4th 388 (D.C. Cir. 2022)	32
<i>Scripps-Howard Radio v. FCC</i> , 316 U.S. 4 (1942)	39
* <i>SEC v. Jarkesy</i> , 603 U.S. 109 (2024)	34, 35, 37, 38, 39, 40
* <i>Tull v. United States</i> , 481 U.S. 412 (1987)	34, 35, 36
<i>Wash. State Grange v. Wash. State Republican Party</i> , 552 U.S. 442 (2008)	32
<i>Willard v. Fairfield So. Co., Inc.</i> , 472 F.3d 817 (11th Cir. 2006)	38
<i>Withrow v. Larkin</i> , 421 U.S. 35 (1975)	42

TABLE OF AUTHORITIES
(continued)

	Page(s)
Statutes	
28 U.S.C. § 2342.....	2, 30, 33
28 U.S.C. § 2462.....	33
47 U.S.C. § 153.....	45
47 U.S.C. § 217.....	5
* 47 U.S.C. § 222	4, 5, 17, 27, 44, 48, 52
47 U.S.C. § 301.....	40
47 U.S.C. § 402.....	2, 30
* 47 U.S.C. § 503	6, 7, 63
* 47 U.S.C. § 504	7, 29, 30, 36
Regulations	
47 C.F.R. § 1.80.....	63
47 C.F.R. § 64.2003.....	5
47 C.F.R. § 64.2007.....	5
47 C.F.R. § 64.2010.....	6, 36
Administrative Materials	
<i>Advantage Telecomms. Corp.</i> , 32 FCC Rcd 3723 (2017)	62
<i>Amendment of Section 1.80(b) of the Commission’s Rules</i> , 34 FCC Rcd 12,824 (2019)	62

TABLE OF AUTHORITIES
(continued)

	Page(s)
Declaratory Ruling, <i>Implementation of the Telecommunications Act of 1996</i> , 28 FCC Rcd 9609 (2013)	47
Order on Reconsideration, <i>Implementation of the Telecommunications Act of 1996</i> , 14 FCC Rcd 14,409 (1999)	47
<i>Preferred Long Distance, Inc.</i> , 30 FCC Rcd 13,711 (2015)	62
<i>Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information</i> , 22 FCC Rcd 6927 (2007)	6
 Other Materials	
Geoffrey Starks, <i>Why It's So Easy for a Bounty Hunter to Find You</i> , N.Y. Times (Apr. 2, 2019).....	42
Jennifer Valentino-DeVries, <i>Service Meant to Monitor Inmates' Calls Could Track You, Too</i> , N.Y. Times (May 10, 2018) 11, 22, 23, 59	
Joseph Cox, <i>I Gave a Bounty Hunter \$300. Then He Located Our Phone</i> , Motherboard, Jan. 8, 2019.....	13
T-Mobile US, Inc. Form 10-K.....	7

GLOSSARY

APA	Administrative Procedure Act
CPNI	Customer Proprietary Network Information
LBS	Location-Based Service
NAL	Notice of Apparent Liability

No. 24-1224 & No. 24-1225

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

SPRINT CORPORATION,
T-MOBILE USA, INC.,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION
and UNITED STATES OF AMERICA,

Respondents.

On Petitions for Review of Orders of
the Federal Communications Commission

BRIEF FOR RESPONDENTS

INTRODUCTION

Respondent Federal Communications Commission (the “FCC” or the “Commission”) assessed monetary forfeitures against Petitioners Sprint Corporation and T-Mobile USA, Inc. (the “Carriers”) for violating the Communications Act by endangering the sensitive location information of tens of millions of their customers. The violations arose from the Carriers’ “location-based services” programs, through which

third parties offered customers a variety of services based on their real-time locations. The Carriers relied on an attenuated chain of contract provisions—which they failed to enforce—to protect against misuse of their customers’ location data. Those measures did not work. When news broke that a location-based service provider had allowed a sheriff in Missouri to illegally track people without their consent, it became clear that the Carriers were not meaningfully in control of their customers’ location information. Yet the Carriers were slow to act, and continued sharing customer location data with dozens of third parties for as much as a year after learning their safeguards were ineffective. In assessing the forfeitures, the Commission found that the Carriers had failed to take reasonable steps to discover and protect against misuse of their customers’ information, as the Communications Act and FCC regulations require.

JURISDICTIONAL STATEMENT

The Commission released the forfeiture orders under review on April 29, 2024. This Court has held that it has jurisdiction under 28 U.S.C. § 2342(1) and 47 U.S.C. § 402(a) to review FCC forfeiture orders so long as the assessed forfeiture has been paid. *See AT&T Corp. v. FCC*, 323 F.3d 1081, 1085 (D.C. Cir. 2003). Petitioners paid the assessed

forfeitures on May 28, 2024, and filed timely petitions for review on June 27, 2024.

STATEMENT OF THE ISSUES

1. Did the Commission act constitutionally in issuing the Orders? Specifically:

(a) Were Sprint and T-Mobile's Seventh Amendment rights satisfied where the carriers paid the assessed forfeitures rather than requiring the Government to bring a *de novo* action for recovery in district court?

(b) Do claims involving the enforcement of regulations protecting information about telecommunications customers fall outside the Seventh Amendment right to a civil jury trial? and

(c) Did the Commission afford Sprint and T-Mobile due process, when settled law permits agencies to both investigate and assess forfeitures against regulated entities, and when the Carriers have not demonstrated that any Commissioner had prejudged the outcome of the Commission's investigation?

2. Did the Commission correctly determine that information about the location of wireless customers is “customer proprietary network information” within the meaning of the Communications Act?

3. Was the Commission’s forfeiture determination reasonable, where Sprint and T-Mobile exposed the location data of tens of millions of their customers to dozens of third parties without effective safeguards?

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes and regulations are set forth in the statutory addendum bound with this brief.

STATEMENT OF THE CASE

I. STATUTORY AND REGULATORY BACKGROUND.

A. Protecting Customer Proprietary Network Information.

The Communications Act requires “[e]very telecommunications carrier . . . to protect the confidentiality of propriety information of, and relating to” its customers. 47 U.S.C. § 222(a). This includes a category of information called “customer proprietary network information” (“CPNI”), which is “information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service,” and “is made available to the carrier by the

customer solely by virtue of the carrier–customer relationship[.]” *Id.* § 222(h)(1)(A).

Section 222(c)(1) allows carriers to disclose a customer’s individually identifiable CPNI to provide telecommunications service (or services necessary to or used in the provision of telecommunications service), but otherwise generally prohibits such disclosure “[e]xcept as required by law or with the approval of the customer[.]” *See* 47 U.S.C. § 222(c)(1). And to ensure that carriers cannot offload their obligations to a third party, “the act, omission, or failure of any officer, agent, or other person acting for or employed by” the carrier and “acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure, of such carrier” *Id.* § 217.

Similarly, except for certain marketing communications, FCC regulations generally require a customer’s “affirmative, express consent” for carriers to “use, disclose, or permit access to [their] customer[s] individually identifiable CPNI.” 47 C.F.R. §§ 64.2007(b) (requiring “opt-in approval” for CPNI disclosures), 64.2003(k) (defining “opt-in approval”). Carriers must also “take reasonable measures to discover and

protect against attempts to gain unauthorized access to CPNI.” *Id.* § 64.2010(a).

The Commission has been particularly concerned about carriers sharing customer information with third parties, because once CPNI is shared, a “carrier no longer has control over it and thus the potential for loss of this data is heightened.” *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd 6927, 6948, ¶ 39 (2007). Accordingly, it has made clear that “a carrier’s [S]ection 222 duty to protect CPNI extends to situations where a carrier shares CPNI with its joint venture partners and independent contractors.” *Id.*

B. The FCC’s Forfeiture Authority.

Anyone who “willfully or repeatedly fail[s] to comply” with the Communications Act or “any rule, regulation, or order issued by the Commission” “shall be liable to the United States for a forfeiture penalty.” 47 U.S.C. § 503(b)(1)(B). Congress has established two alternative procedures governing the FCC’s assessment of a monetary forfeiture.

First, the Commission may refer an alleged violation to an administrative law judge for a hearing. *Id.* § 503(b)(3)(A). Any person

ordered to pay a forfeiture at the end of that proceeding may obtain review in a court of appeals. *Id.*

Alternatively, the Commission may issue a “notice of apparent liability” to the alleged violator, who then has “an opportunity to show, in writing . . . why no . . . forfeiture penalty should be imposed.” *Id.* § 503(b)(4)(A), (C). If the Commission does assess a forfeiture, a party can pay it and then file a petition for review in a court of appeals. *See AT&T Corp.*, 323 F.3d at 1083. If the subject of the forfeiture does not pay, the Government may sue to recover the forfeiture in a “trial de novo” in district court. 47 U.S.C. § 504(a).

II. FACTUAL BACKGROUND AND PROCEEDINGS BELOW.

T-Mobile is the second largest wireless carrier in the United States. In 2023, it had 119.7 million customers, and generated more than \$78.5 billion in revenue. *See* T-Mobile US, Inc. Form 10-K at 5, 34.¹ It merged with Sprint—another major wireless carrier—in 2020. In 2018, news reports revealed that Sprint and T-Mobile had allowed third parties to

¹ <https://www.sec.gov/Archives/edgar/data/1283699/000128369924000008/tmus-20231231.htm>.

access data regarding the location of their customers without their consent, and failed to stop illegal misuse of that information.

A. The Carriers' Location-Based Services Programs.

Sprint and T-Mobile gave access to their customers' location information to third parties that made location-based services like "roadside assistance, medical emergency alerts, and bank fraud prevention" available to the Carriers' customers. Notice of Apparent Liability ("*Sprint NAL*"), *Sprint Corporation*, 35 FCC Rcd 1655, 1661, ¶ 11 (2020); Notice of Apparent Liability ("*T-Mobile NAL*"), *T-Mobile USA, Inc.*, 35 FCC Rcd 1786, 1791, ¶ 13 (2020) (JA367; 127). The Carriers would determine their customers' locations based on which cellular towers were communicating with their devices and then sell that information to "location information aggregators," which would then resell the customers' location information to companies that actually provided the location-based services (or, in some instances, to additional intermediaries). *E.g.*, *T-Mobile NAL* ¶ 13 (JA127).

Sprint had a certification process that "required the Aggregators to test the sub-aggregators and location-based service providers' applications to ensure they met" Sprint's requirements, and aggregators

were supposed to obtain Sprint’s advance written consent before sharing location data with a sub-aggregator. Forfeiture Order (“*Sprint Order*”), *Sprint Corporation*, 39 FCC Rcd 4305 ¶ 10 (Apr. 29, 2024) (quotation marks omitted) (JA290). Similarly, T-Mobile required aggregators to provide information about service providers’ proposed use of customer location data before disclosing it to them. Forfeiture Order (“*T-Mobile Order*”), *T-Mobile USA, Inc.*, 39 FCC Rcd 435 ¶ 10 (JA5). Once T-Mobile approved a particular data-use “campaign,” *id.*, it generated a specific ID that was “used by the [location-based service] provider for every location information request it submitted to the Aggregator, and then likewise transmitted from the Aggregator to T-Mobile,” allowing T-Mobile to track a campaign. *Id.*

The Carriers also required the providers that used their customers’ data to obtain customer consent first. *E.g.*, *Sprint NAL* ¶ 15; *T-Mobile NAL* ¶ 62 (JA369; 141). But neither Sprint nor T-Mobile contracted directly with those providers. *Sprint NAL* ¶ 16; *T-Mobile NAL* ¶ 15 (JA370; 128). Instead, they delegated to the aggregators—with which they did have contracts—the responsibility to ensure that service providers and sub-aggregators had the proper permissions to use

customer locations, and that customers’ data was not misused. *Sprint Order* ¶¶ 9, 48; *T-Mobile Order* ¶¶ 9, 47 (JA290, 306; 5, 20). T-Mobile “did not independently verify the customers’ consent before providing access to the location data,” and “Sprint itself did not notify customers and collect affirmative customer consent for the disclosure of customer location information.” *T-Mobile Order* ¶ 9; *Sprint Order* ¶ 9 (JA5; 290).

Under their contracts with aggregators, Sprint and T-Mobile had “broad authority” to “quickly terminate access to customer location information,” and they had the power to conduct “audits and other internal reviews” of their programs. *Sprint Order* ¶¶ 11, 12; *T-Mobile Order* ¶¶ 10, 12 (JA291; 5, 6).

B. The Misuse of Sprint and T-Mobile Customers’ Data.

a. On May 10, 2018, the *New York Times* reported that a Missouri deputy sheriff named Cory Hutcheson had illegally monitored hundreds of people—including other law-enforcement officers and a judge, *e.g.*, *T-Mobile NAL* ¶ 28 (JA132)—using a location-based service provided by a company called Securus. Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates’ Calls Could Track You, Too* (“Securus

Article”), N.Y. Times (May 10, 2018).² Securus obtained customer location data from an aggregator called LocationSmart, by way of a sub-aggregator called 3Cinteractive, and used it to “enable[] law enforcement and corrections officials to access the location” of wireless customers “*without* the device owner’s knowledge or consent[.]” *Sprint NAL* ¶¶ 22, 20 (emphasis in original); *T-Mobile NAL* ¶ 27 (JA371, 372; 131).

Ostensibly, Securus required its users to upload a copy of the particular legal process that authorized a given request and certify that “the attached document is an official document giving permission to look up the location [of the] phone number requested.” *Sprint Order* ¶ 14 (JA293); Government’s Sentencing Mem. at 3, *United States v. Hutcheson*, No. 18-CR-00041 JAR (E.D. Mo. Apr. 23, 2019) (ECF No. 2086715) (JA185). But in practice, as soon as a user submitted a query, Securus would “*immediately* provide the requested location information (regardless of the adequacy of the uploaded document).” *T-Mobile Order* ¶ 15 (emphasis in original) (JA8). Hutcheson was able to submit fraudulent location requests using completely irrelevant documents like

² <https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html>.

his health insurance policy. *Sprint Order* ¶ 14; *T-Mobile Order* ¶ 15; Sentencing Mem. at 4 (JA293; 8; 186).

