No.

In the Supreme Court of the United States

VERIZON COMMUNICATIONS INC.,
PETITIONER,

v.

FEDERAL COMMUNICATIONS COMMISSION AND
UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

SCOTT H. ANGSTREICH
AASEESH P. POLAVARAPU
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street NW
Suite 400
Washington, DC 20036

JEFFREY B. WALL
Counsel of Record
MORGAN L. RATNER
DANIEL A. MEJIA-CRUZ
SULLIVAN & CROMWELL LLP
1700 New York Avenue NW
Suite 700
Washington, DC 20006
(202) 956-7660
wallj@sullcrom.com

MAXWELL F. GOTTSCHALL
SULLIVAN & CROMWELL LLP
125 Broad Street
New York, NY 10004

QUESTION PRESENTED

Under the Communications Act of 1934, the Federal Communications Commission may assess monetary "forfeiture penalties" for violations of the Act, including the requirement that telecommunications carriers take reasonable measures to protect certain customer data. 47 U.S.C. §§ 222, 503, 504. The FCC may impose such forfeiture penalties in administrative proceedings. *Id.* § 503(b)(4). If a carrier wants to guarantee judicial review, it must pay the penalty and then seek review in a court of appeals, which reviews the agency's order on the administrative record under the deferential standards of the Administrative Procedure Act. 47 U.S.C. § 402(a); 5 U.S.C. § 706(2). If the carrier wants a jury trial, by contrast, it must defy the FCC's order and refuse to pay, after which the Department of Justice may, but is not required to, file a lawsuit in district court to collect the unpaid forfeiture. 47 U.S.C. § 504(a). While waiting for that DOJ lawsuit that might never come, the carrier suffers serious practical and reputational harms from the final FCC order. The question presented is:

Whether the Communications Act violates the Seventh Amendment and Article III by authorizing the FCC to order the payment of monetary penalties for failing to reasonably safeguard customer data, without guaranteeing the defendant carrier a right to a jury trial.

PARTIES TO THE PROCEEDING

Petitioner is Verizon Communications Inc. Respondents are the Federal Communications Commission and the United States of America.

RULE 29.6 DISCLOSURE STATEMENT

Petitioner Verizon Communications Inc. certifies that it is a publicly traded corporation and it has no corporate parent. No publicly held corporation owns 10% or more of Verizon Communications Inc.'s stock.

RELATED PROCEEDINGS

United States Court of Appeals (2d Cir.):

Verizon Communications Inc. v. *Federal Communications Commission, United States of America*, No. 24-1733 (Sept. 10, 2025)

TABLE OF CONTENTS

Page

Introduction 1
Opinions below 4
Jurisdiction 4
Constitutional and statutory provisions involved 4
Statement of the case 4
A. Legal background 4
B. Factual background 8
C. Procedural background 10
Reasons for granting the petition 13
I. The decision below is wrong 14
A. Defendants are entitled to a jury trial when the FCC seeks forfeiture penalties to enforce Section 222 14
B. The Communications Act's judicial-review scheme does not satisfy the Seventh Amendment 17
II. The decision below warrants review 29
A. The courts of appeals are divided on the question presented 30
B. The question presented is important 31
C. The Court should grant review in both this case and *AT&T* 33
Conclusion 35

Appendix A — Court of appeals opinion (Sept. 10, 2025) 1a

Appendix B — FCC order (Apr. 29, 2024) 41a

Appendix C — Constitutional, statutory, and regulatory provisions:
U.S. Const., amend. VII 152a
47 U.S.C. § 222 ..... 152a
47 U.S.C. § 503 ..... 158a
47 U.S.C. § 504 ..... 166a
47 C.F.R. § 1.80 ..... 167a
47 C.F.R. § 64.2010 ..... 176a

TABLE OF AUTHORITIES

Page(s)

Cases:

AT&T, Inc. v. *FCC*,
149 F.4th 491
(5th Cir. 2025).....13, 15-17, 23-24, 28, 30

B & B Hardware, Inc. v. *Hargis Indus., Inc.*,
575 U.S. 138 (2015) 24

Brown v. *United States*,
602 U.S. 101 (2024) 33

Campos-Chaves v. *Garland*,
602 U.S. 447 (2024) 34

Capital Traction Co. v. *Hof*,
174 U.S. 1 (1899) 26-27

Carpenter v. *United States*,
585 U.S. 296 (2018) 8

Curtis v. *Loether*,
415 U.S. 189 (1974) 19

Dimick v. *Schiedt*,
293 U.S. 474 (1935) 1-2, 19, 29

FCC v. *Fox Television Stations, Inc.*,
567 U.S. 239 (2012) 24

Free Enterprise Fund v. *PCAOB*,
561 U.S. 477 (2010) 26

Fuld v. *Palestine Liberation Org.*,
606 U.S. 1 (2025) 33

Granfinanciera, S.A. v. *Nordberg*,
492 U.S. 33 (1989) 20

Knickerbocker Ins. Co. of Chicago v. *Comstock*,
83 U.S. 258 (1872) 20
Meeker v. *Lehigh Valley Railroad Co.*,
236 U.S. 412 (1915) 27-28
Parsons v. *Bedford*,
28 U.S. 433 (1830) 17-19
In re Peterson,
253 U.S. 300 (1920) 23-24, 28-29
Reid v. *Covert*,
354 U.S. 1 (1957) 19
Sackett v. *EPA*,
598 U.S. 651 (2023) 25
SEC v. *Jarkesy*,
603 U.S. 109 (2024) 2, 12-13, 15-18, 20, 29, 31, 33
Simler v. *Conner*,
372 U.S. 221 (1963) 20
Southwick v. *Stevens*,
10 Johns. 443 (N.Y. Sup. Ct. 1813) 26
Sprint Corp. v. *FCC*,
151 F.4th 347 (D.C. Cir. 2025)..... 30-31
Thomas v. *Humboldt County*,
607 U.S. ___ (2025) 18
Tull v. *United States*,
481 U.S. 412 (1987) 15-16
United States v. *Jackson*,
390 U.S. 570 (1968) 24
United States v. *Stevens*,
691 F.3d 620 (5th Cir. 2012) 34

Constitutional provisions:

U.S. Const., amend. VII.....15, 18, 21, 25

Statutes:

Federal Communications Act of 1934,
47 U.S.C. § 151 *et seq.* 4
§ 222 ..... 5, 10, 16
§ 402 ..... 6-7, 22, 27
§ 503 ..... 5-6, 15-16, 20-22, 24, 32
§ 504 ..... 7, 16, 20, 22
Pub. L. No. 104-104, § 702, 110 Stat. 56 5
5 U.S.C. § 706 ..... 7, 27
28 U.S.C.
§ 1254 4
§ 2342 ..... 7, 22
§ 2344 7
§ 2346 7
§ 2347 7
§ 2462 ..... 7, 22

Regulations:

47 C.F.R. § 1.80 ..... 5-6, 11
47 C.F.R. § 64.2007 5
47 C.F.R. § 64.2010 ..... 5, 10, 16

Other authorities:

3 William Blackstone, Commentaries on the Laws of England (8th ed. 1778) 1, 18
Charles W. Wolfram, *The Constitutional History of the Seventh Amendment*, 57 Minn. L. Rev. 639 (1973) 19
Essay of a Democratic Federalist (Oct. 17, 1787), *in* 3 The Complete Anti-Federalist 61 (Herbert Storing ed. 1981) 19

Federal Communications Commission's
Forfeiture Policy Statement & Amendment
of Section 1.80 of the Rules to Incorporate the
Forfeiture Guidelines,
12 FCC Rcd. 17087 (1997) 25

Petition for Writ of Certiorari, *FCC* v. *AT&T*
(No. 25-406) 3-4, 14, 15, 17, 21, 26-27, 31, 33

The Federalist No. 83 (A. Hamilton) 18-19

In the Supreme Court of the United States

No.

VERIZON COMMUNICATIONS INC.,
PETITIONER,

v.

FEDERAL COMMUNICATIONS COMMISSION AND
UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

INTRODUCTION

William Blackstone praised the right to a civil jury trial as "the glory of the English law." 3 William Blackstone, Commentaries on the Laws of England 379 (8th ed. 1778). After its notable omission from the Constitution of 1789, the Framers enshrined that right in the Seventh Amendment. This Court has since affirmed that "[m]aintenance of the jury as a factfinding body is of such importance," and "occupies so firm a place in our history and jurisprudence," "that any seeming curtailment of the right to a jury

trial should be scrutinized with the utmost care." *Dimick* v. *Schiedt*, 293 U.S. 474, 486 (1935).

This Court engaged in that careful scrutiny in *SEC* v. *Jarkesy*, 603 U.S. 109 (2024). In *Jarkesy*, the Court held unconstitutional under the Seventh Amendment an SEC administrative scheme that allowed the agency to impose monetary penalties for fraud without the protections of a jury trial. The Court reasoned that civil monetary penalties designed to punish or deter a wrongdoer—rather than to restore the status quo—are a classic remedy at common law, and a defendant is generally entitled to a jury trial before such remedy is imposed. *Id.* at 123.

The FCC scheme at issue here mirrors the SEC scheme rejected in *Jarkesy* in every material respect. The FCC ordered Verizon to pay $47 million as a forfeiture penalty based on the alleged failure to safeguard customer data. The agency claimed the authority to ratchet up that number to the billions of dollars (or even, by the logic of its statutory interpretation, trillions of dollars), but selected its $47 million fine based on the level of culpability that it perceived here. There can be no doubt that the remedy is punitive and thus legal, and that the underlying cause of action is akin to common-law negligence. So this should have been an easy case under *Jarkesy*.