Both Sprint and T-Mobile’s customers were among those Hutcheson targeted. *Sprint NAL* ¶¶ 20, 47; *T-Mobile NAL* ¶¶ 27, 50 (JA371, 379; 131, 137–38). Yet none of the Carriers’ controls alerted them to Hutcheson’s activities or Securus’s tracking program. *See Sprint NAL* ¶ 22; *T-Mobile NAL* ¶¶ 29–30 (JA372; 132–33). Indeed, Securus’s service was “outside the scope of both Securus’s stated purpose for accessing” customers’ locations “and any agreement with” any aggregator, and its tracking program had not been reviewed by Sprint or T-Mobile. *Sprint Order* ¶ 13; *T-Mobile Order* ¶ 14 (JA292; 7).

b. More than seven months after the *Times* ran its story on Securus’s misuse of customer data, a different outlet reported that wireless customers’ location data was being “sold and resold, with little or no oversight, within the bail bonds industry,” leading to “consumers being tracked without their knowledge or consent.” *Sprint Order* ¶ 18; *T-Mobile Order* ¶ 17 (JA294; 8); Joseph Cox, *I Gave a Bounty Hunter \$300. Then He Located Our Phone* (“*MicroBilt Article*”), Motherboard,

Jan. 8, 2019.³ According to that report, a company called MicroBilt was buying access to location data from Zumigo, one of the aggregators Sprint and T-Mobile contracted with, “and then sell[ing] it to a dizzying number of sectors, including landlords to scope out potential renters; motor vehicle salesmen, and others who are conducting credit checks.” *MicroBilt Article*. “Armed with just a phone number,” MicroBilt could “return a target’s full name and address, geolocate a phone in an individual instance, or operate as a continuous tracking service.” *Id.* See also generally *Sprint Order* ¶ 18; *T-Mobile Order* ¶ 17 (JA294; 8).

T-Mobile knew MicroBilt had access to its customers’ data because it had “reviewed and approved a location-based service campaign” for MicroBilt. See Email from David Solomon, Wilkinson Barker Knauer LLP, to Michael Epshteyn & Rosemary Cabral, FCC Enforcement Bureau (Jan. 28, 2019) (JA196). But T-Mobile explained to the Commission that MicroBilt never mentioned it would disclose location information to third parties. *T-Mobile Order* ¶ 17 (JA8).

³ <https://www.vice.com/en/article/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile/>.

For its part, Sprint was “entirely unaware that Zumigo was providing [location based] services to MicroBilt,” “was unable to identify any record of Zumigo obtaining Sprint’s prior written consent before using MicroBilt,” “was unable to verify whether Sprint’s own credentialing process had been followed with respect to MicroBilt,” and “had no information about whether MicroBilt complied with Sprint’s notice-and-consent processes.” *Sprint Order* ¶ 18 (quotation marks omitted) (JA294).

c. Although the Securus and MicroBilt incidents made clear that the Carriers’ safeguards were inadequate, *see T-Mobile Order* ¶ 53 (JA22), they were not T-Mobile’s first encounter with abuse of customer location data. In July 2017, even before Securus and MicroBilt’s abuses of customer location data were revealed, T-Mobile “learned” “through a third party,” Final Resp. of T-Mobile USA, Inc. to Sept. 13, 2018 Letter of Inquiry at 17 (JA225), that an unknown location-based service provider was “using an obfuscated website domain to provide wireless device-tracking services to bail bond and similar companies without the wireless customer’s authorization.” *T-Mobile Order* ¶ 13 (quotation marks omitted) (JA6). T-Mobile determined the culprit was a company

called LocateUrCell, which was authorized to receive customer location data to locate missing phones. *Id.* T-Mobile “concedes that LocateUrCell’s unauthorized disclosures were made possible and remained hidden” because the relevant requests “were hosted on the same system and used the same campaign ID as . . . authorized requests,” so “T-Mobile could not differentiate between location information requests for the authorized LocateUrCell phone-finding service from location information requests for the unauthorized tracking service.” *Id.* (quotation marks and modifications omitted).

C. The Carriers’ Responses to the Securus and MicroBilt News.

A week after the *Securus Article* was published, Sprint cancelled Securus’s access to customer location information. *Sprint Order* ¶ 15 (JA293). A few days later, it suspended LocationSmart from its location-based services program, and in June, Sprint terminated its contracts with LocationSmart and Zumigo. *Id.* However, it renewed those contracts in August. *Id.* ¶ 17 (JA294). Sprint placed greater restrictions on LocationSmart’s access to customer data, but it renewed its contract with Zumigo “in its entirety[.]” *Id.* This meant that, “unlike LocationSmart, all

of Zumigo’s prior location-based service provider clients again had access to Sprint’s customer location information.” *Id.* (quotation marks omitted).

T-Mobile cut off Securus and 3Cinteractive’s access to its customer location data the day after the *Times* story was published. *T-Mobile Order* ¶ 16 (JA8). On October 26, T-Mobile notified the aggregators that it would not renew their contracts when they expired the following March. *Id.* On January 4, 2019, Zumigo informed T-Mobile that it had suspended MicroBilt’s access to customer location data, and T-Mobile permanently disabled Zumigo’s access to customer location information for purposes of transmitting it to MicroBilt. *T-Mobile Order* ¶ 17 (JA8).

T-Mobile’s location-based service program ultimately came to an end on February 8, 2019—275 days after the *Securus Article* appeared, and Sprint’s program ended on May 31, 2019—more than a year after the story was published. *T-Mobile Order* ¶ 18; *Sprint Order* ¶ 19 (JA9; 295).

D. The Orders Under Review.

The Commission began an investigation immediately after the *Securus Article*’s publication, and in 2020, it issued notices of apparent liability to Sprint and T-Mobile for disclosing CPNI in the form of customer location data without customer consent, and failing to take

reasonable measures to protect against unauthorized access to that CPNI. *Sprint NAL*, ¶¶ 32, 46, 55; *T-Mobile NAL* ¶¶ 38, 49, 58 (JA375, 381, 379; 134, 137, 140). In 2024, after considering Sprint and T-Mobile’s responses and completing its investigation, the Commission issued the *Orders* under review.

1. The Commission Finds That Location Data is CPNI.

In the *Orders*, the Commission first determined that customer location data “falls squarely within” the statutory definition of CPNI, which includes information (i) that “relates to the . . . *location*, and amount of use of a telecommunications service,” and (ii) that a carrier obtains “solely by virtue of the carrier–customer relationship.” *Sprint Order* ¶ 23 (emphasis in *Order*) (quoting 47 U.S.C. § 222(h)(1)(A)); *T-Mobile Order* ¶ 24 (emphasis in *Order*) (quoting same provision) (JA296; 10). In finding that customer location data “relates to’ the location of” Sprint and T-Mobile’s “telecommunications services,” *Sprint Order* ¶ 26; *T-Mobile Order* ¶ 23 (JA297; 10), the Commission explained that “[a] wireless mobile device undergoes an authentication and attachment process to the carrier’s network, via the closest towers,” and that whether a device is “connected (sending/receiving data/voice)” or

“idle,” “the carrier must be aware of and use the device’s location in order for it to enable customers to send and receive calls.” *Sprint Order* ¶ 24; *T-Mobile Order* ¶ 23 (JA296; 10). Sprint and T-Mobile customers “provided their wireless location data” to the companies “because of their customer–carrier relationship,” and “customer[s] ha[ve] no choice but to reveal [their] location” to Sprint or T-Mobile. *Sprint Order* ¶¶ 29, 31; *T-Mobile Order* ¶¶ 28, 30 (JA298, 299; 12–13).

2. The Commission’s Liability Findings.

Having concluded that customer location information is CPNI, the Commission found that both Sprint and T-Mobile had violated the Communications Act and FCC regulations by improperly disclosing that information, and failing to take reasonable steps to discover and protect against its misuse. In terms of improper disclosure, not only did Sprint and T-Mobile make customer data available to Hutcheson without consent, *Sprint NAL* ¶ 48; *T-Mobile NAL* ¶ 51 (JA379; 138), but the Commission found that “*every time*” Sprint or T-Mobile provided location information to Securus “under the guise of its approved use case,” “a separate, unauthorized disclosure occurred.” *Sprint Order* ¶ 42 (emphasis added); *see also T-Mobile Order* ¶ 42 (JA304; 18).

The Commission also found that, both before and after the Securus/Hutcheson incident was reported, Sprint and T-Mobile failed to take reasonable measures to protect their customers' location information. Both carriers' safeguards relied "almost entirely upon contractual agreement[s], passed on to location-based service providers through an attenuated chain of downstream contracts[.]" *Sprint Order* ¶ 48; *T-Mobile Order* ¶ 47 (JA306; 20). For this arrangement to have been effective, Sprint and T-Mobile "would have needed to take steps to determine whether" their requirements "were actually being followed," and "would have had to have a way of distinguishing between a legitimate request for customer location information . . . and an illegitimate one" *Sprint Order* ¶ 48; *T-Mobile Order* ¶ 48 (JA306; 21). But the Commission's investigation revealed no evidence that either carrier "made any meaningful efforts" or "could effectively distinguish between valid and unauthorized requests for location information." *Sprint Order* ¶ 48; *T-Mobile Order* ¶ 48 (JA306; 21).

On the contrary, T-Mobile's use of campaign-specific IDs—which was "simply a technology-based variant of the honor system on which T-Mobile's other safeguards depended," "was vulnerable to the

predictable risk that a third party would use an approved campaign ID to mask location requests made for an unapproved purpose.” *T-Mobile Order* ¶ 51; *T-Mobile NAL* ¶ 71 (JA22; 144). Sure enough, “[a]s T-Mobile learned with the LocateUrCell incident in July 2017, where authorized and unauthorized services used the same campaign-specific ID,” T-Mobile could not “readily distinguish the unauthorized data requests from the authorized ones.” *T-Mobile Order* ¶ 51 (JA22). Likewise, Sprint had no idea MicroBilt had access to its customers’ data, and had no record of authorizing that access. *Sprint Order* ¶ 18 (JA294).

The Carriers also were unable to control entities that received their customers’ data. When they began investigating the Securus incident, neither Sprint nor T-Mobile was able to compel Securus to cooperate. *Sprint Order* ¶ 48; *T-Mobile Order* ¶ 50 (JA306; 21–22). And when the MicroBilt disclosures were revealed, the aggregator Zumigo ignored Sprint’s request for more information about its relationship with MicroBilt. *Sprint Order* ¶¶ 18, 48 (JA294–95, 306). The Commission found that if Sprint and T-Mobile could not secure the cooperation of entities downstream of their contracts with aggregators, then their contracts did not adequately protect customer information. “Whatever a

company’s justification for denying or ignoring . . . requests for information,” the Commission observed, “the refusals are further evidence” that Sprint and T-Mobile “disclosed CPNI to third parties over which [they] had little or no control or authority.” *Sprint Order* ¶ 48; *T-Mobile Order* ¶ 50 (JA306; 22).

The Carriers failed to correct the problems with their location programs within a reasonable time. While the *Securus Article* made them “keenly aware of the inadequacy of [their] safeguards,” they “did not . . . demonstrate that [their] safeguards were made reasonable in the months that followed” the article’s publication. *Sprint Order* ¶ 49; *T-Mobile Order* ¶ 53 (JA306; 22). Instead, they “continued to sell access to [their] customers’ location information under (for all intents and purposes) the *same system* that was exploited by Securus and Hutcheson.” *Sprint Order* ¶ 49 (emphasis in original); *T-Mobile Order* ¶ 53 (emphasis in original) (JA306; 22).

Rather than “deploying enhanced measures to verify consumer consent (even directly verifying consumer consent)” or “shutting down the [location-based services] program,” the Carriers “instead took piecemeal steps” that “did not rectify the systemic vulnerabilities at the

heart of” their programs. *Sprint Order* ¶ 53; *T-Mobile Order* ¶ 58 (JA308; 25). For instance, T-Mobile “worked towards implementing an enhanced notice and consent mechanism,” but it “was never deployed” because T-Mobile and the aggregators could not make it work. *T-Mobile Order* ¶ 55 (JA23). Sprint “suspended location information sharing with LocationSmart,” but “undermined this step by reinstating LocationSmart (and two of its customers) into the program three months later.” *Sprint Order* ¶ 51. (quotation marks omitted) (JA307). And “new procedures that Sprint developed for use in conjunction with the contractual protections failed to address key weaknesses with Sprint’s location-based services program,” with “little evidence that Sprint actually followed through with these policies in a way that had any meaningful impact.” *Id.* (quotation marks omitted) (JA308). Moreover, the MicroBilt incident—which was reported more than seven months after the *Securus Article*—“perfectly illustrates the vulnerability that remained in Sprint’s aggregator program,” because Sprint’s post-*Securus* improvements failed to “detect the presence of an apparently unauthorized location-based service provider,” or “prevent that entity from obtaining Sprint’s customer location information without consent.” *Id.* (JA308).

Finally, the Commission found that these failures, over “a protracted amount of time,” also jeopardized national security and public safety by making it possible “for malicious persons to identify the exact locations of” Sprint and T-Mobile customers “who belong to law enforcement, military, government, or other highly sensitive positions,” as Hutcheson did. *Sprint Order* ¶ 72; *T-Mobile Order* ¶ 92 (JA315; 39).

3. The Forfeitures.

For their violations, the Commission fined T-Mobile \$80,080,000 and Sprint \$12,240,000. *T-Mobile Order* ¶ 74; *Sprint Order* ¶ 62 (JA33; 312). The Commission concluded the Carriers committed a separate violation for each third party to which it had provided access to inadequately protected customer location data, and that each violation continued “every day that each related [location-based service] provider operated in the apparent absence of reasonable measures to protect CPNI[.]” *Sprint Order* ¶¶ 64, 68; *T-Mobile Order* ¶¶ 77, 81 (JA 312, 314; 34, 35). *See also Sprint NAL* ¶ 80 (JA390); *T-Mobile NAL* ¶ 83 (JA147). Starting from 30 days after the publication of the *Securus Article*, the Commission assessed a base forfeiture of \$40,000 per third party for the first day of violation, plus \$2,500 per third party per day for each

subsequent day. *Sprint NAL* ¶ 80; *T-Mobile NAL* ¶ 83 (JA390; 147). Next, applying its forfeiture guidelines, the Commission imposed a 75% upward adjustment to T-Mobile’s fine and a 100% upward adjustment to Sprint’s. *T-Mobile NAL* ¶ 90; *Sprint NAL* ¶ 86 (JA150; 391). Finally, the Commission reduced T-Mobile’s forfeiture by \$11,550,000 (from the originally proposed \$91,630,000) based on an initial miscounting of the entities that received customer data and additional details about the dates T-Mobile terminated certain contracts. *T-Mobile Order* ¶¶ 94–95 (JA40).

Sprint and T-Mobile paid their forfeitures on May 28, 2024, and then filed petitions for review in this Court. (Sprint Pet’n for Rev. at 1 n.2, (ECF No. 2062068); T-Mobile Pet’n for Rev. at 1 n.*, *T-Mobile USA, Inc. v. FCC*, No. 24-1225 (ECF No. 2062080).) The cases were subsequently consolidated. (ECF No. 2069454 (Aug. 12, 2024).)

STANDARDS OF REVIEW

Constitutional challenges to agency actions are reviewed *de novo*. *Nat’l Lifeline Ass’n v. FCC*, 983 F.3d 498, 507 (D.C. Cir. 2020). In determining the best reading of a statute, the Court may “seek aid from the interpretations of those responsible for implementing particular statutes.” *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 394 (2024).

Under the Administrative Procedure Act’s (“APA”) arbitrary-and-capricious standard, the Court will “presume[] the validity of agency action”—including an enforcement action—and “affirm unless the Commission failed to consider relevant factors or made a clear error in judgment[.]” *Cellco P’Ship v. FCC*, 357 F.3d 88, 93–94 (D.C. Cir. 2004); *Grid Radio v. FCC*, 278 F.3d 1314, 1322 (D.C. Cir. 2002). The Court reviews agency factual findings for substantial evidence, which means “more than a scintilla of evidence.” *Archer W. Contractors, LLC v. U.S. Dep’t of Transp.*, 45 F.4th 1, 6 (D.C. Cir. 2022). In doing so, the Court does “does not substitute its judgment for that of the agency,” but reviews it “to ensure that it was reasonable and reasonably explained.” *Crooks v. Mabus*, 845 F.3d 412, 423 (D.C. Cir. 2016).

SUMMARY OF THE ARGUMENT

The Commission acted well within its authority under the Constitution and the Communications Act to assess monetary forfeitures against two major wireless carriers for their failure to take reasonable steps to discover and protect against serious misuse of their customers’ location data by third parties.

I. The *Orders* are constitutional.

a. The Communications Act's forfeiture provisions do not violate the Seventh Amendment right to a jury trial. The statute requires the Government to bring an action in district court in order to recover an unpaid forfeiture, but Sprint and T-Mobile waived that option by paying their fines so they could challenge the *Orders* in this Court.

Suits to enforce CPNI regulations are also not the kind of common-law claim to which the Seventh Amendment applies. A CPNI enforcement action has no common-law analogue and falls within the "public rights" exception to the jury right, both because it involves the regulation of common carriers and because CPNI regulations are part of a scheme governing access to radio spectrum, a public resource.

b. The *Orders* did not offend separation-of-powers principles. Under well-settled Supreme Court precedent, an agency can investigate regulated entities and fine those entities for violations. The Carriers suggest that precedent should be reconsidered, but only the Supreme Court may do that.

c. The Commission did not impermissibly prejudge the Carriers' case. One Commissioner wrote an op-ed urging the FCC to act quickly in response to the Securus incident, but nothing in his article suggested a

refusal to consider the facts or change his views. And the fact that same Commissioner and one other critiqued the computation of fines in individual statements accompanying earlier orders did not suggest their minds—much less the collective view of the Commission—were irrevocably made up.

II. The Commission also correctly found that customer location data falls within the definition of CPNI because it “relates” to the “location” of a telecommunications service. 47 U.S.C. § 222(h)(1). The Carriers argue that the statute applies only to location data generated by the customer’s *use* of a telecommunications service, and thus only protects customers when they are making a phone call. That reading is inconsistent with canons of construction, would produce anomalous results, and ignores the Commission’s conclusion that carriers use customer location data to support the provision of telecommunications service to their customers whether or not a customer is actively making a call. Similarly, the Carriers argue that because they provide both telecommunications and non-telecommunications services, they did not receive customer data “solely” through the customer–*carrier* relationship. But the Carriers’ relationship with their customers was their sole source of access to customer location data, and their argument would allow

carriers to circumvent CPNI regulations just by including non-telecommunications service with their voice offering—a result Congress cannot have intended.

Finally, the Carriers were not denied fair notice of their obligations, because the most natural reading of the statute is that CPNI protections apply to customer location data.

III. The Commission’s finding that the Carriers did not take reasonable measures to protect customer location data is supported by substantial evidence. The Carriers do not dispute the underlying facts; they simply disagree with the Commission’s conclusions, but that is no basis for reversal where those conclusions were well supported. Nor were the Commission’s fines arbitrary or capricious. The Commission reasonably determined that the Carriers committed a discrete violation of the CPNI rules each time they provided a third party access to poorly protected customer data, and it applied reasonable penalties—based on Commission precedent and well below the statutory limit—for each day it found the Carriers failed to correct the serious problems that had been exposed in their management of customer data.

ARGUMENT

I. THE COMMISSION DID NOT VIOLATE THE CARRIERS' CONSTITUTIONAL RIGHTS.

A. The Commission's Forfeiture Authority Does Not Violate the Seventh Amendment.

“In suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved[.]” U.S. Const. amend. VII. The statutory mechanism the Commission employed to assess forfeitures in this case accords with this right.

1. Sprint and T-Mobile Had the Right to a Trial in District Court Before Paying the Commission's Forfeitures.

The Communications Act requires the Government to bring suit in the form of a trial *de novo* in district court before it can recover an FCC forfeiture. 47 U.S.C. § 504(a); *see also, e.g., T-Mobile Order* ¶ 104 (JA44). So even to the extent the Seventh Amendment applies in a forfeiture action, nothing prevented the Carriers from receiving a jury trial before paying a forfeiture. Instead, they waived that right by paying the forfeitures (albeit “under protest”) so they could challenge the *Orders*

directly in this Court.⁴ *See Ill. Citizens Comm. for Broad. v. FCC*, 515 F.2d 397, 401, 405–06 (D.C. Cir. 1974) (noting that “a jury trial was available but was waived” where FCC licensee paid a forfeiture “[d]espite its belief that the Commission’s action was illegal”).

The Carriers acknowledge (Br. 35) that the Government can recover an unpaid forfeiture only following a trial *de novo* in district court. 47 U.S.C. § 504(a). And by their own reading of this Court’s precedent, “all issues” raised in a forfeiture order “would be subject to *de novo* review” in such a trial. (Br. 35 (citing *AT&T Corp.*, 323 F.3d at 1083–85).) Thus, even if the Carriers are correct that recovery of a CPNI forfeiture implicates the right to a jury trial, they could have had one—in an Article III court—if they had waited for the Government to bring a forfeiture recovery action. This would not have forced the Carriers to “play the part of a scofflaw.” (Br. 36.) On the contrary, this Court has confirmed that the subject of an FCC forfeiture “need do nothing at all until it is served with a complaint, at which point it is entitled to a trial

⁴ This Court has held that it does not have original jurisdiction under 47 U.S.C. § 402 and 28 U.S.C. § 2342(1) to review orders assessing forfeitures that have not yet been paid. *See AT&T Corp.*, 323 F.3d at 1085.

de novo in district court.” *Action for Children’s Television v. FCC*, 59 F.3d 1249, 1261 (D.C. Cir. 1995).

The Carriers worry that, if forced to wait to be sued, they could suffer “reputational injury” and the Commission could hold the facts of these cases against them in future matters. (Br. 37.) But the Carriers do not dispute the facts surrounding their failure to protect customer data, which were widely reported in the media, and do not explain why the Commission’s decision to take that publicly available information into account would cause them additional reputational injury. And this Court has suggested that carriers have options to expedite the initiation of an enforcement action. *Action on Children’s Television*, 59 F.3d at 1261.

Sprint and T-Mobile argue that that in other jurisdictions, defendants “in a § 504(a) suit” “may raise only a factual defense to a forfeiture order, not a challenge to the order’s legal validity,” (Br. 35 (quotation marks omitted)), so the Government “could assure more limited review [than would be available in this Circuit] by bringing its . . . collection suit in a different jurisdiction[.]” (Br. 36.)⁵ But that is

⁵ The Carriers also argue in a footnote that it violates the nondelegation doctrine to allow the Commission the choice between
(continued...)

not what happened here, and the Court should not find the Commission’s forfeiture powers unconstitutional based on a set of facts that did not occur.⁶

Moreover, even in jurisdictions they claim allow “more limited review,” (Br. 36), the Carriers do not deny that they would be entitled to have a jury determine the facts of their case, which is what the Seventh Amendment guarantees. *See Landry v. New Amsterdam Cas. Co.*, 279 F.2d 214, 215 (5th Cir. 1960) (per curiam) (“It is the province of the court to decide questions of law and the province of the jury to determine the

bringing an enforcement action before an administrative law judge or issuing a notice of apparent liability. (Br. 39–40 n.16.) Although “cursory arguments made only in footnotes” are “deem[ed] forfeited,” *Abdelfattah v. U.S. Dep’t of Homeland Sec.*, 787 F.3d 524, 532 (D.C. Cir. 2015), the argument is also wrong. The nondelegation doctrine applies to delegations of *legislative* authority. *Sanchez v. Office of State Superintendent of Ed.*, 45 F.4th 388, 401 (D.C. Cir. 2022). How the Commission carries out its enforcement powers is an exercise of *executive* authority which is within an agency’s discretion. *See Meta Platforms, Inc. v. FTC*, 723 F. Supp. 3d 64, 94 (D.D.C. 2024), *aff’d*, No. 24-5054, 2024 WL 1549732 (D.C. Cir. Mar. 29, 2024) (per curiam) (unpublished).

⁶ To the extent the Carriers purport to mount a facial challenge to the Commission’s forfeiture authority, courts “must be careful not to go beyond the statute’s facial requirements and speculate about ‘hypothetical’ or ‘imaginary’ cases.” *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 450 (2008).

facts[.]”). To the extent the Carriers argue that pursuing a jury trial in district court would require them to forego prompt judicial review of a forfeiture order, their complaint is with the Hobbs Act, which assigns the courts of appeals jurisdiction to review Commission orders. 28 U.S.C. § 2342(1). And to the extent the carriers worry they will suffer “reputational injury” (Br. 37) waiting to be sued, their issue is with the five-year limitations period for all Government actions to collect forfeitures. 28 U.S.C. § 2462. But neither of those statutes prevents the carriers from obtaining a jury trial should the Government pursue recovery of a forfeiture in district court under Section 504.

2. CPNI Enforcement Actions Are Not The Type of Common-Law Claim That Requires a Jury Trial.

Because the Carriers paid their forfeitures, the question of whether a carrier *would be* entitled to a jury had the Government sued it is premature, and the Court need not decide it. *Qassim v. Trump*, 927 F.3d 522, 530 (D.C. Cir. 2019) (“[C]ourts must avoid the premature adjudication of constitutional questions[.]” (quotation marks and modifications omitted)). But in any event, CPNI enforcement actions are not the kind of claim for which the Seventh Amendment requires a jury. *See Sprint Order* ¶¶ 81–82; *T-Mobile Order* ¶¶ 104–05 (JA319–21; 43–

45). In *SEC v. Jarkesy*, 603 U.S. 109 (2024), the Court held that the Seventh Amendment prohibits the SEC from imposing fines for securities fraud following an administrative hearing without a jury. But the enforcement of CPNI rules is nothing like the kinds of claims *Jarkesy* held mandate a jury trial.

The Seventh Amendment jury right applies to claims that are legal (as opposed to equitable) in nature—*i.e.*, to “those actions that are analogous to [s]uits at common law[.]” *Tull v. United States*, 481 U.S. 412, 417 (1987) (quotation marks omitted). To determine whether an action is the kind historically “tried in courts of law [rather] than . . . equity or admiralty,” courts “must examine both the nature of the action and of the remedy sought.” *Id.* Under *Tull*, a court “compare[s] the statutory action to 18th-century actions brought in the courts of England prior to the merger of the courts of law and equity,” and examines whether the remedy sought is “legal or equitable in nature.” *Id.* at 417–18. “What determines whether a monetary remedy is legal is if it is designed to punish or deter the wrongdoer[.]” *Jarkesy*, 603 U.S. at 123 (quotation marks omitted). And although the *Jarkesy* Court viewed the remedy as “the more important consideration” in determining whether the jury

right applies—and found it “all but dispositive” under the facts of that case—courts must still “consider the cause of action[.]” *Id.*; see also *Tull*, 481 U.S. at 417.

a. CPNI Enforcement Does Not Resemble Any Action at Common Law.

Unlike the fraud claims in *Jarkesy*—which bore a “close relationship” to “common law fraud,” 603 U.S. at 125—CPNI regulations protecting customer information generated in connection with telecommunications services would have been completely unknown to the “18th-century . . . courts of England prior to the merger of the courts of law and equity.” *Tull*, 481 U.S. at 417. As the *Jarkesy* Court explained, when Congress gave the SEC authority to assess civil penalties, it “deliberately used ‘fraud’ and other common law terms of art,” and thus “incorporated prohibitions from common law fraud into federal securities law.” *Id.* This “created an enduring link between federal securities fraud and its common law ‘ancestor,’” which “confirms that” the SEC’s fraud proceeding was “legal in nature.” *Id.* (some quotation marks omitted). In contrast, the FCC’s CPNI rules, including the requirement that carriers take reasonable steps to discover and protect against misuse of customer

information, *see* 47 C.F.R. § 64.2010(a), bear no clear relationship—much less a close one—to any common-law claim.

It is true that “[a]ctions by the Government to *recover* civil penalties under statutory provisions . . . historically have been viewed as . . . requiring trial by jury.” *Tull*, 481 U.S. at 418–19 (emphasis added). But this was not an action to recover a debt; it was a proceeding to determine whether the Carriers violated customer information protections that were unknown to the common law. And while it did result in the assessment of a penalty, that penalty could only be collected in a separate action in district court where a jury *could* have been available. *See* 47 U.S.C. § 504(a).⁷

Similarly, the Carriers’ effort to liken CPNI regulations to a common-law negligence claim proves too much: Yes, the CPNI rules

⁷ In *Tull*, the Government brought a lawsuit accusing a real estate developer of violating the Clean Water Act and seeking penalties. 481 U.S. at 414, 420. The Court found that this action was analogous to a common-law debt action, and held that the district court violated the Seventh Amendment by denying the defendants’ request for a jury. *Id.* at 420, 415. The Court also suggested, without deciding, that the underlying charge was analogous to a common-law nuisance claim. *Id.* at 420. *Tull* thus does not respond to the situation where the underlying claim has no common-law analogue and where collection of fines is determined in a different proceeding.