The government, however, has seized on a distinct statutory quirk to defend the FCC's penalty scheme. After the FCC imposes a final payment order in-house, a telecommunications carrier has two options to pursue further review. First, it can pay the FCC order and go right to the court of appeals (where no jury is available). Second, the carrier can defy the FCC's order and wait to see whether the Department

of Justice decides to bring a collection action in district court at some point over the next five years. Because *that potential collection action* carries a right to a jury trial, the FCC sees no Seventh Amendment problem with imposing massive in-house penalties beforehand. The Second Circuit and D.C. Circuit have both blessed the FCC's theory, while the Fifth Circuit has rejected it as pure constitutional circumvention.

The after-the-fact possibility of a jury trial does not comply with the Seventh Amendment for several reasons. First, a jury trial in a separate collection action cannot possibly satisfy the Seventh Amendment's guarantee of a jury trial in *this* action, in which the government has imposed a final, multimillion-dollar penalty on a defendant. Second, linking a jury trial to a possible collection action is no guarantee at all; it leaves a defendant carrier as an adjudicated violator that gets its day in court only if the Department of Justice so chooses. Third, this penalty-now-trial-later system imposes far too heavy burdens on the exercise of a carrier's Seventh Amendment rights. To maintain even the chance at an eventual jury, a carrier must forgo its right to appeal and incur the practical, financial, and reputational costs of flouting a final agency order requiring prompt payment of a potentially massive penalty. Unsurprisingly, carriers never choose that option; they pay, so that they can immediately appeal. This is, in short, only the faintest shadow of the jury trial right that Blackstone praised, the Framers preserved, and this Court reinvigorated in *Jarkesy*.

Of course, the Court need not decide the merits now. There is a clear, acknowledged 2-1 circuit split. The government has also sought certiorari. *See* Peti-

tion for Writ of Certiorari, *FCC* v. *AT&T* (No. 25-406) (filed Oct. 3, 2025) (*AT&T* Pet.). Everyone agrees that the question is critical both to the FCC and to the carriers subject to its jurisdiction. This case is a clean vehicle, which has long traveled parallel with *AT&T*. The Court therefore should grant both cases, consolidate them for briefing and oral argument, and realign the parties so that the carriers are on one side and the FCC is on the other.

OPINIONS BELOW

The opinion of the court of appeals (App., *infra*, 1a-40a) is not yet reported but is currently available at 2025 WL 2609127. The Federal Communications Commission's order (App., *infra*, 41a-151a) is available at 39 FCC Rcd. 4259.

JURISDICTION

The court of appeals entered judgment on September 10, 2025. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

Relevant constitutional and statutory provisions are reproduced in the appendix to this petition. App., *infra*, 152a-179a.

STATEMENT OF THE CASE

A. Legal Background

1. In 1934, Congress created the Federal Communications Commission and charged the agency with "regulating interstate and foreign commerce in communication by wire and radio." 47 U.S.C. § 151 *et seq.*

Decades later, Congress added Section 222 to the Communications Act. Telecommunications Act of 1996, Pub. L. No. 104-104, § 702, 110 Stat. 56, 148-149 (1996). That provision imposes on telecommunications carriers the duty to protect the confidentiality of certain customer information known as "customer proprietary network information," or CPNI. 47 U.S.C. § 222(c); *see id.* § 222(h)(1) (defining CPNI as information relating to "the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service" that is "made available solely . . . by virtue of the carrier-customer relationship").

The Commission has implemented Section 222 through regulations that require carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a). Those regulations generally require a customer's "opt-out approval or opt-in approval" before CPNI is disclosed. *Id.* § 64.2007(b).

Violations of Section 222 or its implementing regulations are subject to hefty fines. The FCC may impose inflation-adjusted monetary forfeiture penalties capped (in 2020) at about $200,000 for each violation or each day of a continuing violation, up to about $2 million for any single act or failure to act. 47 U.S.C. § 503(b)(2)(B); *see* 47 C.F.R. § 1.80(b)(2), (12) (adjusting the statutory maximum for inflation); App., *infra*, 114a.

In determining the amount of a forfeiture, the Commission may consider "the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other mat-

ters as justice may require." 47 U.S.C. § 503(b)(2)(E). The Commission claims the discretion to impose "upward adjustments" to base penalty amounts of 50 to 100%. App., *infra*, 121a-122a. The Commission also claims practically unlimited discretion in how it counts violations—including whether a violation amounts to a single continuing act or instead separate violations. *See id.* at 114a-115a (citing 47 U.S.C. § 503(b); 47 C.F.R. § 1.80(b)). By subdividing a single act or course of conduct into many violations, the Commission can shatter the statutory ceiling—sending penalties soaring far beyond $2 million.

2. To enforce the Communications Act, Congress authorized the Commission to impose monetary forfeiture penalties in administrative proceedings. 47 U.S.C. § 503(b)(1)(B). Section 503 establishes two alternative procedures through which the Commission may reach a final decision.

First, the Commission may proceed by formal adjudication before an administrative law judge or the Commission itself. 47 U.S.C. § 503(b)(3). A carrier can seek review in a court of appeals of any forfeiture order issued after a formal adjudication. *Id.* §§ 503(b)(3)(A), 402(a).

Second—and far more commonly—the Commission may, as it did here, issue a written notice of apparent liability and provide the defendant carrier an opportunity to submit a written response. 47 U.S.C. § 503(b)(4). After considering the carrier's written response, the Commission decides whether to affirm its notice—in which case it issues a final forfeiture order that directs the defendant to pay the penalty, normally within 30 days. 47 C.F.R. § 1.80(g)(3).

This second path, in turn, opens up two potential avenues for judicial review.

Option 1: After the agency issues a final forfeiture order, the defendant may pay in full and then petition for review within 60 days in an appropriate court of appeals under the Hobbs Act. 47 U.S.C. § 402(a); 28 U.S.C. §§ 2342(1), 2344. The court of appeals will review the FCC's order on the administrative record; no jury is involved. 28 U.S.C. §§ 2346, 2347(a). The court will set aside the agency's decision under deferential APA standards—that is, only if it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). Constitutional questions are reviewed de novo. App., *infra*, 10a.

Option 2: After the agency issues a final forfeiture order, the defendant can refuse to pay the penalty. At that point, the defendant is in violation of the order and becomes a debtor to the U.S. government, and the Department of Justice must decide whether to enforce the Commission's forfeiture order and collect the money. If the Department chooses to enforce the order, it must file a civil suit in district court "in the name of the United States" within five years of the FCC's order. 47 U.S.C. § 504(a); 28 U.S.C. § 2462. DOJ can file suit either where the defendant-carrier's principal office is located or in any district in which the carrier has deployed its communications network. 47 U.S.C. § 504(a). The defendant is entitled to a jury "trial de novo" in that collection action. *Ibid.*

In practice, Option 2—the Section 504 process—is entirely theoretical for telecommunications carriers. To the best of Verizon's knowledge, it has never been used where the Commission has imposed a forfeiture

on a carrier. Section 504 actions instead are typically brought against operators of unlicensed radio or television stations, and are resolved through summary judgment or default judgment. No Section 504 jury trial has actually occurred, at least within the last 50 years. *See* C.A. Chamber of Commerce Amicus Br. 12 ("The FCC does not point to a single actual Section 504(a) jury trial ever, and a search of cases citing Section 504(a) suggests that there has never been one."). That is not surprising because, as a practical matter, telecommunications carriers that appear regularly before the Commission—including to obtain and transfer the licenses they require to do business—do not willingly invite the serious consequences that would result from defying a final agency order that requires them to pay the government millions of dollars.

B. Factual Background

Verizon provides nationwide voice and data services over its wireless network. To enable calls and data transmissions, customer devices and carrier towers continually "ping" one another. Because carriers know the locations of their towers—and customers typically keep devices on their person—carriers may be able to approximate a customer's location at any given time. *See Carpenter* v. *United States*, 585 U.S. 296, 300, 309 (2018) (explaining that cell phones "continuously scan their environment looking for the best signal" and connect to wireless networks "several times a minute," creating a "detailed and comprehensive record of the person's movements").

Until March 2019, Verizon operated a Location-Based Services (LBS) program that—with the customers' affirmative consent—granted certain third

parties access to device-location information for customers' benefit. The other nationwide wireless carriers (including AT&T) operated similar programs. App., *infra*, 122a n.261. Verizon's program worked through two "location information aggregators," LocationSmart and Zumigo. *Id.* at 49a-50a. These aggregators contracted with other companies that offered services wireless customers desired, like roadside assistance and fraud mitigation. *Id.* at 51a-52a.

Verizon required companies seeking access to device-location information to submit applications to participate in the program, and its contracts included various information-security requirements. App., *infra*, 50a-51a. All approved providers in Verizon's LBS program had to obtain explicit consent from a Verizon customer before requesting access to that customer's location data. *Ibid.* As part of its approval process and ongoing monitoring, Verizon also relied on an outside auditor. *Id.* at 52a-53a. That auditor was tasked with reconciling daily location-request logs with customer consent records and engaging in fraud-detection efforts to make sure LBS providers did not violate the program's terms. *Ibid.* Based on these audits, Verizon could cut access to providers that failed to meet program standards and requirements. *Id.* at 58a-59a.

In May 2018, the *New York Times* reported that a program participant named Securus Technologies, Inc. had misused Verizon's and other wireless carriers' LBS programs to let a law-enforcement officer obtain device-location information in an unapproved manner and without adequate verification of customer consent. App., *infra*, 54a-56a. In particular, a Missouri sheriff had exploited the Securus system "for

non-law enforcement purposes" and without valid legal process. *Id.* at 55a.