“impos[e] a duty of care to refrain from unreasonable actions that might harm others,” (Br. 31), but the duty they refer to is a modern statutory creation, which only underscores the *absence* of an historic analogue. This Court has addressed efforts to convert federal statutory obligations into common-law tort claims in the context of the Federal Tort Claims Act, holding that “[d]uties set forth in *federal law* do not . . . automatically create duties cognizable under *local tort law*,” and “[t]he pertinent inquiry is whether the duties set forth in the federal law are analogous to those imposed under local tort law.” *Art Metal-U.S.A., Inc. v. United States*, 753 F.2d 1151, 1157–58 (D.C. Cir. 1985) (emphasis in original). Almost any comprehensive statutory scheme will impose duties of care. If an analogy to common-law negligence could rest on such a generality, there would be no reason to examine the nature of a claim, and *Tull* and *Jarkesy*’s instruction to do so would be a dead letter.

b. CPNI Regulations Fall Within the “Public Rights Exception.”

CPNI regulations also fall within the Seventh Amendment’s “public rights exception,” which “permit[s] Congress to assign certain matters to agencies for adjudication even though such proceedings would not afford the right to a jury trial.” *Jarkesy*, 603 U.S. at 120. Public rights cases are

those “in which the Government sues in its sovereign capacity to enforce public rights created by statutes within the power of Congress to enact[.]” *Atlas Roofing Co., Inc. v. OSHA*, 430 U.S. 442, 450 (1977). Such cases “historically could have been determined exclusively by the executive and legislative branches, even when they were presented in such form that the judicial power was capable of acting on them[.]” *Jarkesy*, 603 U.S. at 128 (citations and modifications omitted).

a. The Commission’s CPNI regulations are imposed on telecommunications common carriers, and, accordingly, vindicate a public right. “The distinctive characteristic of a common carrier is that [it] undertakes to carry for all people indifferently, and hence is regarded in some respects as a public servant.” *Willard v. Fairfield So. Co., Inc.*, 472 F.3d 817, 821 (11th Cir. 2006) (modification omitted). And when “one devotes his property to a use in which the public has an interest, he, in effect, grants to the public an interest in that use, and must submit to be controlled by the public for the common good” *Munn v. Illinois*, 94 U.S. 113, 126 (1877).

The historical understanding that common carriers perform a public function was part of the common law long before the Seventh Amendment was drafted; the Court in *Munn* traced it at least as far back

as the 17th Century. *See id.* at 126 (noting, in 1877, that Lord Chief Justice Hale “more than two hundred years ago” explained “when private property is ‘affected with a public interest, it ceases to be *juris privati* only”). And there is a direct connection between this historic understanding of common carriers and modern telecommunications carriers like Sprint and T-Mobile: When Congress created the FCC, it consolidated several existing agencies’ powers—including the Interstate Commerce Commission’s authority over telephone and telegraph carriers, and the Postmaster General’s power to fix rates for telegrams—which historically had been understood to concern public rights. *See Scripps-Howard Radio v. FCC*, 316 U.S. 4, 7 (1942) (describing creation of FCC); *Crowell v. Benson*, 285 U.S. 22, 50 (1932) (listing, among “[f]amiliar illustrations of administrative agencies created for the determination of [public rights],” agencies “exercis[ing] . . . congressional power” over “interstate. . . commerce” and “the facilities of the post office”).

Enforcement of common-carrier regulations, therefore, falls into the category of cases that historically “could have been determined exclusively by the executive and legislative branches,” *Jarkesy*, 603 U.S. at 112, and does not implicate the Seventh Amendment.

b. CPNI protections also fall within the public rights exception because they are part of a regulatory scheme that governs access to a public resource from which Sprint and T-Mobile derive enormous private gain: wireless spectrum. As this Court has observed, “the electromagnetic spectrum . . . is not the private property of any individual or group; rather, it is a public resource in which every citizen has an interest.” *Nat’l Broad. Co. v. FCC*, 516 F.2d 1101, 1191 (D.C. Cir. 1974). The United States “maintain[s] control . . . over all the channels of radio transmission,” and no one may “use or operate any apparatus for the transmission of . . . communications or signals by radio” “except under and in accordance with” the Communications Act. 47 U.S.C. § 301. Since carriers must operate their networks in accordance with the Communications Act (including its CPNI protections), by enforcing CPNI rules, the Commission is enforcing a condition of access to a public resource—*i.e.*, a public right.

The Supreme Court’s treatment of patent rights—one of the specific examples of a public right the Court has provided, *see, e.g., Jarkesy*, 603 U.S. at 130; *Oil States Energy Servs. v. Greene’s Energy Grp.*, 584 U.S. 325, 334 (2018)—underscores why regulations governing wireless

licenses are a public right as well. Patent rights “did not exist at common law,” and were instead “a creature of statute[.]” *Oil States*, 584 U.S. at 335. “[T]he grant of a patent is a matter between the public, who are the grantors, and the patentee.” *Id.* (quotation marks and modifications omitted). This reasoning applies with equal force to the grant of a wireless license, and the right of licensees’ customers to have their data protected is by logical extension a public right.

B. The Commission Did Not Violate Separation-of-Powers or Due Process Principles.

a. Sprint and T-Mobile argue that it violates due process and the separation-of-powers for the Commission to act “as rule-maker, investigator, prosecutor, judge, and jury.” (Br. 37.) They cite Supreme Court precedent *upholding* the combination of investigative and adjudicative functions in an agency, but contend that it is “ripe for reconsideration[.]” (Br. 38.) Of course, only the Supreme Court can “reconsider” Supreme Court precedent. *See, e.g., Rodriguez de Quijas v. Shearson/American Express, Inc.*, 490 U.S. 477, 484 (1989). Under settled law, due process permits “the initial charge or determination of probable cause and the ultimate adjudication” to be “made by the same agency,” and also, “due process may be satisfied by providing for a neutral

adjudicator to conduct a *de novo* review” of an agency’s factual and legal conclusions. *In re Zdravkovich*, 634 F.3d 574, 579 (D.C. Cir. 2011) (quotation marks and modifications omitted) (quoting *Withrow v. Larkin*, 421 U.S. 35, 58 (1975)); *Concrete Pipe and Prods. of Cal., Inc. v. Constr. Laborers Pension Tr. for So. Cal.*, 508 U.S. 602, 619 (1993). The Carriers offer no reason to upset this precedent.

b. Sprint and T-Mobile also claim that two Commissioners prejudged their cases. (Br. 38). But an official is unconstitutionally conflicted only where “he has demonstrably made up his mind about important and specific factual questions and is impervious to contrary evidence.” *Fogo De Chao (Holdings) Inc. v. U.S. Dep’t of Homeland Sec.*, 769 F.3d 1127, 1148 (D.C. Cir. 2014). That did not happen here.

The Carriers cite a *New York Times* article in which Commissioner Starks wrote that the Commission should act quickly to address reports of the Securus incident and other breaches. See Geoffrey Starks, *Why It’s So Easy for a Bounty Hunter to Find You*, N.Y. Times (Apr. 2, 2019).⁸ But that article does not even name Sprint or T-Mobile, much less suggest

⁸ <https://www.nytimes.com/2019/04/02/opinion/fcc-wireless-regulation.html>.

that the Commissioner had formed an immutable opinion as to the specific facts surrounding their location-based services programs. The Carriers also take out of context a statement by then-Commissioner Rosenworcel in a dissent accompanying the Notices of Apparent Liability. The Commissioner did not say that “the carriers’ actions were ‘a violation of the law’” (Br. 39 n.15), she said that “collection and distribution or sale” of geolocation data “without [consumers’] permission or without reasonable safeguards in place” is “a violation of the law,” which is a legal interpretation, not a factual conclusion. Dissenting Statement of Commissioner Rosenworcel, *T-Mobile NAL* (JA156). Likewise, Commissioners Rosenworcel and Starks voiced concern with the Commission’s method for calculating penalties, opining that the proposed fines might be inadequate based on the information known at the time. But that does not indicate an unwillingness to consider Sprint and T-Mobile’s arguments against liability, especially considering that the Commission did ultimately lower T-Mobile’s fine in response to information it presented. The Commission did not improperly prejudge the Carriers’ cases.

II. CUSTOMER LOCATION INFORMATION IS CPNI.

The Commission correctly determined that customer location data is CPNI. CPNI “relates to the quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer” 47 U.S.C. § 222(h)(1)(A) (emphasis added). The Commission rightly concluded that this definition includes customer location data.

There is no dispute that the location information at issue here was generated by customer devices connecting to Sprint and T-Mobile’s networks: As the Commission explained, a mobile device connects to a carrier’s network through the closest tower, and a carrier needs to know a device’s location in order to allow a customer to receive and place calls. *E.g.*, *Sprint NAL* ¶ 37 (JA376). And since a carrier must know which tower a device is connected to at all times in order to deliver telecommunications to that device, the location of that tower “relates to the . . . location . . . of a telecommunications service,” and is CPNI. 47 U.S.C. § 222(h)(1)(A). The Carriers’ efforts to resist this straightforward conclusion lack merit.

A. CPNI Is Not Limited to Call Location Information.

Sprint and T-Mobile argue that the statute only protects a customer's location while the customer is "*making or receiving a voice call.*" (Br. 40 (emphasis in brief) (quoting dissenting statement of Commissioner Carr (JA51)).) Thus, they contend, "a device's passive registration with a network tower" does not generate CPNI when the device "is not being used for a call[.]" (Br. 42.) This argument misreads the statute, misapplies the rules of construction, and cannot be squared with congressional intent.

a. The definition of CPNI makes no mention of *a voice call*; it refers to a *telecommunications service*. Sprint and T-Mobile argue that "a 'telecommunications service' . . . offers the actual 'transmission' of a voice," so "[i]nformation about the location of a *device* that is not engaged in telecommunications is not information about the location of use of a *telecommunications service*" and thus not CPNI. (Br. 42 (emphasis in original).) But this conflates using a telecommunications service with engaging in telecommunications. Although telecommunications is limited to the "the transmission" of "information of the user's choosing," telecommunications *service*—the term used in the statute—is the "*offering* of telecommunications for a fee[.]" 47 U.S.C. § 153(50), (53)

(emphasis added). That definition does not turn on whether a customer is presently *using* the service offered, so it does not follow that CPNI regulations only protect a customer's location when talking on the phone.

Nor is using a telecommunications service confined to actively talking on the phone, as the Commission explained. Sprint and T-Mobile's customers "subscribe to [their] commercial mobile service to enable them to receive and transmit calls." *Sprint Order* ¶ 27; *T-Mobile Order* ¶ 26 (JA297; 12). Thus, "[w]hen customers' devices are exchanging communications with [the carriers'] network, and thereby ensuring that they can receive incoming calls and place outgoing calls," it is "a clear case of using the service to which they have subscribed, even outside the moments in time when they are engaged in calls." *Sprint Order* ¶ 27; *T-Mobile Order* ¶ 26 (JA297; 12). Sprint and T-Mobile obtained location information from customer devices connected to their network in order to facilitate telecommunications on that network. The information thus related to the location of a telecommunications service and was CPNI.

b. The Carriers' arguments from prior Commission orders and legislative history are unavailing. The Carriers cite a 2013 ruling in which the Commission clarified that CPNI regulations apply to information stored on customers' devices. Declaratory Ruling ("2013

Order”), *Implementation of the Telecommunications Act of 1996*, 28 FCC Rcd 9609 (2013). In the *2013 Order*, the Commission addressed carriers’ practice of installing software on customer devices to monitor network performance, and discussed a specific tool that recorded information such as “the telephone numbers of calls dialed and received and the location of the device at the time of the calls,” which were used to “diagnose dropped calls or areas with no service.” *Id.* at 9616, ¶ 22 & n.46. By referring to a call’s location, the Commission was illustrating a particular kind of data that a specific provider was collecting; it was not delimiting the kinds of information subject to CPNI regulations.

Also in the *2013 Order*, the Commission listed examples of data that that “does not pertain to a telecommunications service,” including “information that pertains to the device’s access of the carrier’s data network[.]” *Id.* at 9618–19, ¶ 28 & n.66. Likewise, CTIA points (CTIA Amicus Br. 17) to the *1999 Order*, where the Commission discussed information that “is not received by a carrier *in connection with its provision of telecommunications service.*” Order on Reconsideration, *Implementation of the Telecommunications Act of 1996*, 14 FCC Rcd 14,409, 14,492, ¶ 159 (1999) (emphasis added). Neither of these orders

helps the Carriers, because their customers' location information "supported *both* data and voice services," (Br. 52 (emphasis in original)), and here, the Commission specifically found that when a customer's device connects to the Carriers' network to be able to make or receive a phone call, the customer is using a telecommunications service. The Commission's statements about data gathered outside the context of telecommunications service are not relevant here.

Finally, the Carriers point out that the word "location" was added to the definition of CPNI as part of a broader amendment that added references to "call location information" elsewhere in Section 222, and argue that the two terms therefore "mean[] the same thing." (Br. 48–49.) It makes sense to talk about *call* location in those other provisions, because they relate specifically to routing *calls* to 911. 47 U.S.C. § 222(d)(4). But Congress did *not* refer to *call* location when it defined CPNI. And when statutory words differ, courts "normally presume that" "Congress acts intentionally and purposely . . ." *Burlington N. & Santa Fe Ry. Co. v. Whyte*, 548 U.S. 53, 63 (2006).

c. To support their position that CPNI rules apply only when a customer is on a call, Sprint and T-Mobile argue that the words "of use"

in the phrase “quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service” modify every noun in the list, including “location,” so that the relevant category is not the *location*, but the *location of use* of a telecommunications service. (Br. 42–43.) Under this reading, to be CPNI, information must relate not to the—

Quantity;
Technical configuration;
Type;
Destination;
Location; or
Amount of use } of a telecommunications service

but rather, to the—

Quantity;
Technical configuration;
Type;
Destination;
Location; or
Amount } *of use* of a telecommunications service

For starters, even if this were the correct interpretation, it would not get Sprint and T-Mobile far because, as shown above, a customer uses a telecommunications service whenever the customer’s device is ready to receive or place a call, so there is no meaningful difference between the location of a telecommunications service and the location of use of a telecommunications service. *See Sprint Order* ¶¶ 25–27 (JA296–97)

(finding that customer location information meets the definition of CPNI under either interpretation). But the Carriers’ interpretation is also not the best reading of the statute.

When a statute “include[s] a list of terms or phrases followed by a limiting clause,” courts typically apply the “rule of the last antecedent” which “provides that a limiting clause or phrase should ordinarily be read as modifying only the noun or phrase that it immediately follows.” *Lockhart v. United States*, 577 U.S. 347, 351 (2016) (modifications and quotation marks omitted); *Sprint Order* ¶ 25; *T-Mobile Order* ¶ 24 (JA296; 10–11). Here, that tool of construction shows that “of use” in the CPNI definition refers only to the *amount of use*—not the *location* of use—of a telecommunications service, and thus that the location information protected by the statute is not limited to the location of a phone call.

Sprint and T-Mobile argue (Br. 47–48) that a different canon of construction applies, and yields the opposite result. Under the “series-qualifier canon,” a modifier that appears after an “integrated list” “normally applies to the entire series” that precedes it. *Facebook, Inc. v. Duguid*, 592 U.S. 395, 402, 403, 404 (2021) (quotation marks and modifications omitted). Sprint and T-Mobile do not explain what makes

a list “integrated,” but the language in *Facebook* looks nothing like the definition of CPNI. *Facebook* involved the phrase “store or produce telephone numbers . . . using a random or sequential number generator,” and the Court held that “using a random or sequential number generator” modified both “store” and “produce.” *Id.* at 402. In contrast, in *Lockhart*, the Court applied the rule of last antecedent when construing a reference to “aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor” and held that “involving a minor” modified only “abusive sexual conduct,” which immediately preceded it. 577 U.S. at 350. The serial listing of nouns in the CPNI definition reads as an enumeration of independent factors, and structurally resembles the language in *Lockhart*, not *Facebook*.⁹

The Carriers’ reading of the statute would also lead to awkward or duplicative results. For example, if “of use” modified every item that precedes it, then CPNI would include information about the “technical

⁹ Furthermore, when the qualifier at the end of a list is set off by a comma, it “is evidence that the qualifier is supposed to apply to all the antecedents instead of only the immediately preceding one.” *Facebook*, 592 US at 403 (quotation marks omitted). And whereas the qualifier in *Facebook* did indeed follow a comma, neither the definition of CPNI nor the language in *Lockhart* includes a comma before the final qualifier.

configuration of use” of a telecommunications service, but it is not clear what that would mean. *Sprint Order* ¶ 25; *T-Mobile Order* ¶ 25 (JA296; 11). One can comfortably speak of the configuration of a telecommunications service, but it would be awkward at best (and arguably unintelligible) to refer to the configuration of such a service’s “use.” Moreover, under the Carriers’ reading, CPNI would pertain to both the “quantity of use” and “amount of use” of a telecommunications service, rendering the two terms duplicative, in violation of the canon against surplusage. *See, e.g., Air Transport Ass’n v. U.S. Dep’t of Agriculture*, 37 F.4th 667, 672 (D.C. Cir. 2022). The Commission’s reading avoids these problems.

B. Sprint and T-Mobile Had Access to Their Customers’ Location Data Solely by Virtue of the Carrier–Customer Relationship.

To count as CPNI, customer information must be available to a carrier solely by virtue of the customer–carrier relationship. 47 U.S.C. § 222(h)(1)(A). Sprint and T-Mobile do not deny that they had access to their customers’ location data solely as a result of their *relationship* with their customers, but argue that that relationship was not solely a “*carrier–customer* relationship”—and thus that it fell outside the scope of the CPNI rule, (Br. 51–53), because they also offer data service. They

reason that data service is not telecommunications service, so “[f]or any customer with both voice and data services, . . . location information was not generated ‘solely’ because of the voice subscription[.]” (Br. 8, 52.) In other words, Sprint and T-Mobile urge that their failure to discover and protect against misuse of their telecommunications customers’ information does not violate CPNI rules as long as they simultaneously offer non-telecommunications service to those same customers.

a. The Carriers’ argument makes a hash of the statutory text. The focus of the CPNI rule is whether the parties’ *relationship* was the sole source of access to a customer’s data—which it undisputably was—not whether a carrier solely provided a specific kind of service. The Commission rightly was “not persuaded that the fact that location information can be associated with a non-telecommunications service the carrier also provides takes the resulting *relationship* outside the scope of the ‘carrier–customer’ relationship for the specific purposes of the CPNI definition.” *Sprint Order* ¶ 32 (emphasis in original); *T-Mobile Order* ¶ 31 (emphasis in original) (JA299; 13). The Commission also found that the companies’ argument was “belied by the technical and marketplace realities . . . as experienced by [their] customers.” *Sprint Order* ¶ 30;

T-Mobile Order ¶ 29 (JA299; 13). Carriers must be aware of the location of their customers’ devices “in order . . . to send and receive calls,” and a customer “has no choice but to reveal [his or her] location” to a wireless provider. *Sprint Order* ¶ 31; *T-Mobile Order* ¶ 30 (JA299; 13). Nor do Sprint and T-Mobile “dispute that the carrier–customer relationship fully enables [them] to obtain the location data at issue here.” *Sprint Order* ¶ 31; *T-Mobile Order* ¶ 30 (JA299; 13).

b. Sprint and T-Mobile’s construction would also lead to the anomalous—and easily manipulable—result that a carrier providing voice-only service must protect its customers’ location data, but a carrier providing voice *and data* service—even a data service as ubiquitous as text messaging (*see* Br. 8)—has no such obligation, even if the voice service and location information are exactly the same. There is no reason to believe that Congress, having specifically required carriers to safeguard their customers’ personally identifying information, intended to let those same carriers effectively opt out of that requirement by providing telecommunications services *plus something else*.

C. The Carriers Had Sufficient Notice That Customer Location Data is CPNI.

Finally, the plain text of the statute put the carriers on notice that CPNI includes customer location information.¹⁰ As the Commission observed, “[t]he fair notice doctrine . . . provides redress only if an agency’s interpretation is so far from a reasonable person’s understanding of the regulations that they could not have fairly informed the regulated party of the agency’s perspective.” *Sprint Order* ¶ 36 (JA301) (citing *Miss. Comm’n on Env’t Quality v. EPA*, 790 F.3d 138, 186 (D.C. Cir. 2015)). Indeed, agencies can—and regularly do—interpret statutes in light of the unique facts of an adjudication and apply that interpretation in that specific case. *See Neustar, Inc. v. FCC*, 857 F.3d 886, 895 (D.C. Cir. 2017). Sprint and T-Mobile were not denied fair notice of the Commission’s interpretation of the CPNI rules because, as we have shown, that interpretation—based on a simple reading of the plain language of the statute—was the most natural. *See NetworkIP, LLC v.*

¹⁰ Additionally, the Carriers claim they were “left to guess at what ‘reasonable measures’ [to protect CPNI] might mean.” (Br. 63.) But surely they did not need to be told that, to the extent they relied on contractual requirements, it was unreasonable to ignore whether they “were actually being followed,” *Sprint Order* ¶ 48 (JA306), or to disregard major compliance failures once revealed.

FCC, 548 F.3d 116, 125 (D.C. Cir. 2008) (finding “the fair notice doctrine . . . satisfied” where the FCC had the “most natural” interpretation of its order); *see also id.* at 123 (noting that this Court has “never applied the fair notice doctrine in a case where the agency’s interpretation is the most natural one”).

III. THE COMMISSION’S LIABILITY FINDINGS AND THE FORFEITURES IT ASSESSED WERE LAWFUL.

The Commission assessed forfeitures that are well-supported by the facts and grounded in Commission precedent. Far from being arbitrary or capricious, they appropriately reflect the seriousness of Sprint and T-Mobile’s violations.

A. Substantial Evidence Supports the Commission’s Finding of Liability.

Sprint and T-Mobile point to the safeguards they allegedly had in place to argue that they acted reasonably in protecting their customers’ data (Br. 57–61), but the Commission already considered these arguments and found that the Carriers’ measures were insufficient, and ineffectively implemented.

a. Sprint “apparently did not review third-party proposals for using its customer location information, did not review customer consent records, and did not exercise its right to audit the Aggregators.” *Sprint*

Order ¶ 72 (JA315). In addition, Sprint “apparently had no history of internally reviewing and approving third-party proposals for using Sprint’s customer location information before [it] actually disclosed the data,” “apparently never internally reviewed consumer consent records,” and “apparently never exercised its right to audit the Aggregators’ practices before 2018.” *Sprint NAL* ¶ 84 (JA390, 391). “Sprint’s apparent decision to simply trust the Aggregators and their location-based service provider customers even after the *New York Times* report” was “confounding.” *Id.* (JA390).

Sprint describes the steps it took to suspend access to customer locations in the wake of the *Securus Article* (Br. 60), but the Commission found that Sprint “undermined” those efforts by “reinstating [the aggregator] LocationSmart (and two of its customers) into the program three months later.” *Sprint Order* ¶ 51 (JA307). Nor did “cutting off some providers’ access to Sprint location information” “improve the safeguards for consumers whose location information could be disclosed under . . . arrangements that remained in place.” *Id.*

Likewise, “nothing that T-Mobile . . . provided [the Commission] shows that it made any meaningful efforts or that it could effectively

distinguish between valid and unauthorized requests for location information.” *T-Mobile Order* ¶ 48 (JA21). “T-Mobile knew as early as July 2017”—when it learned about LocateUrCell’s unauthorized use of customer location data¹¹—that “relying on provisions in its contract with LocationSmart was not at all successful at protecting customer location information against misuse,” yet it failed to promptly correct that problem. *T-Mobile NAL* ¶ 87 (JA149). And although the Carriers tout their adherence to CTIA Guidelines, (Br. 58), those guidelines “do not include best practices recommendations for carriers that sell access to their customers’ location information to location-based providers ” and do not address the legal issues presented here. *T-Mobile Order* ¶¶ 47, 64 (quotation marks omitted) (JA20, 29). T-Mobile also emphasizes its “2018 risk assessment” (Br. 59), but, citing privilege, it refused to disclose the results of that assessment, so the Commission could not evaluate

¹¹ T-Mobile claims that this incident shows its protections *were* effective, because they allowed it to shut down LocateUrCell’s unauthorized program. (Br. 62.) But the record reveals only that T-Mobile “learned” about that program “through a third party,” which says nothing about the role T-Mobile’s safeguards might have played. Final Resp. of T-Mobile USA, Inc. to Sept. 13, 2018 Letter of Inquiry at 17 (JA225). And T-Mobile cannot deny that those same measures did *not* identify Securus’s abuses of customer data.

T-Mobile’s “vague assertions about the underlying concerns and any changes it made[.]” *T-Mobile Order* ¶ 48 (quotation marks omitted) (JA21). In the end, the three publicized breaches of customer data “persuade[d]” the Commission that “the assessments either were not designed to detect vulnerabilities in the consent mechanism or failed meaningfully to do so.” *T-Mobile Order* ¶ 48 (JA21).

b. The Carriers’ claim that the Commission found them liable for failing to “terminat[e] their entire LBS programs immediately following a single newspaper article” (Br. 61) does not fairly characterize the facts or the Commission’s decision. The Carriers themselves recognized that the *Securus Article* indicated major problems in their location-based services programs, because they cut off Securus’s access to customer location information in response. (*E.g.*, Br. 61.) In any event, the Commission did not fine the carriers for not immediately *terminating* their programs; it fined them for not taking “definitive steps to *remedy* the obvious . . . issues” the article laid bare.¹² *Sprint Order* ¶ 53 (emphasis added); *T-Mobile Order* ¶ 58 (JA308; 25).

¹² The Commission also did not fine the Carriers for the first 30 days after the *Securus Article* was published, reasoning that they could
(continued...)

Similarly, the Carriers’ contention that Securus’s concededly unauthorized access to customer locations “did not suggest a widespread problem,” (Br. 62), overlooks the facts. “Securus’s entire location-finding service” “was outside the scope of not only its approved use case, but also beyond any agreement with either Aggregator” and “T-Mobile conceded that it was unable to distinguish location requests unrelated to the authorized use case.” *T-Mobile Order* ¶ 42 (JA18). This meant that on a system-wide level, the Carriers’ method for regulating access to customer location data did not work.

All in all, the evidence substantially supported the Commission’s finding that the Carriers failed to take reasonable steps to protect their customers’ data.

B. The Commission Assessed Lawful Forfeitures.

a. There was also nothing arbitrary or capricious about the specific forfeitures the Commission assessed. Sprint and T-Mobile do not appear to challenge the Commission’s decision to fine them for multiple days of violations, but they take issue with the finding that they

have “either end[ed] the[ir] program[s] or reform[ed] [their] practices” in that time. *E.g.*, *Sprint Order* ¶ 35 n.124 (JA301).

committed a *separate* ongoing violation for *each* third party (11 for Sprint and 81 for T-Mobile, *Sprint Order* ¶ 64; *T-Mobile Order* ¶ 77 (JA312; 34)) they improperly let access their customers' data. (Br. 65-66.)