The day after the article was published, Verizon directed LocationSmart to terminate access for Securus and its intermediary. App., *infra*, 58a. Verizon also immediately stopped approving new LBS offerings. *Id.* at 58a-61a; C.A. Doc. 38-1, at 13 (Nov. 4, 2024). Ultimately, Verizon wound down its LBS program, phasing out most remaining providers in 2018—except those providing roadside assistance—and completely ending the program by March 2019. App., *infra*, 59a-61a.

C. Procedural Background

1. After the *New York Times* article, the FCC's Enforcement Bureau opened an investigation into Verizon and three other wireless carriers (AT&T, Sprint, and T-Mobile). In February 2020, the FCC issued similar notices of apparent liability to all four, alleging violations of 47 U.S.C. § 222 and 47 C.F.R. § 64.2010. *See* App., *infra*, 144a. The Commission proposed a $48,318,750 fine for Verizon's "apparent willful and repeated violation of section 222 of the Act and section 64.2010 of the Commission's CPNI rules." *Id.* at 61a.

2. After receiving and considering Verizon's written response, the Commission issued a final forfeiture order. App., *infra*, 43a. The agency concluded that the device-location data at issue constituted CPNI under Section 222, and that Verizon had failed to reasonably protect that information both before and after the Securus disclosures. *Id.* at 63a-64a, 82a-83a. Instead of finding a single violation, the Commission divined 63 continuing violations—one for each aggrega-

tor or provider that remained in the LBS program more than 30 days after the *Times* investigation was published—and adopted a 50% upward adjustment for supposedly "egregious misconduct." *Id.* at 120a-122a; *see* 47 C.F.R. § 1.80(b)(11), Table 3. That brought the total fine to nearly $47 million (reflecting a modest reduction from the proposed penalty to correct minor errors). App., *infra*, 138a. The Commission described this figure as "eminently *conservative*," because the Commission "could well have" used "the total number of Verizon subscribers when determining the number of violations" and thus found literally "tens of millions" of violations. *Id.* at 116a-117a (emphasis in original).

Having settled on the supposedly "conservative" penalty of tens of millions of dollars, the Commission rendered its official determination. It "*ordered* that . . . Verizon Communications *is liable* for a monetary forfeiture in the amount of . . . $46,901,250 for willfully and repeatedly violating section 222 of the Act and section 64.2010 of the Commission's rules." App., *infra*, 138a (emphasis added). The Commission also ordered that "[p]ayment for the forfeiture *shall be made*" within 30 days, following the process in 47 C.F.R. § 1.80. *Id.* at 139a (emphasis added). That rule directs that forfeitures "be paid electronically using the Commission's electronic payment system" at the FCC's fee-processing website. 47 C.F.R. § 1.80(i); *see* https://www.fcc.gov/licensing-databases/fees (outlining payment methods).

3. Verizon paid the penalty and filed a timely petition for review in the Second Circuit. Verizon contended that the Commission had exceeded its statutory authority in a variety of ways and that, as relevant

here, the in-house forfeiture order violated the Seventh Amendment.

The court of appeals denied the petition. App., *infra*, 40a. The court rejected Verizon's constitutional challenge, holding that the Commission's in-house forfeiture process was consistent with Article III and the Seventh Amendment. *Id.* at 34a. The court assumed without deciding that the Seventh Amendment applied, but concluded that Verizon "had, and chose to forgo, the opportunity" for a jury trial via the Section 504 process—the deliberately-become-delinquent option discussed earlier. *Id.* at 3a; *see id.* at 34a.

In the court of appeals' view, the Communications Act "differs significantly" from the statutes at issue in *SEC* v. *Jarkesy*, 603 U.S. 109 (2024), because Section 504 of the Act "requires the government to enforce any penalty in a 'trial de novo' in federal district court." App., *infra*, 36a. The court reasoned that Verizon could have declined to pay the forfeiture and awaited a Department of Justice collection action; had it done so, it "could have gotten such a trial." *Id.* at 35a. The court believed that the forfeiture order itself created no constitutional problem because the order, though final, "does not, by itself, compel payment." *Id.* at 36a. And because the government can compel payment only through a later collection action (with a jury trial), the court reasoned that the agency's in-house adjudication "create[s] no Seventh Amendment injury." *Ibid.*

The court of appeals rejected Verizon's arguments that a Section 504 trial is constitutionally inadequate. It thus described Verizon's choice not to withhold payment and hope for such a trial as a "waiver of the jury-trial right." App., *infra*, 36a. Verizon had em-

phasized the serious consequences for carriers stuck with unchallenged, unpaid final forfeiture orders—including the FCC's own policy of using "the underlying facts of a prior violation that shows a pattern of non-compliant behavior" against a carrier in future proceedings. *Id.* at 37a. Although the court "share[d] Verizon's concerns regarding these 'real-world impacts,'" it "fail[ed] to see how they implicate the Seventh Amendment, which requires a jury trial only upon an effort to collect payment of monetary damages." *Ibid.* The court further stated that Verizon would face similar "collateral consequences" even if the agency had only admonished it. *Ibid.*

The court of appeals acknowledged that the Fifth Circuit had reached the opposite conclusion, holding in *AT&T, Inc.* v. *FCC*, 149 F.4th 491 (5th Cir. 2025) that the FCC's forfeiture process inflicts an immediate constitutional injury because the agency has already "adjudged a carrier guilty . . . and levied fines." App., *infra*, 36a (quoting *AT&T*, 149 F.4th at 503). But the court here summarily rejected that reasoning, deeming the Fifth Circuit's concerns "misplaced." *Ibid.*

REASONS FOR GRANTING THE PETITION

This FCC enforcement action for monetary penalties is "legal in nature" and therefore "implicates the Seventh Amendment" right to a jury in "suits at common law." *Jarkesy*, 603 U.S. at 121-122, 133-134. The court of appeals nevertheless found no Seventh Amendment problem because Verizon "could have declined to pay the forfeiture" ordered by the FCC "and preserved its opportunity for a *de novo* jury trial if the government sought to collect." App., *infra*, 36a.

That decision is incorrect, and it creates a square 2-1 conflict among the courts of appeals.

Just over a month ago, the government petitioned for a writ of certiorari in the case on the other side of that split. *See AT&T* Pet. This Court's review is warranted in both cases, which should be granted and consolidated. That is the Court's typical practice when it receives petitions from multiple lower-court decisions presenting the same question at virtually the same time. Here, that treatment is particularly appropriate because both *AT&T* and this case arise out of essentially one overarching FCC investigation against multiple carriers accused of similar wrongdoing.

I. THE DECISION BELOW IS WRONG.

The court of appeals did not suggest—and it is unclear whether the government still contends—that the FCC's action for forfeiture penalties here falls outside the Seventh Amendment. Instead, the court's defense of the FCC's penalty scheme rests on the argument that a jury trial in a potential after-the-fact collection action can rehabilitate a deficient administrative order adjudicating liability, calculating damages, and compelling payment within 30 days. As a matter of history, precedent, and common sense, the Seventh Amendment is not so easily avoided.

A. Defendants Are Entitled To A Jury Trial When The FCC Seeks Forfeiture Penalties To Enforce Section 222.

To begin, the Seventh Amendment guarantees a right to a jury trial when the FCC seeks forfeiture penalties under Section 222. The FCC's claim for forfeiture penalties here is on all fours with the SEC's

claim for civil penalties in *Jarkesy*, which this Court held was "legal in nature," did not involve a public right, and therefore "implicates the Seventh Amendment." 603 U.S. at 122, 125, 134. The Fifth Circuit easily concluded as much in *AT&T*. *See* 149 F.4th at 497-503. And the government does not even appear to contest the point: its petition for certiorari from the Fifth Circuit does not seek review of that holding. *AT&T* Pet. 7.

The court of appeals here "assume[d] for the sake of argument that Verizon has a Seventh Amendment right to trial by jury on the charges" here. App., *infra*, 34a. There was no need to assume; the question is not close. The Seventh Amendment guarantees that in "[s]uits at common law . . . the right of trial by jury shall be preserved." U.S. Const., amend. VII. As *Jarkesy* explained, "[t]o determine whether a suit is legal in nature," courts must "consider the cause of action and the remedy it provides." 603 U.S. at 122-123. Both considerations clearly mark Section 222 actions as legal in nature.

Begin with the "more important" consideration: whether the "cause[] of action . . . provide[s] a type of remedy available only in law courts." *Jarkesy*, 603 U.S. at 123, 136 (citation omitted). As in *Jarkesy*, "the remedy is all but dispositive" here. *Id.* at 123. The FCC invoked its statutory authority to order a "forfeiture penalty," 47 U.S.C. § 503(b)(1), of nearly $47 million. FCC forfeiture penalties are plainly designed to punish wrongdoing rather than "restore the status quo." *Tull* v. *United States*, 481 U.S. 412, 422 (1987). Like the SEC in *Jarkesy*, the FCC decides the amount of the penalty by looking to "the nature, circumstances, extent, and gravity of the violation," as

well as the carrier's "degree of culpability" and "history of prior offenses." 47 U.S.C. § 503(b)(2)(E); *see* App., *infra*, 122a-124a (imposing "substantial upward adjustment" here because the "conduct was egregious" and as a significant "disincentive to engage in similar conduct"). And like the SEC, the FCC is "not obligated to return any money to victims," *Jarkesy*, 603 U.S. at 124; the forfeiture is "payable into the Treasury," 47 U.S.C. § 504(a). At the Founding, "only courts of law issued monetary penalties to punish culpable individuals." *Jarkesy*, 603 U.S. at 123 (citation omitted). So that remedy "effectively decides that this suit implicates the Seventh Amendment right." *Id.* at 125.