According to Sprint and T-Mobile, in improperly making customer data available to dozens of individual entities, they committed “at most, a single, continuing failure to act[.]” (Br. 65.) But by their own account, each third party’s access to customer data was a unique circumstance. “T-Mobile required aggregators to seek preapproval for each distinct service . . . [a location-based service] provider might offer,” and Sprint “grant[ed] LBS providers access to customer location information” following a “Certification’ process[.]” (Br. 15–16.) The available location-based services were “varied,” (Br. 12), and each provider’s access to customer data was governed by its own contract with an aggregator or sub-aggregator. *Sprint Order* ¶ 9; *T-Mobile Order* ¶ 9 (JA290; 5). Each third party with access to unprotected customer data embodied a separate failure by Sprint and T-Mobile to protect that information; the fact that they repeated those failures many times over does not transform them into a single violation.

b. The Commission also did not assess disproportionate fines. The maximum allowable fine at the time for each day of a continuing violation was \$204,892.¹³ See *Sprint NAL* ¶ 76 & n.190; *T-Mobile NAL* ¶ 79 & n.190 (JA 387; 146). The Commission started much lower, with a base forfeiture of \$40,000 per third party given access to customer data—the same amount it has used in other consumer-protection cases, see *Sprint NAL*, ¶ 80; *T-Mobile NAL* ¶ 84 (JA 389; 147–48) (citing *Advantage Telecomms. Corp.*, 32 FCC Rcd 3723 (2017) & *Preferred Long Distance, Inc.*, 30 FCC Rcd 13,711 (2015)))—and added \$2,500 per third party per day the violations continued. *Sprint Order* ¶ 62; *T-Mobile Order* ¶ 74 (JA312; 33). Sprint and T-Mobile do not claim that either of the daily forfeiture amounts was unreasonable, and they resulted in a base forfeiture significantly below what the statute allowed. If these forfeiture amounts add up to a substantial total, it is only because Sprint and T-Mobile’s violations persisted for a substantial length of time.

The Commission also followed the statute and the agency’s forfeiture guidelines in imposing upward adjustments to the carriers’

¹³ See *Amendment of Section 1.80(b) of the Commission’s Rules*, 34 FCC Rcd 12,824 (2019) (adding inflation adjustments to statutory values).

penalties. *T-Mobile Order* ¶ 92; *Sprint Order* ¶ 62 (JA39; 312). Congress requires the Commission to “take into account the nature, circumstances, extent, and gravity” of a violation, as well as the violator’s “ability to pay,” 47 U.S.C. § 503(b)(1)(E). And the Commission’s regulations provide that factors including “egregious misconduct,” “substantial harm,” and “repeated or continuous violation” will justify an upward adjustment. 47 C.F.R. § 1.80(b)(11) Table 3 (capitalization modified). The Commission’s adjustments appropriately reflected Sprint and T-Mobile’s “egregious” and ongoing conduct. *Sprint Order* ¶ 72; *T-Mobile Order* ¶ 92 (JA315; 39). The Commission also rightly “took into account” the Carriers’ status as “major telecommunications provider[s]” in adopting a penalty that would “adequately provide [them] with the necessary disincentive to engage in similar conduct again in the future.” *Id.*

Sprint and T-Mobile argue that, unlike other recipients of large FCC fines, they “did not commit fraud,” and “even assuming they misunderstood their statutory or regulatory duties, there is no evidence that they violated the law willfully.” (Br. 68.) This downplays the seriousness of the violations the Commission found. Far from a “misunderstanding,” Sprint “did not review third-party proposals for

using its customer location information, did not review customer consent records, and did not exercise its right to audit the Aggregators,” and T-Mobile “showed reckless disregard for CPNI requirements by relying on ‘implicit consent’ for the disclosure of location information.” *Sprint Order* ¶ 72; *T-Mobile Order* ¶ 92 (JA315; 39). This pattern of failures jeopardized “highly sensitive location information” of “tens of millions of consumers,” and created a threat to national security and public safety. *T-Mobile Order* ¶¶ 80, 92 (JA35; 39). Those failures, and their significant consequences, amply justified the substantial fines that the Commission assessed.

CONCLUSION

The Court should deny the petitions for review.

January 10, 2025

Respectfully submitted,

/s/ John R. Grimm

P. Michele Ellison
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

John R. Grimm
Counsel

Doha G. Mekki
*Acting Assistant Attorney
General*

Robert B. Nicholson
Matthew A. Waring
Attorneys

U.S. DEPARTMENT OF JUSTICE
950 Pennsylvania Ave. NW
Washington, DC 20530

FEDERAL COMMUNICATIONS
COMMISSION
45 L Street NE
Washington, DC 20554
(202) 418-1740
fcclitigation@fcc.gov

CERTIFICATE OF COMPLIANCE

Certificate of Compliance With Type-Volume Limitation, Typeface Requirements and Type Style Requirements

1. This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f) and D.C. Circuit Rule 32(e)(1):
 - this document contains 12,348 words, *or*
 - this document uses a monospaced typeface and contains _____ lines of text.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:
 - this document has been prepared in a proportionally spaced typeface using Microsoft Word for Office 365 in 14-point Century Schoolbook, *or*
 - this document has been prepared in a monospaced spaced typeface using _____ with _____.

/s/ John R. Grimm
John R. Grimm
Counsel for Respondents

STATUTORY ADDENDUM

STATUTORY ADDENDUM CONTENTS

	Page
28 U.S.C. § 2342	Add. 1
28 U.S.C. § 2462	Add. 3
47 U.S.C. § 153	Add. 4
47 U.S.C. § 217	Add. 5
47 U.S.C. § 222	Add. 6
47 U.S.C. § 301	Add. 9
47 U.S.C. § 402	Add. 10
47 U.S.C. § 503	Add. 11
47 U.S.C. § 504	Add. 14
47 C.F.R. § 1.80	Add. 15
47 C.F.R. § 64.2007	Add. 23
47 C.F.R. § 64.2010	Add. 24

28 U.S.C. § 2342

Jurisdiction of court of appeals

The court of appeals (other than the United States Court of Appeals for the Federal Circuit) has exclusive jurisdiction to enjoin, set aside, suspend (in whole or in part), or to determine the validity of—

(1) all final orders of the Federal Communications Commission made reviewable by section 402(a) of title 47;

(2) all final orders of the Secretary of Agriculture made under chapters 9 and 20A of title 7, except orders issued under sections 210(e), 217a, and 499g(a) of title 7;

(3) all rules, regulations, or final orders of—

(A) the Secretary of Transportation issued pursuant to section 50501, 50502, 56101–56104, or 57109 of title 46 or pursuant to part B or C of subtitle IV, subchapter III of chapter 311, chapter 313, or chapter 315 of title 49; and

(B) the Federal Maritime Commission issued pursuant to section 305, 41304, 41308, or 41309 or chapter 421 or 441 of title 46;

(4) all final orders of the Atomic Energy Commission made reviewable by section 2239 of title 42;

(5) all rules, regulations, or final orders of the Surface Transportation Board made reviewable by section 2321 of this title;

(6) all final orders under section 812 of the Fair Housing Act; and

(7) all final agency actions described in section 20114(c) of title 49.

Jurisdiction is invoked by filing a petition as provided by section 2344 of this title.

28 U.S.C. § 2462

§ 2462. Time for commencing proceedings

Except as otherwise provided by Act of Congress, an action, suit or proceeding for the enforcement of any civil fine, penalty, or forfeiture, pecuniary or otherwise, shall not be entertained unless commenced within five years from the date when the claim first accrued if, within the same period, the offender or the property is found within the United States in order that proper service may be made thereon.

47 U.S.C. § 153

Definitions

For the purposes of this chapter, unless the context otherwise requires—

* * *

(50) Telecommunications

The term “telecommunications” means the transmission, between or among points specified by the user, of information of the user’s choosing, without change in the form or content of the information as sent and received.

* * *

(53) Telecommunications service

The term “telecommunications service” means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

* * *

47 U.S.C. § 217

Agents' acts and omissions; liability of carrier

In construing and enforcing the provisions of this chapter, the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person.

47 U.S.C. § 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.

* * *

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

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

(2) Disclosure on request by customers

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

(3) Aggregate customer information

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

* * *

(d) Exceptions

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

* * *

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

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

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

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

* * *

(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.

* * *

47 U.S.C. § 301

License for radio communication or transmission of energy

It is the purpose of this chapter, among other things, to maintain the control of the United States over all the channels of radio transmission; and to provide for the use of such channels, but not the ownership thereof, by persons for limited periods of time, under licenses granted by Federal authority, and no such license shall be construed to create any right, beyond the terms, conditions, and periods of the license. No person shall use or operate any apparatus for the transmission of energy or communications or signals by radio (a) from one place in any State, Territory, or possession of the United States or in the District of Columbia to another place in the same State, Territory, possession, or District; or (b) from any State, Territory, or possession of the United States, or from the District of Columbia to any other State, Territory, or possession of the United States; or (c) from any place in any State, Territory, or possession of the United States, or in the District of Columbia, to any place in any foreign country or to any vessel; or (d) within any State when the effects of such use extend beyond the borders of said State, or when interference is caused by such use or operation with the transmission of such energy, communications, or signals from within said State to any place beyond its borders, or from any place beyond its borders to any place within said State, or with the transmission or reception of such energy, communications, or signals from and/or to places beyond the borders of said State; or (e) upon any vessel or aircraft of the United States (except as provided in section 303(t) of this title); or (f) upon any other mobile stations within the jurisdiction of the United States, except under and in accordance with this chapter and with a license in that behalf granted under the provisions of this chapter.

47 U.S.C. § 402

Judicial review of Commission's orders and decisions

(a) Procedure

Any proceeding to enjoin, set aside, annul, or suspend any order of the Commission under this chapter (except those appealable under subsection (b) of this section) shall be brought as provided by and in the manner prescribed in chapter 158 of Title 28.

* * *

47 U.S.C. § 503

Forfeitures

(b) Activities constituting violations authorizing imposition of forfeiture penalty; amount of penalty; procedures applicable; persons subject to penalty; liability exemption period

(1) Any person who is determined by the Commission, in accordance with paragraph (3) or (4) of this subsection, to have—

(A) willfully or repeatedly failed to comply substantially with the terms and conditions of any license, permit, certificate, or other instrument or authorization issued by the Commission;

(B) willfully or repeatedly failed to comply with any of the provisions of this chapter or of any rule, regulation, or order issued by the Commission under this chapter or under any treaty, convention, or other agreement to which the United States is a party and which is binding upon the United States;

* * *

shall be liable to the United States for a forfeiture penalty. A forfeiture penalty under this subsection shall be in addition to any other penalty provided for by this chapter; except that this subsection shall not apply to any conduct which is subject to forfeiture under subchapter II, part II or III of subchapter III, or section 507 of this title.

(2)(A) If the violator is (i) a broadcast station licensee or permittee, (ii) a cable television operator, or (iii) an applicant for any broadcast or cable television operator license, permit, certificate, or other instrument or authorization issued by the Commission, the amount of any forfeiture penalty determined under this section shall not exceed \$25,000 for each violation or each day of a continuing violation, except that the amount

assessed for any continuing violation shall not exceed a total of \$250,000 for any single act or failure to act described in paragraph (1) of this subsection.

(B) If the violator is a common carrier subject to the provisions of this chapter or an applicant for any common carrier license, permit, certificate, or other instrument of authorization issued by the Commission, the amount of any forfeiture penalty determined under this subsection shall not exceed \$100,000 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of \$1,000,000 for any single act or failure to act described in paragraph (1) of this subsection.

* * *

(3)(A) At the discretion of the Commission, a forfeiture penalty may be determined against a person under this subsection after notice and an opportunity for a hearing before the Commission or an administrative law judge thereof in accordance with section 554 of Title 5. Any person against whom a forfeiture penalty is determined under this paragraph may obtain review thereof pursuant to section 402(a) of this title.

(B) If any person fails to pay an assessment of a forfeiture penalty determined under subparagraph (A) of this paragraph, after it has become a final and unappealable order or after the appropriate court has entered final judgment in favor of the Commission, the Commission shall refer the matter to the Attorney General of the United States, who shall recover the amount assessed in any appropriate district court of the United States. In such action, the validity and appropriateness of the final order imposing the forfeiture penalty shall not be subject to review.

(4) Except as provided in paragraph (3) of this subsection, no forfeiture penalty shall be imposed under this subsection against any person unless and until—

(A) the Commission issues a notice of apparent liability, in writing, with respect to such person;

(B) such notice has been received by such person, or until the Commission has sent such notice to the last known address of such person, by registered or certified mail; and

(C) such person is granted an opportunity to show, in writing, within such reasonable period of time as the Commission prescribes by rule or regulation, why no such forfeiture penalty should be imposed.

Such a notice shall (i) identify each specific provision, term, and condition of any Act, rule, regulation, order, treaty, convention, or other agreement, license, permit, certificate, instrument, or authorization which such person apparently violated or with which such person apparently failed to comply; (ii) set forth the nature of the act or omission charged against such person and the facts upon which such charge is based; and (iii) state the date on which such conduct occurred. Any forfeiture penalty determined under this paragraph shall be recoverable pursuant to section 504(a) of this title.

* * *

47 U.S.C. § 504

Forfeitures

(a) Recovery

The forfeitures provided for in this chapter shall be payable into the Treasury of the United States, and shall be recoverable, except as otherwise provided with respect to a forfeiture penalty determined under section 503(b)(3) of this title, in a civil suit in the name of the United States brought in the district where the person or carrier has its principal operating office or in any district through which the line or system of the carrier runs: *Provided*, That any suit for the recovery of a forfeiture imposed pursuant to the provisions of this chapter shall be a trial de novo: *Provided further*, That in the case of forfeiture by a ship, said forfeiture may also be recoverable by way of libel in any district in which such ship shall arrive or depart. Such forfeitures shall be in addition to any other general or specific penalties provided in this chapter. It shall be the duty of the various United States attorneys, under the direction of the Attorney General of the United States, to prosecute for the recovery of forfeitures under this chapter. The costs and expenses of such prosecutions shall be paid from the appropriation for the expenses of the courts of the United States.

* * *

Federal Communications Commission

§ 1.80

Radio Service are set forth in part 5 of this chapter.

(e) Rules governing applications for authorizations in the Domestic Public Radio Services are set forth in part 21 of this chapter.

(f) Rules governing applications for authorizations in the Industrial, Scientific, and Medical Service are set forth in part 18 of this chapter.

(g) Rules governing applications for certification of equipment are set forth in part 2, subpart J, of this chapter.

(h) Rules governing applications for commercial radio operator licenses are set forth in part 13 of this chapter.

(i) Rules governing applications for authorizations in the Common Carrier and Private Radio terrestrial microwave services and Local Multipoint Distribution Services are set out in part 101 of this chapter.

[28 FR 12415, Nov. 22, 1963, as amended at 44 FR 39180, July 5, 1979; 47 FR 53378, Nov. 26, 1982; 61 FR 26670, May 28, 1996; 62 FR 23162, Apr. 29, 1997; 63 FR 36596, July 7, 1998; 66 FR 47895, Sept. 14, 2001; 78 FR 25160, Apr. 29, 2013]

MISCELLANEOUS PROCEEDINGS

§ 1.80 Forfeiture proceedings.