The "close relationship" between Section 222 and a common-law cause of action—traditional negligence—"confirms that conclusion." *Jarkesy*, 603 U.S. at 125; *see AT&T*, 149 F.4th at 499 (noting that the "substance" of Section 222 "is closely analogous to a negligence action"). Section 222 imposes a statutory "duty to protect the confidentiality" of CPNI. 47 U.S.C. § 222(a). The FCC has long understood that duty to require carriers to "take reasonable measures to discover and protect against unauthorized access." 47 C.F.R. § 64.2010(a). A forfeiture action under Section 222 thus closely resembles a common-law negligence suit, even if the two actions are not "identical." *Jarkesy*, 603 U.S. at 126; *see Tull*, 481 U.S. at 421 ("precisely analogous common-law cause of action" not required).

Finally, notwithstanding the FCC's argument below (which the government has not repeated to this Court in its *AT&T* petition), the fact that Section 222 regulates common carriers does not bring this case

within the so-called "public rights exception" to Article III or the Seventh Amendment. At common law, negligence claims for damages against such carriers were "routinely adjudicated in state and federal courts," so they are not "within the 'historic categories of adjudications' falling *outside* Article III." *AT&T*, 149 F.4th at 501 (quoting *Jarkesy*, 603 U.S. at 130). Regardless, the exception simply does not apply where, as here, the government attempts to enforce a statute that both "provides civil penalties" and "target[s] the same basic conduct" as a common-law tort. *Jarkesy*, 603 U.S. at 134.

In short, an FCC action seeking a monetary forfeiture penalty for violations of Section 222 is undoubtedly a "suit[] in which legal rights [are] to be ascertained and determined." *Parsons* v. *Bedford*, 28 U.S. 433, 447 (1830). The Seventh Amendment therefore guarantees a defendant carrier the right to a jury.

B. The Communications Act's Judicial-Review Scheme Does Not Satisfy The Seventh Amendment.

The court of appeals nonetheless held that "there is no Seventh Amendment problem here"—a holding that the government defends in its pending *AT&T* petition. App., *infra*, 35a; *AT&T* Pet. 7. The court found the Seventh Amendment satisfied "because Verizon could have gotten" a jury trial by refusing to comply with the FCC's forfeiture order, defaulting on that final agency order, and then waiting to see whether the Department of Justice would bring a collection suit in district court where Verizon could demand a jury trial. App., *infra*, 35a; *see id.* at 40a

("[W]e conclude that, assuming Verizon has a Seventh Amendment right to a trial by jury, those rights were not violated because [Verizon] had, but chose to forgo, an opportunity for a § 504(a) trial."). That Section 504 process does not comply with the Seventh Amendment's demands.

1. The FCC forfeiture proceeding here was itself a "suit at common law" requiring a jury.

The Seventh Amendment entitled Verizon to plead its case to a jury *before* the FCC entered its forfeiture order, not to possibly do so long after the fact. Like the in-house SEC "enforcement action" at issue in *Jarkesy*, 603 U.S. at 115, the FCC forfeiture proceeding here was one "in which legal rights were to be ascertained and determined," *Parsons*, 28 U.S. at 447 (Story, J.). The FCC forfeiture action itself was therefore in substance a "[s]uit[] at common law" in which Verizon had the right to demand a jury. U.S. Const., amend. VII. Requiring Verizon to "defend [itself] before the agency rather than before a jury" was thus a denial of Verizon's Seventh Amendment rights. *Jarkesy*, 603 U.S. at 115.

a. "Those who founded our Nation considered the right to trial by jury a fundamental part of their birthright." *Thomas* v. *Humboldt County*, 607 U.S. ___ (2025) (slip op. 2) (Gorsuch, J., respecting the denial of certiorari). To that generation, a collection of "sensible and upright jurymen, chosen by lot from among those of the middle rank" and "not appointed till the hour of trial," were thought "the best investigators of truth." Blackstone 380; *see* The Federalist No. 83, pp. 500-501 (C. Rossiter ed. 1961) (A. Ham-

ilton). The jury also served a more overtly political function: it "provide[d] the common citizen with a sympathetic forum in suits against the government." Charles W. Wolfram, *The Constitutional History of the Seventh Amendment*, 57 Minn. L. Rev 639, 708 (1973). As one prominent Antifederalist put it, juries were a bulwark against "lordly" adjudicators more often inclined "to protect the officers of government" than rule for the "weak and helpless citizen." *Essay of a Democratic Federalist* (Oct. 17, 1787), *in* 3 The Complete Anti-Federalist 61 (Herbert Storing ed. 1981). Others extolled the jury as an important check on "unwise legislative and administrative policies." Wolfram, 57 Minn. L. Rev. at 705.

Despite its advantages, few claimed that the jury should decide *all* civil disputes; it was "well known" to the Framers that "in courts of equity and admiralty" in both England and the colonies, "juries d[id] not intervene." *Parsons*, 28 U.S. at 446. But the Framers enshrined in the Seventh Amendment what they "regarded as the normal and preferable mode of disposing of issues of fact in civil cases," *Dimick*, 293 U.S. at 485-486, preserving that procedure "inviolate[]" "against the passing demands of expediency or convenience." *Reid* v. *Covert*, 354 U.S. 1, 10 (1957).

Thus, "it has long been settled that the right extends beyond the common-law forms of action recognized at that time." *Curtis* v. *Loether*, 415 U.S. 189, 193 (1974). As Justice Story explained in *Parsons*, the Seventh Amendment "embrace[s] all suits which are not of equity and admiralty jurisdiction, *whatever may be the peculiar form which they may assume to settle legal rights*." 28 U.S. at 447 (emphasis added).

b. An FCC in-house forfeiture proceeding to enforce Section 222 is one such "peculiar form" of settling legal rights. Exercising authority conferred on it by statute, the Commission "*determine[s]*" whether a carrier has "willfully or repeatedly failed to comply with" its duty to reasonably safeguard customer data. 47 U.S.C. § 503(b)(1) (emphasis added). The Commission "*determine[s]*" whether the carrier is "liable to the United States for a forfeiture penalty." *Ibid.* (emphasis added). And the Commission "*determine[s]*" the "amount of [that] forfeiture penalty," *id.* § 503(b)(2) (emphasis added), which is then immediately "payable into the Treasury," *id.* § 504(a). An FCC forfeiture action is therefore "in its basic character a suit to determine and adjudicate" "traditional common-law issues": whether the carrier has breached a legal duty and, if so, "the amount" it is "obligated to pay." *Simler* v. *Conner*, 372 U.S. 221, 223 (1963).

Under this Court's cases going back to *Parsons*, Congress cannot "conjure away the Seventh Amendment by mandating that [such] traditional legal claims" be resolved by an "administrative tribunal." *Granfinanciera, S.A.* v. *Nordberg*, 492 U.S. 33, 52 (1989); *see Jarkesy*, 603 U.S. at 134 (what "matters is the substance of the action, not where Congress has assigned it"); *Knickerbocker Ins. Co. of Chicago* v. *Comstock*, 83 U.S. 258, 269 (1872) (Seventh Amendment reaches legal actions regardless of "the particular form of procedure which may be adopted"). Before a suit at common law reaches its conclusion, the "aid of juries is not only deemed appropriate but is required by the Constitution itself." *Granfinanciera*, 492 U.S. at 51 (citation omitted). Precluding Ver-

izon from invoking the "aid" of a jury during the FCC forfeiture proceeding itself thus violated Verizon's Seventh Amendment rights.

2. The possibility of a separate Section 504 collection action does not cure the Seventh Amendment violation.

In rejecting that conclusion, the Second Circuit (echoed by the government in its pending petition) characterized the FCC's in-house adjudication as merely an "initial decision" that lacks any Seventh Amendment significance. *AT&T* Pet. 11; *see* App., *infra*, 36a, 126a n.270. The court of appeals reasoned that an "FCC[] forfeiture order . . . does not, by itself, compel payment." App., *infra*, 36a. Instead, the court noted, pointing to Section 504, "the government needs to initiate a collection action to do that." *Ibid.* The court thus concluded that the FCC proceedings that occur "before a § 504(a) trial create no Seventh Amendment injury." *Ibid.* That is wrong for at least three reasons.

a. First, an FCC forfeiture proceeding and a subsequent DOJ collection action are two *different* "[s]uits at common law," U.S. Const., amend. VII—not one elongated action. The Seventh Amendment, by its plain terms, requires that a jury also be available in the initial, rights-determining suit.

Again, a forfeiture proceeding before the FCC is a distinct legal action in its own right: the "Commission" "determine[s]" legal rights and obligations "in accordance with" certain required procedures. 47 U.S.C. § 503(b)(1). That adjudication results in a final order determining that the carrier is "liable to the United States." *Id.* § 503(b)(1). A subsequent

Section 504 proceeding is an entirely distinct "civil suit," "instituted" "in the name of the United States" to collect the debt it is now owed. *Id.* § 504. That suit is "prosecute[d]" by a different entity (the relevant U.S. attorney) in a different forum (federal court). *Id.* § 504(a). The two suits even have different limitations periods: FCC forfeiture proceedings may reach conduct going back only one year, *id.* § 503(b)(6), whereas Section 504 actions may be brought within five years of the unpaid forfeiture order, 28 U.S.C. § 2462.

To be sure, the Section 504 collection action would be necessary to force a carrier to pay the FCC's final penalty, if a carrier ever chose delinquency. But the possibility that DOJ might need to serve as an enforcement arm does not somehow convert the FCC's order into a meaningless suggestion, as the Second Circuit effectively held. An FCC order is still a final and binding "order of the Commission" that carries the force of law and is reviewable in the courts of appeals. 47 U.S.C. § 402(a); *see* 28 U.S.C. § 2342(1).

The order against Verizon is a perfect example. It concludes with the following language, standard in FCC forfeiture orders:

> **IT IS ORDERED** that . . . Verizon Communications **IS LIABLE FOR A MONETARY FORFEITURE** in the amount of [$46,901,250] for willfully and repeatedly violating section 222 of the [Communications] Act. . . . Payment of the forfeiture shall be made . . . within thirty (30) calendar days.

App., *infra*, 138a-139a. That language could not be any plainer that it "compel[s] payment," even if the Communications Act also provides for a collection proceeding when a regulated party fails to pay. *Id.* at 36a.

In short, by the time any Section 504 collection suit is filed, an organ of the federal government will have "already found the facts," "adjudged guilt, and levied punishment" without a jury. *AT&T*, 149 F.4th at 503. The "possibility of a back-end [S]ection 504 trial" up to five years later does not avoid the Seventh Amendment violation. *Ibid.*

b. Second, even assuming that the "opportunity for a § 504(a) trial" satisfies Verizon's right to a jury, App., *infra*, 40a, the Communications Act does not actually *guarantee* that "opportunity" to carriers at all. Carriers have no statutory entitlement to appeal an adverse FCC forfeiture order to an Article III court in which a jury is available. The most that a carrier can do is defy the order and bait the government into starting a new collection action. Even then, a carrier's access to a jury is still entirely in the hands of the Department of Justice. Nothing requires the government to file a Section 504 collection suit. And if the government opts not to bring such an action within the five-year limitations period, no jury is ever made available. True enough, the carrier then avoids paying—but it misses the chance to wipe away an adjudication of liability in a classic suit at common law.

c. Third, at a minimum, forcing a carrier to sacrifice its only chance at guaranteed judicial review of an FCC forfeiture order, just to preserve the possibility of a jury trial, is an impermissible burden and "undue obstruction of the right to a jury trial." *In re Peter-*

son, 253 U.S. 300, 310 (1920); *cf. United States* v. *Jackson*, 390 U.S. 570, 581, 583 (1968) (statute that permitted application of the death penalty "only to those defendants who assert the right to contest their guilt before a jury" "impose[d] an impermissible burden upon the assertion of a constitutional right").

Paying an FCC-mandated forfeiture, rather than waiting for a Section 504 collection suit that may never come, is a carrier's only means of guaranteeing judicial review of the FCC's order. In the real world, carriers never pass up that surefire path to judicial review because unpaid FCC forfeiture orders have significant "real-world impacts." *AT&T*, 149 F.4th at 503. The FCC's public determination of wrongdoing can harm a carrier's "reputation." *FCC* v. *Fox Television Stations, Inc.*, 567 U.S. 239, 256 (2012). Carriers must account for unpaid orders on their books, include them in securities filings, and disclose them in applications for government contracts. FCC forfeiture orders may even have claim- or issue-preclusive effect in subsequent court proceedings. *See B & B Hardware, Inc.* v. *Hargis Indus., Inc.*, 575 U.S. 138, 149 (2015).

Before the Commission itself, an unpaid forfeiture order can also have serious collateral consequences. For one thing, the FCC "has the statutory power to take into account 'any history of prior offenses' when setting the level of a forfeiture penalty" for future violations of the Communications Act. *Fox*, 567 U.S. at 255 (quoting 47 U.S.C. § 503(b)(2)(E)). At least as significantly, carriers are repeat players that must constantly appear before the Commission to procure or transfer required licenses, obtain the necessary approval for mergers, and so on. Carriers know that

the Commission will take into account their refusal to pay a forfeiture in these proceedings. Indeed, the Commission forthrightly claims the power to "us[e] the underlying facts of a prior violation" against a party in license or merger proceedings. App., *infra*, 37a (quoting *Commission's Forfeiture Pol'y Statement & Amend. of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, 12 FCC Rcd. 17087, 17103 (1997)). To the extent carriers dispute those facts (or dispute that they amount to a "violation"), they have no real choice but to pay the penalty and challenge the FCC's conclusions on appeal. Waiting around for the chance at a jury is the least appealing of a decidedly "unappetizing menu of options." *Sackett* v. *EPA*, 598 U.S. 651, 671 (2023).

Although the Second Circuit "share[d] Verizon's concerns regarding these 'real-world impacts,'" the court "fail[ed] to see how they implicate the Seventh Amendment." App., *infra*, 37a. That is hard to understand. The real-world impacts of flouting an order to pay a penalty to the government are the costs that carriers must bear if they want even a chance of pleading their case to a jury—the very right that is supposed to be "preserved" to them by the Seventh Amendment. U.S. Const., amend. VII. In the circumstances here, those costs create an impermissible burden on the Seventh Amendment right.

The court of appeals also suggested that only immediate financial harms, not "reputational and practical harms," trigger the Amendment's protection. App., *infra*, 37a. The court thus appeared to believe that a jury is required only just before a defendant may be legally (but not practically) forced to cut a check. But the Framers intended the Seventh

Amendment to protect against all injuries that flow from a jury-less adjudication of an action at law. That is why the Seventh Amendment guarantees a jury to both plaintiffs and defendants, even though plaintiffs are generally in no danger of being ordered to pay money. And that is why parties are constitutionally entitled to a jury in all kinds of cases having nothing to do with property—including cases solely concerning intangible, reputational harms. *See, e.g.*, *Southwick* v. *Stevens*, 10 Johns. 443, 446 (N.Y. Sup. Ct. 1813) ("It was for the jury to determine how far the ridicule of the plaintiff . . . prejudice[d] him in the eyes of the public.").

3. The FCC judicial-review scheme finds no support in this Court's precedents.

This Court has never signed off on the penalty-now-trial-later approach to the Seventh Amendment embodied in the FCC's forfeiture scheme. That "lack of historical precedent" is itself a "telling indication of the severe constitutional problem" here. *Free Enterprise Fund* v. *PCAOB*, 561 U.S. 477, 505 (2010) (citation omitted). The court of appeals and the government have nevertheless identified two decisions that they claim establish the constitutionality of the FCC forfeiture scheme. *See AT&T* Pet. 9; App., *infra*, 36a-37a. Properly understood, neither does.

First, in *Capital Traction Co.* v. *Hof*, 174 U.S. 1 (1899), this Court upheld a statute that authorized justices of the peace to enter initial judgment in suits at law involving small debts, without initial use of a jury. But *Hof* upheld the statute only because it gave "*either party*" the "right to appeal" the initial judgment "to a court of record, *and to have a trial by jury*

in that court." *Id.* at 45 (emphasis added). The Court explained that the Seventh Amendment "does not prescribe at what stage of an action a trial by jury must, if demanded, be had," so long as the opportunity to invoke that right within that single case is at least "preserved through an appeal." *Id.* at 23, 25.

The FCC's penalty system, which allows for the imposition of $47 million in penalties (and far higher ones), bears no resemblance to *Hof*'s system for adjudicating "small debts." 174 U.S. at 18, 28. Moreover, unlike in *Hof*, the statutory scheme here confers no *right* to appeal an FCC forfeiture order to a federal court "and to have a trial by jury in that court." *Id.* at 45. Instead, the appeal right is strictly circumscribed to petitions for review in a court of appeals, without a jury or full review of facts. 47 U.S.C. § 402(a), (g); 5 U.S.C. § 706(2). By contrast, to access a jury, a carrier must defy the FCC's order and wait to be sued by the United States in a separate matter, all while suffering serious collateral consequences. And even then, the Department of Justice holds the only set of keys to the courtroom. None of that is consistent with a carrier's Seventh Amendment right to "have [its] case decided by a jury before it is finally settled." *Hof*, 174 U.S. at 30.

The government also relies on *Meeker* v. *Lehigh Valley Railroad Co.*, 236 U.S. 412 (1915). *AT&T* Pet. 8. The government claims that *Meeker* upheld against a Seventh Amendment challenge "a statute that empowered the Interstate Commerce Commission (ICC) to make an initial award of damages" so long as the statute "allowed the carrier to demand a jury trial when the injured party sued . . . to collect the damages." *Ibid.*

That is an unsupportable reading of *Meeker*—which is perhaps why neither of the courts of appeals to side with the government has invoked it. In fact, *Meeker*'s Seventh Amendment ruling had nothing to do with whether the ICC could constitutionally adjudicate the relevant dispute without providing a jury, or whether providing a jury in a back-end enforcement suit was sufficient protection for defendants. Those questions never came up. Instead, as the Fifth Circuit explained in *AT&T*, this Court addressed only the constitutionality of a specific "provision treating the ICC's initial factfinding as a 'rebuttable presumption.'" 149 F.4th at 502 n.15 (quoting *Meeker*, 236 U.S. at 430). The challenger railroad had argued that the Seventh Amendment forbade Congress from imposing that presumption. *Meeker* rejected that argument, explaining that the presumption was "merely a rule of evidence" that took no ultimate "question of fact from either court or jury." 236 U.S. at 430 (citing "many other state and Federal enactments establishing other rebuttable presumptions"). The Court accordingly had no need to decide whether "the railroad had a jury right in the action" in the first place. *AT&T*, 149 F.4th at 502 n.15.

This Court's subsequent decision in *Peterson*, 253 U.S. at 300, is instructive on the reach of both *Meeker* and *Hof*. In *Peterson*, a federal district court appointed an "auditor" to "form a judgment and express an opinion upon such of the items as he found to be in dispute," and his report was then "admitted at the trial before the jury as prima facie evidence" on those factual issues. *Id.* at 306. The Court found no Seventh Amendment problem with that procedure. Citing *Hof*, the Court noted that "delay in reaching

the jury trial," standing alone, does not "infringe the constitutional right." *Id.* at 310. And citing *Meeker*, the Court held that it is not "unconstitutional" to "endow[] an official act or finding with a presumption of regularity or of verity." *Id.* at 311. But what *would* have been unconstitutional, Justice Brandeis explained, was allowing the auditor to "finally determine any of the issues in th[e] action." *Id.* at 307 (citation omitted). The Seventh Amendment ensures that "enjoyment of the right of trial by jury be not obstructed, and that the ultimate determination of issues of fact by the jury be not interfered with." *Id.* at 310. Because the FCC's forfeiture scheme obstructs and interferes with that protection, it cannot be squared with the Seventh Amendment.