(a) *Persons against whom and violations for which a forfeiture may be assessed.* A forfeiture penalty may be assessed against any person found to have:

(1) Willfully or repeatedly failed to comply substantially with the terms and conditions of any license, permit, certificate, or other instrument of authorization issued by the Commission;

(2) Willfully or repeatedly failed to comply with any of the provisions of the Communications Act of 1934, as amended; or of any rule, regulation or order issued by the Commission under that Act or under any treaty, convention, or other agreement to which the United States is a party and which is binding on the United States;

(3) Violated any provision of section 317(c) or 508(a) of the Communications Act;

(4) Violated any provision of sections 227(b) or (e) of the Communications Act or of §§64.1200(a)(1) through (5) and 64.1604 of this title;

(5) Violated any provision of section 511(a) or (b) of the Communications Act or of paragraph (b)(6) of this section;

(6) Violated any provision of section 1304, 1343, or 1464 of Title 18, United States Code; or

(7) Violated any provision of section 6507 of the Middle Class Tax Relief and Job Creation Act of 2012 or any rule, regulation, or order issued by the Commission under that statute.

NOTE 1 TO PARAGRAPH (a): A forfeiture penalty assessed under this section is in addition to any other penalty provided for by the Communications Act, except that the penalties provided for in paragraphs (b)(1) through (4) of this section shall not apply to conduct which is subject to a forfeiture penalty or fine under sections 202(c), 203(e), 205(b), 214(d), 219(b), 220(d), 223(b), 364(a), 364(b), 386(a), 386(b), 506, and 634 of the Communications Act. The remaining provisions of this section are applicable to such conduct.

(b) *Limits on the amount of forfeiture assessed—*(1) *Forfeiture penalty for a broadcast station licensee, permittee, cable television operator, or applicant.* If the violator is a broadcast station licensee or permittee, a cable television operator, or an applicant for any broadcast or cable television operator license, permit, certificate, or other instrument of authorization issued by the Commission, except as otherwise noted in this paragraph (b)(1), the forfeiture penalty under this section shall not exceed \$59,316 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of \$593,170 for any single act or failure to act described in paragraph (a) of this section. There is no limit on forfeiture assessments for EEO violations by cable operators that occur after notification by the Commission of a potential violation. See section 634(f)(2) of the Communications Act (47 U.S.C. 554). Notwithstanding the foregoing in this section, if the violator is a broadcast station licensee or permittee or an applicant for any broadcast license, permit, certificate, or other instrument of authorization issued by the Commission, and if the violator is determined by the Commission to have broadcast obscene, indecent, or profane material, the forfeiture penalty under this section shall

not exceed \$479,945 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of \$4,430,255 for any single act or failure to act described in paragraph (a) of this section.

(2) *Forfeiture penalty for a common carrier or applicant.* If the violator is a common carrier subject to the provisions of the Communications Act or an applicant for any common carrier license, permit, certificate, or other instrument of authorization issued by the Commission, the amount of any forfeiture penalty determined under this section shall not exceed \$237,268 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of \$2,372,677 for any single act or failure to act described in paragraph (a) of this section.

(3) *Forfeiture penalty for a manufacturer or service provider.* If the violator is a manufacturer or service provider subject to the requirements of section 255, 716, or 718 of the Communications Act (47 U.S.C. 255, 617, or 619), and is determined by the Commission to have violated any such requirement, the manufacturer or service provider shall be liable to the United States for a forfeiture penalty of not more than \$136,258 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of \$1,362,567 for any single act or failure to act.

(4) *Forfeiture penalty for a 227(e) violation.* Any person determined to have violated section 227(e) of the Communications Act or the rules issued by the Commission under section 227(e) of the Communications Act shall be liable to the United States for a forfeiture penalty of not more than \$13,625 for each violation or three times that amount for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of \$1,362,567 for any single act or failure to act. Such penalty shall be in addition to any other forfeiture penalty provided for by the Communications Act.

(5) *Forfeiture penalty for a 227(b)(4)(B) violation.* Any person determined to have violated section 227(b)(4)(B) of the Communications Act or the rules in 47 CFR part 64 issued by the Commission under section 227(b)(4)(B) of the Communications Act shall be liable to the United States for a forfeiture penalty determined in accordance with paragraphs (A)–(F) of section 503(b)(2) plus an additional penalty not to exceed \$11,580.

(6) *Forfeiture penalty for pirate radio broadcasting.* (i) Any person who willfully and knowingly does or causes or suffers to be done any pirate radio broadcasting shall be subject to a fine of not more than \$2,316,034; and

(ii) Any person who willfully and knowingly violates the Act or any rule, regulation, restriction, or condition made or imposed by the Commission under authority of the Act, or any rule, regulation, restriction, or condition made or imposed by any international radio or wire communications treaty or convention, or regulations annexed thereto, to which the United States is party, relating to pirate radio broadcasting shall, in addition to any other penalties provided by law, be subject to a fine of not more than \$115,802 for each day during which such offense occurs, in accordance with the limit described in this section.

(7) *Forfeiture penalty for a section 6507(b)(4) Tax Relief Act violation.* If a violator who is granted access to the Do-Not-Call registry of public safety answering points discloses or disseminates any registered telephone number without authorization, in violation of section 6507(b)(4) of the Middle Class Tax Relief and Job Creation Act of 2012 or the Commission's implementing rules in 47 CFR part 64, the monetary penalty for such unauthorized disclosure or dissemination of a telephone number from the registry shall be not less than \$127,602 per incident nor more than \$1,276,024 per incident depending upon whether the conduct leading to the violation was negligent, grossly negligent, reckless, or willful, and depending on whether the violation was a first or subsequent offense.

Federal Communications Commission

§ 1.80

(8) *Forfeiture penalty for a section 6507(b)(5) Tax Relief Act violation.* If a violator uses automatic dialing equipment to contact a telephone number on the Do-Not-Call registry of public safety answering points, in violation of section 6507(b)(5) of the Middle Class Tax Relief and Job Creation Act of 2012 or the Commission's implementing rules in 47 CFR part 64, the monetary penalty for contacting such a telephone number shall be not less than \$12,760 per call nor more than \$127,602 per call depending on whether the violation was negligent, grossly negligent, reckless, or willful, and depending on whether the violation was a first or subsequent offense.

(9) *Forfeiture penalty for a failure to block.* Any person determined to have failed to block illegal robocalls pursuant to §§ 64.6305(g) and 64.1200(n) of this chapter shall be liable to the United States for a forfeiture penalty of no more than \$23,727 for each violation, to be assessed on a per-call basis.

(10) *Maximum forfeiture penalty for any case not previously covered.* In any case not covered in paragraphs (b)(1) through (9) of this section, the amount of any forfeiture penalty determined under this section shall not exceed \$23,727 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of \$177,951 for any single act or failure to act described in paragraph (a) of this section.

(11) *Factors considered in determining the amount of the forfeiture penalty.* In determining the amount of the forfeiture penalty, the Commission or its designee will take into account the nature, circumstances, extent and gravity of the violations and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require.

TABLE 1 TO PARAGRAPH (b)(11)—BASE AMOUNTS FOR SECTION 503 FORFEITURES

Forfeitures	Violation amount
Misrepresentation/lack of candor	(¹)
Failure to file required DODC required forms, and/or filing materially inaccurate or incomplete DODC information	\$15,000
Construction and/or operation without an instrument of authorization for the service	10,000
Failure to comply with prescribed lighting and/or marking	10,000
Violation of public file rules	10,000
Violation of political rules: Reasonable access, lowest unit charge, equal opportunity, and discrimination	9,000
Unauthorized substantial transfer of control	8,000
Violation of children's television commercialization or programming requirements	8,000
Violations of rules relating to distress and safety frequencies	8,000
False distress communications	8,000
EAS equipment not installed or operational	8,000
Alien ownership violation	8,000
Failure to permit inspection	7,000
Transmission of indecent/obscene materials	7,000
Interference	7,000
Importation or marketing of unauthorized equipment	7,000
Exceeding of authorized antenna height	5,000
Fraud by wire, radio or television	5,000
Unauthorized discontinuance of service	5,000
Use of unauthorized equipment	5,000
Exceeding power limits	4,000
Failure to Respond to Commission communications	4,000
Violation of sponsorship ID requirements	4,000
Unauthorized emissions	4,000
Using unauthorized frequency	4,000
Failure to engage in required frequency coordination	4,000
Construction or operation at unauthorized location	4,000
Violation of requirements pertaining to broadcasting of lotteries or contests	4,000
Violation of transmitter control and metering requirements	3,000
Failure to file required forms or information	3,000
Per call violations of the robocall blocking rules	2,500
Failure to make required measurements or conduct required monitoring	2,000
Failure to provide station ID	1,000
Unauthorized pro forma transfer of control	1,000
Failure to maintain required records	1,000

TABLE 2 TO PARAGRAPH (b)(11)—VIOLATIONS UNIQUE TO THE SERVICE

Violation	Services affected	Amount
Unauthorized conversion of long distance telephone service	Common Carrier	\$40,000
Violation of operator services requirements	Common Carrier	7,000
Violation of pay-per-call requirements	Common Carrier	7,000
Failure to implement rate reduction or refund order	Cable	7,500
Violation of cable program access rules	Cable	7,500
Violation of cable leased access rules	Cable	7,500
Violation of cable cross-ownership rules	Cable	7,500
Violation of cable broadcast carriage rules	Cable	7,500
Violation of pole attachment rules	Cable	7,500
Failure to maintain directional pattern within prescribed parameters	Broadcast	7,000
Violation of broadcast hoax rule	Broadcast	7,000
AM tower fencing	Broadcast	7,000
Broadcasting telephone conversations without authorization	Broadcast	4,000
Violation of enhanced underwriting requirements	Broadcast	2,000

TABLE 3 TO PARAGRAPH (b)(11)—ADJUSTMENT CRITERIA FOR SECTION 503 FORFEITURES

Upward Adjustment Criteria:

- (1) Egregious misconduct.
- (2) Ability to pay/relative disincen-tive.
- (3) Intentional violation.
- (4) Substantial harm.
- (5) Prior violations of any FCC re-quirements.
- (6) Substantial economic gain.
- (7) Repeated or continuous viola-tion.

Downward Adjustment Criteria:

- (1) Minor violation.
- (2) Good faith or voluntary disclo-sure.
- (3) History of overall compliance.
- (4) Inability to pay.

TABLE 4 TO PARAGRAPH (b)(11)—NON-SECTION 503 FORFEITURES THAT ARE AFFECTED BY THE DOWNWARD ADJUSTMENT FACTORS¹—Continued

Violation	Statutory amount after 2023 annual in-fla-tion adjustment
Sec. 227(e) Caller Identification.	\$13,625/violation. \$40,875/day for each day of continuing violation, up to \$1,362,567 for any single act or fail-ure to act.
Sec. 364(a) Forfeit-ures (Ships).	\$11,864/day (owner).
Sec. 364(b) Forfeit-ures (Ships).	\$2,374 (vessel master).
Sec. 386(a) Forfeit-ures (Ships).	\$11,864/day (owner).
Sec. 386(b) Forfeit-ures (Ships).	\$2,374 (vessel master).
Sec. 511 Pirate Radio Broad-casting.	\$2,316,034, \$115,802/day.
Sec. 634 Cable EEO.	\$1,052/day.

TABLE 4 TO PARAGRAPH (b)(11)—NON-SECTION 503 FORFEITURES THAT ARE AFFECTED BY THE DOWNWARD ADJUSTMENT FACTORS¹

Violation	Statutory amount after 2023 annual in-fla-tion adjustment
Sec. 202(c) Com-mon Carrier Dis-crimination.	\$14,236, \$712/day.
Sec. 203(e) Com-mon Carrier Tar-iffs.	\$14,236, \$712/day.
Sec. 205(b) Com-mon Carrier Pre-scriptions.	\$28,472.
Sec. 214(d) Com-mon Carrier Line Extensions.	\$2,847/day.
Sec. 219(b) Com-mon Carrier Re-ports.	\$2,847/day.
Sec. 220(d) Com-mon Carrier Records & Ac-counts.	\$14,236/day.
Sec. 223(b) Dial-a-Porn.	\$147,529/day.

¹ Unlike section 503 of the Act, which establishes maximum forfeiture amounts, other sections of the Act, with two excep-tions, state prescribed amounts of forfeitures for violations of the relevant section. These amounts are then subject to miti-gation or remission under section 504 of the Act. One excep-tion is section 223 of the Act, which provides a maximum for-feiture per day. For convenience, the Commission will treat this amount as if it were a prescribed base amount, subject to downward adjustments. The other exception is section 227(e) of the Act, which provides maximum forfeitures per violation, and for continuing violations. The Commission will apply the factors set forth in section 503(b)(2)(E) of the Act and this table 4 to determine the amount of the penalty to assess in any particular situation. The amounts in this table 4 are ad-justed for inflation pursuant to the Debt Collection Improve-ment Act of 1996 (DCIA), 28 U.S.C. 2461. These non-section 503 forfeitures may be adjusted downward using the “Down-ward Adjustment Criteria” shown for section 503 forfeitures in table 3 to this paragraph (b)(11).

NOTE 2 TO PARAGRAPH (b)(11): *Guidelines for Assessing Forfeitures.* The Commission and its staff may use the guidelines in tables 1 through 4 of this paragraph (b)(11) in par-ticular cases. The Commission and its staff retain the discretion to issue a higher or lower forfeiture than provided in the guide-lines, to issue no forfeiture at all, or to apply alternative or additional sanctions as per-mitted by the statute. The forfeiture ceilings

Federal Communications Commission

§ 1.80

per violation or per day for a continuing violation stated in section 503 of the Communications Act and the Commission’s rules are described in paragraph (b)(12) of this section. These statutory maxima became effective September 13, 2013. Forfeitures issued under other sections of the Act are dealt with separately in table 4 to this paragraph (b)(11).