II. THE DECISION BELOW WARRANTS REVIEW.

The court of appeals' decision warrants this Court's review. There is now an acknowledged, clear 2-1 split on the question presented. The answer to that question will have significant practical ramifications for how the FCC enforces federal communications law. And the decision here substantially weakens a right with "so firm a place in our history" that, as the Court reiterated just two Terms ago, "any seeming curtailment" of that right must be "scrutinized with the utmost care." *Jarkesy*, 603 U.S. at 121 (quoting *Dimick*, 293 U.S. at 486). The Court should grant both the petition here and the government's petition in *AT&T* (No. 25-406) and consolidate them for argument.

A. The Courts Of Appeals Are Divided On The Question Presented.

The decision below deepens a textbook circuit split. In holding that the FCC's judicial-review scheme satisfies the Seventh Amendment, the Second Circuit sided with the D.C. Circuit in *Sprint Corp.* v. *FCC*, 151 F.4th 347 (D.C. Cir. 2025)—decided just a month beforehand—and against the Fifth Circuit in *AT&T*. The Second Circuit's opinion acknowledged the division, App., *infra*, 34a, 36a, as does the government's petition for certiorari in *AT&T* (at 16-17).

The lower courts' decisions in *Verizon*, *AT&T*, and *Sprint* arise out of closely related FCC enforcement proceedings concerning each defendant carrier's handling of customer-location data. Each decision addressed the same argument raised by the carriers: whether the FCC violated the Seventh Amendment by adjudicating, in-house and without a jury, the Commission's claim for monetary penalties based on failure to reasonably protect certain customer data.

In *AT&T*, as discussed above, the Fifth Circuit ruled for the carrier. Relying on this Court's decision in *Jarkesy*, the court explained that the FCC proceedings violated the Seventh Amendment because (i) monetary penalties are an "archetypal common law remedy" and (ii) an action to recover such penalties for failing to safeguard customer data is "closely analogous to a negligence action" at common law. 149 F.4th at 499. The court then rejected the FCC's argument—adopted by the Second Circuit here—that the "possibility of a back-end section 504 trial" gave AT&T "everything promised by the Seventh Amendment." *Id.* at 503.

The D.C. Circuit in *Sprint* squarely disagreed. Like the Second Circuit here, the court declined to decide whether the Seventh Amendment applies, reasoning that Section 504 already "allowed the Carriers to obtain a jury trial before suffering any legal consequences." *Sprint*, 151 F.4th at 359. The court observed that if the FCC never sought to enforce its order, the carriers "would not be required to pay a dime." *Id.* at 361. Because the carriers "chose to pay their fines" rather than hold out for a collection action, they could not later "complain that they were denied a right" that the court found protected by Section 504. *Id.* at 360. The D.C. Circuit acknowledged the Fifth Circuit's contrary decision in *AT&T* but found it "unconvinc[ing]." *Id.* at 361.

B. The Question Presented Is Important.

The question presented is undeniably important. The Second Circuit's decision permits the FCC to adjudicate classic legal disputes without guaranteeing to defendants the right most "prized by the American colonists." *Jarkesy*, 603 U.S. at 121. This Court's intervention is necessary to protect that right and to cabin a sweeping expansion of administrative power.

The question also carries significant policy consequences. As the government's petition in *AT&T* notes, the FCC's authority to impose forfeiture penalties is a "frequently used" tool in the Commission's enforcement toolbox and one of its "most important regulatory remedies." *AT&T* Pet. 17. The availability of the jury-trial right is particularly important in disputes concerning carriers' protection of customer data. In our increasingly connected age, such disputes have taken on a greater significance, as the FCC's

sweeping enforcement program against many major telecommunications carriers demonstrates.

Under the Second Circuit's approach, the Commission may unilaterally adjudicate and impose punitive monetary penalties across vast swaths of the communications industry—all without an Article III court or jury. And the FCC claims truly sweeping penal power. For example, it asserts that its authority to punish any "willful[] or repeated[]" violation of its rules, 47 U.S.C. § 503(b)(1)(B), affords it the discretion to treat each instance of a customer's data breach as a separate offense. In its order here, the agency insisted that Verizon's practices "placed the sensitive location information of *all* its customers at unreasonable risk," and accordingly the Commission "could well have chosen to look to the total number of Verizon subscribers when determining the number of violations." App., *infra*, 116a. That approach, the agency explained, "would have resulted in significantly higher forfeiture than what was proposed." *Id.* at 117a. By the agency's own math, it could have ordered a final penalty of up to $236 *trillion*, or seven times the current GDP of the United States. *See* Verizon, 2018 Annual Report 2, https://www.verizon.com/about/sites/default/files/2018-Verizon-Annual-Report.pdf (reporting 118 million wireless retail connections). Even the supposedly conservative method the FCC ultimately adopted—treating each of the 63 participants in Verizon's program as a separate, continuing violation, assessed daily until their access to customer data ended—produced a hefty $47 million forfeiture.

The question presented in this case and in *AT&T* thus arises in a particularly stark financial context. In *Jarkesy*, the SEC order at issue levied a penalty of

$300,000. 603 U.S. at 119. By contrast, the forfeiture orders against Verizon, AT&T, Sprint, and other carriers for violating Section 222 total roughly $200 million. And that $200 million is, in the FCC's view, an act of benevolence: nothing prevents the agency from imposing exponentially larger penalties in future cases. These are huge sums of money that cannot be left in legal limbo, with carriers stuck between (1) paying up and forgoing any possibility of a jury trial, or (2) defying a federal agency's final order and seeing whether the hammer drops, all while facing the real-world consequences of owing an unpaid debt to the United States and having been found in violation of the law.

C. The Court Should Grant Review In Both This Case And *AT&T*.

As noted, the government has already asked this Court to resolve the clear 2-1 split on a constitutional issue of surpassing importance. *See AT&T* Pet. 15. Although Verizon obviously disagrees with the merits arguments in the government's petition in *AT&T*, the government's other arguments in support of certiorari are correct and are equally applicable here.

To the extent the Court is inclined to grant the government's petition, Verizon respectfully submits that granting and consolidating both cases would be appropriate. That is the Court's typical practice when receiving petitions for certiorari from separate lower-court decisions presenting the same question. *See, e.g.*, *Fuld* v. *Palestine Liberation Organization*, 606 U.S. 1 (2025) (consolidated with *United States* v. *Palestine Liberation Organization*, No. 24-151); *Brown* v. *United States*, 602 U.S. 101 (2024) (consolidated

with *Jackson* v. *United States*, No. 22-6640); *Campos-Chaves* v. *Garland*, 602 U.S. 447 (2024) (consolidated with *Garland* v. *Singh*, No. 22-884). And granting both cases would also avoid any potential vehicle problems that could arise from circuit-specific law about the scope of legal defenses in Section 504 trials. As the government's petition in *AT&T* explains (at 14-15), the Fifth Circuit has held that defendants in such trials may contest only the agency's factual findings, *see United States* v. *Stevens*, 691 F.3d 620, 622 (5th Cir. 2012), whereas the Second Circuit below held that defendants may raise both factual and legal challenges, *see* App., *infra*, 38a-39a. Granting both petitions would ensure that the Court can resolve the constitutional question regardless of Section 504's scope.

Consolidation would be particularly appropriate here because both *AT&T* and *Verizon* have been closely linked since their inception. Both cases began with contemporaneous FCC investigations prompted by the same *New York Times* article. The Commission issued notices of apparent liability the same day in both investigations. Each forfeiture proceeding then culminated in a final administrative order—also handed down on the same day—that each carrier had violated Section 222 and was required to pay a massive penalty. Both AT&T and Verizon complied with their respective FCC orders to guarantee immediate review in the courts of appeals, which reached divergent Seventh Amendment conclusions in opinions issued within weeks of each another.

For all those reasons, this Court should grant review in both cases and consolidate them. For efficiency's sake—including to reduce both cases to a single

set of briefs—it should also realign AT&T as petitioner alongside Verizon in the consolidated cases.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

SCOTT H. ANGSTREICH
AASEESH P. POLAVARAPU
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street NW
Suite 400
Washington, DC 20036

JEFFREY B. WALL
Counsel of Record
MORGAN L. RATNER
DANIEL A. MEJIA-CRUZ
SULLIVAN & CROMWELL LLP
1700 New York Avenue NW
Suite 700
Washington, DC 20006
(202) 956-7660
wallj@sullcrom.com

MAXWELL F. GOTTSCHALL
SULLIVAN & CROMWELL LLP
125 Broad Street
New York, NY 10004

Counsel for Verizon Communications Inc.

NOVEMBER 6, 2025

APPENDIX

APPENDIX

TABLE OF CONTENTS

Page

Appendix A — Court of appeals opinion (Sept. 10, 2025) 1a

Appendix B — FCC order (Apr. 29, 2024) 41a

Appendix C — Constitutional, statutory, and regulatory provisions:

U.S. Const., amend. VII 152a
47 U.S.C. § 222 ..... 152a
47 U.S.C. § 503 ..... 158a
47 U.S.C. § 504 ..... 166a
47 C.F.R. § 1.80 ..... 167a
47 C.F.R. § 64.2010 ..... 176a

APPENDIX A

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

No. 24-1733

VERIZON COMMUNICATIONS INC.,
Petitioner,

v.

FEDERAL COMMUNICATIONS COMMISSION, UNITED STATES OF AMERICA,
Respondents.[*]

Argued: April 29, 2005

Decided: September 10, 2025

Before LYNCH, LEE, and NATHAN, *Circuit Judges*.

NATHAN, *Circuit Judge*:

In the wake of news reporting about Verizon Communications Inc.'s (Verizon) mishandling of its customers' location data, the Federal Communications Commission (FCC or the Commission) commenced an enforcement action against the company. Exercising its authority to pursue monetary forfeitures, *see* 47 U.S.C. § 503(b)(1)(B), (b)(4), the Commission preliminarily concluded that Verizon violated § 222 of the

[*] The Clerk of Court is respectfully directed to amend the caption as set forth above.

Communications Act and § 64.2010 of the agency's regulations.[1] After considering Verizon's responses, the FCC subsequently affirmed its findings, imposing a $46.9 million penalty due to Verizon's failure to reasonably safeguard a category of statutorily protected information known as "customer proprietary network information."

Before this Court, Verizon challenges the forfeiture order on various grounds. Verizon first argues that the customer location data it was found to have mishandled is not statutorily protected because it does not satisfy the definition of customer proprietary network information. *See id.* § 222(h)(1)(A). It also contests the liability finding as arbitrary and capricious and the forfeiture amount as violative of the statutory penalty cap. *See id.* § 503(b)(2)(B). Finally, Verizon contends that the FCC's forfeiture proceedings deprived the company of a jury trial in an Article III forum and so infringed its Seventh Amendment rights.

We disagree. The customer data at issue plainly qualifies as customer proprietary network information, triggering the Communication Act's privacy protections. And the forfeiture order both soundly imposed

---

[1] The FCC's findings in the Notice of Apparent Liability are preliminary. *See Verizon Commc'ns*, 35 FCC Rcd. 1698, 1699 (2020) ("In this Notice of Apparent Liability, we *propose* a penalty of $48,318,750 against Verizon . . . for *apparently* violating section 222 of the Communications Act and the Commission's regulations[.]" (emphasis added)). In the forfeiture order that the FCC later issued, it confirmed the bulk of the agency's prior findings, concluding, after Verizon was given an opportunity to respond, that it "f[ound] no reason to cancel or withdraw the proposed penalty." *In re Verizon Commc'ns*, No. 24-41, 2024 WL 1905229, at *1 (F.C.C. Apr. 29, 2024).

liability and remained within the strictures of the penalty cap. Nothing about the Commission's proceedings, moreover, transgressed the Seventh Amendment's jury trial guarantee. Indeed, Verizon had, and chose to forgo, the opportunity for a jury trial in federal court. Thus, we DENY Verizon's petition.

BACKGROUND

I. Legal Background

The Communications Act of 1934, 47 U.S.C. §§ 151 *et seq.*, empowers the FCC "to regulate all interstate and foreign communication by wire or radio and all persons engaged within the United States in such communication." *N.Y. State Telecomms. Ass'n, Inc. v. James*, 101 F.4th 135, 140 (2d Cir. 2024) (quotation marks omitted).

When Congress amended the Communications Act in 1996, it created a new framework to govern the protection and use of the information that telecommunications carriers obtain by virtue of providing such a service. Telecommunications Act of 1996, Pub. L. No. 104-104, § 222, 110 Stat. 56, 148-49. Under that framework, enshrined in § 222, carriers have "a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and *customers*[.]" 47 U.S.C. § 222(a) (emphasis added).

One such form of protected customer data is customer proprietary network information. This category of information is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a

telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." *Id.* § 222(h)(1)(A). By statute, a carrier "shall only use, disclose, or permit access to individually identifiable customer proprietary network information" to provide "the telecommunications service from which such information is derived" or "services necessary to, or used in" providing that service "[e]xcept as required by law or *with the approval of the customer*." *Id.* § 222(c)(1) (emphasis added).

The FCC has issued regulations implementing § 222's requirements. Carriers must "take reasonable measures to discover and protect against attempts to gain unauthorized access to [customer proprietary network information]." 47 C.F.R. § 64.2010(a). Carriers must also generally obtain the "opt-in approval" of their customers before disclosing such information. *Id.* § 64.2007(b).[2]

Congress authorized the FCC to enforce § 222 and the agency's rules through monetary forfeitures. *See* 47 U.S.C. § 503(b)(1)(B). Section 503(b) of the Communications Act provides two routes by which the Commission may pursue such a forfeiture. *See AT&T Corp. v. Fed. Commc'ns Comm'n*, 323 F.3d 1081, 1083 (D.C. Cir. 2003). Under § 503(b)(3), the FCC may initiate a formal adjudication before an administrative law judge (ALJ) or the Commission itself. 47 U.S.C.

---

[2] Opt-in approval "requires that the carrier obtain from the customer affirmative, express consent allowing the requested [customer proprietary network information] usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request." 47 C.F.R. § 64.2003(k).

§ 503(b)(3)(A). Any resulting forfeiture order is reviewable in a court of appeals. *Id.* "If the penalty remains unpaid once the forfeiture determination becomes final, the United States may bring a collection action in district court." *AT&T Corp.*, 323 F.3d at 1083 (citing 47 U.S.C. § 503(b)(3)(B)).

Alternatively, under § 503(b)(4), the FCC may, as it did here, follow a more informal procedure. Under that procedure, the Commission issues a Notice of Apparent Liability and gives the alleged violator an opportunity to respond in writing. 47 U.S.C. § 503(b)(4)(A)-(C). After considering the response, the FCC decides whether to affirm the notice, and if so, issues a forfeiture order. *See* 47 C.F.R. § 1.80(g)(4). At that point, the carrier has two options for judicial review, depending on whether it opts to timely pay the penalty. If the carrier declines to pay the ordered forfeiture amount, the Commission may refer the matter to the Department of Justice to commence a collection action in federal district court, where the carrier is entitled to a "trial de novo." 47 U.S.C. § 504(a). We refer to this proceeding as a § 504(a) trial. If, however, the carrier chooses to pay the forfeiture amount, it may seek review in the appropriate court of appeals pursuant to 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1). *See AT&T Corp.*, 323 F.3d at 1084-85; *ABC, Inc. v. Fed. Commc'ns Comm'n*, 404 F. App'x 530, 534 (2d Cir. 2011), *vacated and remanded on other grounds sub nom.*, *Fed. Commc'ns Comm'n v. Fox Television Stations, Inc.*, 567 U.S. 239, 132 S.Ct. 2307, 183 L.Ed.2d 234 (2012).[3]

---

[3] This is the first time in a published opinion that we have stated that, as long as the carrier pays the forfeiture amount, courts of

II. Factual Background

Petitioner Verizon provides its customers with mobile-voice and data services through its wireless network. To enable a customer to make and receive calls and to transmit data, customers' devices and a carrier's cell towers must regularly exchange information, which we refer to as "pinging" each other. Because carriers know the locations of their towers, and because customers typically carry their phones on their person or nearby, carriers like Verizon generally know their customers' location at all times.

Until March 2019, Verizon, like many other carriers, ran a "location-based services" program that sold access to certain kinds of wireless customer location data. As part of that program, Verizon contracted with "location information aggregators," which collected customer data and resold it to third-party location-based services providers. Verizon had arrangements with two aggregators, LocationSmart and Zumigo, which in turn contracted with 63 third-party entities.[4] These entities purportedly used customer location data for six specific types of purposes or "[u]se [c]ases": "call

---

appeals have jurisdiction to review a forfeiture order issued pursuant to § 503(b)(4). The parties do not dispute that Verizon's payment of the forfeiture amount preserves our jurisdiction to review the FCC's forfeiture order. In any event, we find that, for the reasons articulated by the D.C. Circuit in *AT&T Corp.*, 323 F.3d at 1084-85, we have jurisdiction to review Verizon's appeal.

[4] Early on, the forfeiture order suggests that 65 third-party entities joined the location-based services program. But Verizon clarified that two of these companies did not actually participate despite being approved to do so.

routing, roadside assistance, proximity marketing, transportation and logistics, fraud mitigation/ identity management, and mobile gaming/lottery." *In re Verizon Commc'ns*, No. 24-41, 2024 WL 1905229, at *4 (F.C.C. Apr. 29, 2024) (quotation marks omitted).

Verizon did not itself provide notice and obtain or verify consent to access customer location data. Rather, it largely delegated those functions via contract. Verizon's contracts with the aggregators, for example, required that location-based services providers give notice and seek affirmative, opt-in consent before accessing customer information. And prior to joining the program, providers had to submit an application describing the company's intended use case and its notice-and-consent process. To verify that customers were indeed consenting to disclosure of their data, Verizon relied primarily on an external auditor, Aegis Mobile, LLC, which collected and matched customer location requests and consent events on a daily basis.[5] Both sets of records were submitted to Aegis by the aggregators, who in turn collected them from the third-party providers. If a contracting party failed to meet Verizon's standards, Verizon could cut off access to customer location data at any time.

On May 10, 2018, the *New York Times* published an article reporting security breaches involving Verizon's (and other major carriers') location-based services program. According to the *New York Times*, a company called Securus Technologies, Inc. (Securus) was misusing the program to enable law enforcement officers to

[5] Verizon's monitoring efforts purportedly had additional components as well, such as regular audits.

access location data *without* customers' knowledge or consent, so long as the officers uploaded a warrant or some other legal authorization. But, as Verizon concedes, Securus had been approved for a different use case altogether. And because Securus did not actually review the documents that law enforcement personnel uploaded, a now-former Missouri sheriff, Cory Hutcheson, was able to access customer data with no legal process at all. Instead of providing warrants or other legal authorization, Hutcheson uploaded utterly irrelevant materials, such as "his health insurance policy, his auto insurance policy, and pages selected from Sheriff training materials." *Verizon Commc'ns*, 2024 WL 1905229, at *5 (quotation marks omitted).