(12) *Inflation adjustments to the maximum forfeiture amount.* (i) Pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, Public Law 114–74 (129 Stat. 599–600), which amends the Federal Civil Monetary Penalty Inflation Adjustment Act of 1990, Public Law 101–410 (104 Stat. 890; 28 U.S.C. 2461 note), the statutory maximum amount of a forfeiture penalty assessed under this section shall be adjusted annually for inflation by order published no later than

January 15 each year. Annual inflation adjustments will be based on the percentage (if any) by which the Consumer Price Index for all Urban Consumers (CPI-U) for October preceding the date of the adjustment exceeds the prior year’s CPI-U for October. The Office of Management and Budget (OMB) will issue adjustment rate guidance no later than December 15 each year to adjust for inflation in the CPI-U as of the most recent October.

(ii) The application of the annual inflation adjustment required by the foregoing Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 results in the following adjusted statutory maximum forfeitures authorized by the Communications Act:

TABLE 5 TO PARAGRAPH (b)(12)(ii)

U.S. Code citation	Maximum penalty after 2023 annual inflation adjustment
47 U.S.C. 202(c)	\$14,236, \$712.
47 U.S.C. 203(e)	\$14,236, \$712.
47 U.S.C. 205(b)	\$28,472.
47 U.S.C. 214(d)	\$2,847.
47 U.S.C. 219(b)	\$2,847.
47 U.S.C. 220(d)	\$14,236.
47 U.S.C. 223(b)	\$147,529.
47 U.S.C. 227(b)(4)(B)	\$59,316, plus an additional penalty not to exceed \$11,580; \$593,170, plus an additional penalty not to exceed \$11,580; \$237,268, plus an additional penalty not to exceed \$11,580; \$2,372,677, plus an additional penalty not to exceed \$11,580; \$479,945, plus an additional penalty not to exceed \$11,580; \$4,430,255, plus an additional penalty not to exceed \$11,580; \$23,727, plus an additional penalty not to exceed \$11,580; \$177,951, plus an additional penalty not to exceed \$11,580; \$136,258, plus an additional penalty not to exceed \$11,580; \$1,362,567, plus an additional penalty not to exceed \$11,580.
47 U.S.C. 227(e)	\$13,625, \$40,875, \$1,362,567.
47 U.S.C. 362(a)	\$11,864.
47 U.S.C. 362(b)	\$2,374.
47 U.S.C. 386(a)	\$11,864.
47 U.S.C. 386(b)	\$2,374.
47 U.S.C. 503(b)(2)(A)	\$59,316, \$593,170.
47 U.S.C. 503(b)(2)(B)	\$237,268, \$2,372,677.
47 U.S.C. 503(b)(2)(C)	\$479,945, \$4,430,255.
47 U.S.C. 503(b)(2)(D)	\$23,727, \$177,951.
47 U.S.C. 503(b)(2)(F)	\$136,258, \$1,362,567.
47 U.S.C. 507(a)	\$2,350.
47 U.S.C. 507(b)	\$345.
47 U.S.C. 511	\$2,316,034, \$115,802.
47 U.S.C. 554	\$1,052.
Sec. 6507(b)(4) of Tax Relief Act	\$1,276,024/incident.
Sec. 6507(b)(5) of Tax Relief Act	\$127,602/call.

NOTE 3 TO PARAGRAPH (b)(12): Pursuant to Public Law 104–134, the first inflation adjustment cannot exceed 10 percent of the statutory maximum amount.

(c) *Limits on the time when a proceeding may be initiated.* (1) In the case of a broadcast station, no forfeiture penalty shall be imposed if the viola-

tion occurred more than 1 year prior to the issuance of the appropriate notice or prior to the date of commencement of the current license term, whichever is earlier. For purposes of this paragraph, “date of commencement of the current license term” means the date of commencement of the last term of

license for which the licensee has been granted a license by the Commission. A separate license term shall not be deemed to have commenced as a result of continuing a license in effect under section 307(c) pending decision on an application for renewal of the license.

(2) In the case of a forfeiture imposed against a carrier under sections 202(c), 203(e), and 220(d), no forfeiture will be imposed if the violation occurred more than 5 years prior to the issuance of a notice of apparent liability.

(3) In the case of a forfeiture imposed under section 227(e), no forfeiture will be imposed if the violation occurred more than 4 years prior to the date on which the appropriate notice was issued.

(4) In the case of a forfeiture imposed under section 227(b)(4)(B), no forfeiture will be imposed if the violation occurred more than 4 years prior to the date on which the appropriate notice is issued.

(5) In all other cases, no penalty shall be imposed if the violation occurred more than 1 year prior to the date on which the appropriate notice is issued.

(d) *Preliminary procedure in some cases; citations.* Except for a forfeiture imposed under sections 227(b), 227(e)(5), 511(a), and 511(b) of the Act, no forfeiture penalty shall be imposed upon any person under the preceding sections if such person does not hold a license, permit, certificate, or other authorization issued by the Commission, and if such person is not an applicant for a license, permit, certificate, or other authorization issued by the Commission, unless, prior to the issuance of the appropriate notice, such person:

(1) Is sent a citation reciting the violation charged;

(2) Is given a reasonable opportunity (usually 30 days) to request a personal interview with a Commission official, at the field office which is nearest to such person's place of residence; and

(3) Subsequently engages in conduct of the type described in the citation. However, a forfeiture penalty may be imposed, if such person is engaged in (and the violation relates to) activities for which a license, permit, certificate, or other authorization is required or if such person is a cable television operator, or in the case of violations of sec-

tion 303(q), if the person involved is a nonlicensee tower owner who has previously received notice of the obligations imposed by section 303(q) from the Commission or the permittee or licensee who uses that tower. Paragraph (c) of this section does not limit the issuance of citations. When the requirements of this paragraph have been satisfied with respect to a particular violation by a particular person, a forfeiture penalty may be imposed upon such person for conduct of the type described in the citation without issuance of an additional citation.

(e) *Preliminary procedure in Preventing Illegal Radio Abuse Through Enforcement Act (PIRATE Act) cases.* Absent good cause, in any case alleging a violation of subsection (a) or (b) of section 511 of the Act, the Commission shall proceed directly to issue a notice of apparent liability for forfeiture without first issuing a notice of unlicensed operation.

(f) *Alternative procedures.* In the discretion of the Commission, a forfeiture proceeding may be initiated either: (1) By issuing a notice of apparent liability, in accordance with paragraph (f) of this section, or (2) a notice of opportunity for hearing, in accordance with paragraph (g).

(g) *Notice of apparent liability.* Before imposing a forfeiture penalty under the provisions of this paragraph, the Commission or its designee will issue a written notice of apparent liability.

(1) *Content of notice.* The notice of apparent liability will:

(i) Identify each specific provision, term, or condition of any act, rule, regulation, order, treaty, convention, or other agreement, license, permit, certificate, or instrument of authorization which the respondent has apparently violated or with which he has failed to comply,

(ii) Set forth the nature of the act or omission charged against the respondent and the facts upon which such charge is based,

(iii) State the date(s) on which such conduct occurred, and

(iv) Specify the amount of the apparent forfeiture penalty.

(2) *Delivery.* The notice of apparent liability will be sent to the respondent,

by certified mail, at his last known address (see §1.5).

(3) *Response.* The respondent will be afforded a reasonable period of time (usually 30 days from the date of the notice) to show, in writing, why a forfeiture penalty should not be imposed or should be reduced, or to pay the forfeiture. Any showing as to why the forfeiture should not be imposed or should be reduced shall include a detailed factual statement and such documentation and affidavits as may be pertinent.

(4) *Forfeiture order.* If the proposed forfeiture penalty is not paid in full in response to the notice of apparent liability, the Commission, upon considering all relevant information available to it, will issue an order canceling or reducing the proposed forfeiture or requiring that it be paid in full and stating the date by which the forfeiture must be paid.

(5) *Judicial enforcement of forfeiture order.* If the forfeiture is not paid, the case will be referred to the Department of Justice for collection under section 504(a) of the Communications Act.

(h) *Notice of opportunity for hearing.* The procedures set out in this paragraph apply only when a formal hearing under section 503(b)(3)(A) of the Communications Act is being held to determine whether to assess a forfeiture penalty.

(1) Before imposing a forfeiture penalty, the Commission may, in its discretion, issue a notice of opportunity for hearing. The formal hearing proceeding shall be conducted by an administrative law judge under procedures set out in subpart B of this part, including procedures for appeal and review of initial decisions. A final Commission order assessing a forfeiture under the provisions of this paragraph is subject to judicial review under section 402(a) of the Communications Act.

(2) If, after a forfeiture penalty is imposed and not appealed or after a court enters final judgment in favor of the Commission, the forfeiture is not paid, the Commission will refer the matter to the Department of Justice for collection. In an action to recover the forfeiture, the validity and appropriateness of the order imposing the forfeiture are not subject to review.

(3) Where the possible assessment of a forfeiture is an issue in a hearing proceeding to determine whether a pending application should be granted, and the application is dismissed pursuant to a settlement agreement or otherwise, and the presiding judge has not made a determination on the forfeiture issue, the presiding judge shall forward the order of dismissal to the attention of the full Commission. Within the time provided by §1.117, the Commission may, on its own motion, proceed with a determination of whether a forfeiture against the applicant is warranted. If the Commission so proceeds, it will provide the applicant with a reasonable opportunity to respond to the forfeiture issue (see paragraph (f)(3) of this section) and make a determination under the procedures outlined in paragraph (f) of this section.

(i) *Payment.* The forfeiture should be paid electronically using the Commission's electronic payment system in accordance with the procedures set forth on the Commission's website, www.fcc.gov/licensing-databases/fees.

(j) *Remission and mitigation.* In its discretion, the Commission, or its designee, may remit or reduce any forfeiture imposed under this section. After issuance of a forfeiture order, any request that it do so shall be submitted as a petition for reconsideration pursuant to §1.106.

(k) *Effective date.* Amendments to paragraph (b) of this section implementing Pub. L. No. 101–239 are effective December 19, 1989.

[43 FR 49308, Oct. 23, 1978, as amended at 48 FR 15631, Apr. 12, 1983; 50 FR 40855, Oct. 7, 1985; 55 FR 25605, June 22, 1990; 56 FR 25638, June 5, 1991; 57 FR 23161, June 2, 1992; 57 FR 47006, Oct. 14, 1992; 57 FR 48333, Oct. 23, 1992; 58 FR 6896, Feb. 3, 1993; 58 FR 27473, May 10, 1993; 62 FR 4918, Feb. 3, 1997; 62 FR 43475, Aug. 14, 1997; 63 FR 26992, May 15, 1998; 65 FR 60868, Oct. 13, 2000; 69 FR 47789, Aug. 6, 2004; 72 FR 33914, June 20, 2007; 73 FR 9018, Feb. 19, 2008; 73 FR 44664, July 31, 2008; 76 FR 43203, July 20, 2011; 76 FR 82388, Dec. 30, 2011; 77 FR 71137, Nov. 29, 2012; 78 FR 10100, Feb. 13, 2013; 78 FR 49371, Aug. 14, 2013; 81 FR 42555, June 30, 2016; 82 FR 8171, Jan. 24, 2017; 82 FR 57882, Dec. 8, 2017; 83 FR 4600, Feb. 1, 2018; 84 FR 2462, Feb. 7, 2019; 85 FR 2318, Jan. 15, 2020; 85 FR 22029, Apr. 21, 2020; 85 FR 38333, June 26, 2020; 85 FR 63172, Oct. 6, 2020; 86 FR 3830, Jan. 15, 2021; 86 FR 15797, Mar. 25, 2021; 86 FR 18159, Apr. 7, 2021; 87 FR 397, Jan. 5, 2022; 88 FR 784, Jan. 5, 2023; 88 FR 40116, June 21, 2023]

§ 1.83 Applications for radio operator licenses.

(a) Application filing procedures for amateur radio operator licenses are set forth in part 97 of this chapter.

(b) Application filing procedures for commercial radio operator licenses are set forth in part 13 of this chapter. Detailed information about application forms, filing procedures, and where to file applications for commercial radio operator licenses is contained in the bulletin “Commercial Radio Operator Licenses and Permits.” This bulletin is available from the Commission’s Forms Distribution Center by calling 1–800–418–FORM (3676).

[47 FR 53378, Nov. 26, 1982, as amended at 58 FR 13021, Mar. 9, 1993; 63 FR 68920, Dec. 14, 1998]

§ 1.85 Suspension of operator licenses.

Whenever grounds exist for suspension of an operator license, as provided in section 303(m) of the Communications Act, the Chief of the Wireless Telecommunications Bureau, with respect to amateur and commercial radio operator licenses, may issue an order suspending the operator license. No order of suspension of any operator’s license shall take effect until 15 days’ notice in writing of the cause for the proposed suspension has been given to

the operator licensee, who may make written application to the Commission at any time within the said 15 days for a hearing upon such order. The notice to the operator licensee shall not be effective until actually received by him, and from that time he shall have 15 days in which to email the said application. In the event that conditions prevent emailing of the application before the expiration of the 15-day period, the application shall then be emailed as soon as possible thereafter, accompanied by a satisfactory explanation of the delay. Upon receipt by the Commission of such application for hearing, said order of suspension shall be designated for hearing by the Chief, Wireless Telecommunications Bureau and said suspension shall be held in abeyance until the conclusion of the hearing. Upon the conclusion of said hearing, the Commission may affirm, modify, or revoke said order of suspension. If the license is ordered suspended, the operator shall send his operator license to the Mobility Division, Wireless Telecommunications Bureau, in Washington, DC, on or before the effective date of the order, or, if the effective date has passed at the time notice is received, the license shall be sent to the Commission forthwith.

[85 FR 85529, Dec. 29, 2020]

§ 1.87 Modification of license or construction permit on motion of the Commission.

(a) Whenever it appears that a station license or construction permit should be modified, the Commission shall notify the licensee or permittee in writing of the proposed action and reasons therefor, and afford the licensee or permittee at least thirty days to protest such proposed order of modification, except that, where safety of life or property is involved, the Commission may by order provide a shorter period of time.

(b) The notification required in paragraph (a) of this section may be effectuated by a notice of proposed rule-making in regard to a modification or addition of an FM or television channel to the Table of Allotments (§§ 73.202 and 73.504 of this chapter) or Table of Assignments (§73.606 of this chapter). The Commission shall send a copy of any

47 C.F.R. § 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 § 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.

47 C.F.R. § 64.2010

Safeguards on the disclosure of customer proprietary network information.

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

* * *