The day after the *New York Times* article, Verizon terminated access to customer location data for both Securus and 3Cinteractive, the intermediary that had supplied Securus with the data by way of a contract with aggregator LocationSmart. Verizon also stopped approving any new participants or use cases. A month later, Verizon announced its intention to terminate the location-based services program altogether. But it did not stop selling customer location data to most (57) of its providers and the aggregator Zumigo until some six months later. And LocationSmart, together with four roadside-assistance providers, retained access to customer location data into 2019. In the meantime, the program continued to operate more or less as it always had.

Soon after the *New York Times* article, the FCC's Enforcement Bureau launched an investigation into Verizon's location-based services program. And in

February 2020, the Commission issued Verizon a Notice of Apparent Liability for its apparent violations of § 222 of the Communications Act and § 64.2010 of the agency's regulations by failing to protect its customers' proprietary network information. After considering Verizon's responses, the Commission affirmed the notice and issued a forfeiture order.

In that order, the FCC concluded that the location data disclosed through Verizon's location-based services program is protected as customer proprietary network information under § 222. And it found that Verizon failed to reasonably protect that information both before and after the Securus/Hutcheson disclosures. Basing its penalty on Verizon's post-disclosure conduct, the Commission determined that Verizon engaged in 63 continuing violations of § 222 and its implementing regulations: one for each ongoing relationship with an aggregator or location-based services provider that retained access to customer data more than 30 days after publication of the *New York Times* article.[6] It also applied a 50% upward adjustment on top of the base forfeiture amount for, among other things, "egregious" conduct, and it rejected Verizon's constitutional challenges to the forfeiture order. In the end, Verizon was directed to pay $46.9 million within 30 days of the order.

---

[6] The FCC's original calculation of the forfeiture included two companies which, as explained above, *see supra* [App. 6a] n.4, never participated in the location-based services program. But upon Verizon's clarification, the FCC exercised its discretion to exclude these two entities and reduce the forfeiture amount accordingly.

Verizon paid the penalty and filed a timely petition for review in this Court pursuant to 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1).

STANDARD OF REVIEW

Under the Administrative Procedure Act (APA), we will generally overturn agency action only if it is "arbitrary, capricious, an abuse of discretion," or otherwise contrary to law. 5 U.S.C. § 706(2).

We review constitutional questions and matters of statutory interpretation *de novo*. *See Cablevision Sys. Corp. v. Fed. Commc'ns Comm'n*, 570 F.3d 83, 91 (2d Cir. 2009); *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 394, 144 S.Ct. 2244, 219 L.Ed.2d 832 (2024). "An agency's factual findings must be supported by substantial evidence, which means such relevant evidence as a reasonable mind might accept as adequate to support a conclusion." *Cablevision Sys. Corp.*, 570 F.3d at 91 (quotation marks omitted).

DISCUSSION

Verizon raises a number of challenges to the FCC's forfeiture order in its petition for review. On the statutory side of things, Verizon argues that § 222 does not cover the customer location data at issue in this case, that the FCC's liability finding was arbitrary and capricious, and that the penalty exceeds the statutory cap. Verizon also brings a constitutional challenge, asserting that the imposition of the forfeiture, without a jury trial, violates its Seventh Amendment rights. On all of these challenges, the FCC has the better of the arguments.

I. SCOPE OF § 222

Verizon's first challenge to the forfeiture order concerns the scope of § 222 of the Communications Act. On Verizon's theory, customer proprietary network information essentially covers only customers' *call*-location data, not their *device*-location data. And since its location-based services program sold only device-location information, Verizon argues that § 222 does not apply. We are not persuaded.

Section 222(h)(1)(A) defines customer proprietary network information as including "*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*." 47 U.S.C. § 222(h)(1)(A) (emphasis added). Thus, to qualify as customer proprietary network information, customer location data must meet two conditions. First, the information must "relate[ ] to the . . . location . . . of a telecommunications service." *Id.*[7] And second, the

[7] One of Verizon's amici, CTIA – The Wireless Association (CTIA), but not Verizon, argues that the statute is best read to define customer proprietary network information as that which "relates to the . . . location . . . *of use* of a telecommunications service." 47 U.S.C. § 222(h)(1)(A) (emphasis added). Pursuant to the rule of the last antecedent, however, "a limiting . . . 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, 136 S.Ct. 958, 194 L.Ed.2d 48 (2016) (quotation marks omitted). Although the rule is not absolute and can be overcome by context, *id.*, the context here supports rather than undermines the application of the rule. Reading

information must be "made available to the carrier . . . solely by virtue of the carrier-customer relationship." *Id.* Device-location data comfortably satisfies both conditions.

Starting with the first prong of the analysis, both parties agree that Verizon's wireless-voice services are telecommunications services within the meaning of the statute. *See* 47 U.S.C. § 153(53). Verizon contends, however, that the location information does not reveal the location of telecommunications services, because "Verizon did not need to wait for a customer to be on a call" to obtain that information. Pet. Br. at 33. Rather, Verizon could ping a device owned by a customer who was not using or did not purchase any voice service

---

the phrase "of use" as modifying each category of enumerated information, as opposed to just the word "amount," would create unnecessary anomalies. For example, it would make little sense to read § 222(h)(1)(A) to refer to the "technical configuration . . . of use of a telecommunications service." 47 U.S.C. § 222(h)(1)(A). More-over, if we were to adopt CTIA's preferred construction, there would be no principled distinction between the statute's references to "quantity of use" and "amount of use," rendering one of those phrases surplusage. *See Quantity*, BLACK'S LAW DICTIONARY (12th ed. 2024) (defining "quantity" as "[t]he amount of something measurable"). By contrast, if "of use" only modifies "amount," we can more readily interpret "quantity . . . of a telecommunications service" as referring to, for example, how many phone lines a customer has purchased, and "amount of use" of such a service as referring to, for example, the number and length of that customer's calls. Since "we construe statutes to avoid surplusage," *Perez v. Westchester Cnty. Dep't of Corr.*, 587 F.3d 143, 155 (2d Cir. 2009), the better reading of § 222(h)(1)(A) is that, to qualify as customer proprietary network information, the information must "relate[ ] to the . . . location . . . of a telecommunications service," not to the "location . . . of use" of such a service. 47 U.S.C. § 222(h)(1)(A).

(e.g., a customer who had a data-only plan, which is not a telecommunications service under the statute, *see infra* [App. 13a] & n.9). For this reason, Verizon claims, the location-based services program "relates to" "only the location of a device, not of a telecommunications service." *Id.*

Verizon is mistaken. As explained above, a wireless carrier "must be aware of and use [a] device's location in order for it to enable customers to send and receive calls." *Verizon Commc'ns*, 2024 WL 1905229, at *8 (quotation marks omitted). Thus, customers' devices and Verizon's cell towers regularly communicate to "ensur[e] that [customers] can receive incoming calls and place outgoing calls." *Id.* at *9. That is true *whether a customer is on a call or not*, since the device must continuously maintain a connection to the carrier's network for any incoming call to be received. Accordingly, the device-location data of customers to whom Verizon is providing voice services clearly relates to the location where they are receiving the voice service. And so, it "relates to the . . . location . . . of a telecommunications service." 47 U.S.C. § 222(h)(1)(A).[8]

---

[8] We would reach the same conclusion even if we construed "of use" to modify all terms in the statutory definition of customer proprietary network information, *see supra* [App. 10a-11a] n.7, since, as the Commission reasoned, "[w]hen customers' devices are exchanging communications with Verizon's network, and thereby ensuring that they can receive incoming calls and place outgoing calls," they are clearly "using the [telecommunications] service to which they have subscribed, even outside the moments in time when they are engaged in calls." *Verizon Commc'ns*, 2024 WL 1905229, at *9.

Verizon suggests that this argument "ignores the record," because to generate the location information that Verizon sold through its location-based services program, the company had to "specially ping" a customer's wireless device, "separately from the normal course network communications" with that device. Reply Br. at 14 (quotation marks omitted). But nothing about this special pinging takes the device-location information at issue here outside the purview of the statute. Verizon's program collected the same data, using the same technological infrastructure, as that used to approximate the location of a customer's device to enable voice services, rendering it "related to" the location of a telecommunications service. *See Mizrahi v. Gonzales*, 492 F.3d 156, 159 (2d Cir. 2007) ("Congress's use of the phrase 'relating to' in federal legislation generally signals its expansive intent.").[9] Plus, it would be perverse to grant greater statutory privacy protection to device-location data collected only for use by Verizon than to the same data collected for disclosure to third parties. And it is well-settled that "[c]ourts should interpret statutes to avoid absurd results." *In re Nine W. LBO Sec. Litig.*, 87 F.4th 130, 145 (2d Cir. 2023).

Verizon also draws on statutory context and legislative history to support its theory that § 222(h)(1)(A) embraces only call-location information. But its

---

[9] For the same reason, and for reasons explained more fully below, *see infra* [App. 16a-18a], we reject the argument, to the extent that Verizon makes it, that for data-only customers, the device-location at issue in this case is not "related to" a telecommunications service because the provision of data services is not a telecommunications service under the statute.

arguments are inconclusive at best and, in any event, cannot override the statute's plain meaning.

By way of background, when Congress enacted the Telecommunications Act in 1996, "location" was not included in the definition of customer proprietary network information. That was added in 1999, along with other amendments to § 222, via the Wireless Communications and Public Safety Act, Pub. L. No. 106-81, § 5(3), 113 Stat. 1286, 1289 (1999). As part of those amendments, Congress crafted a new exception to § 222(c)(1)'s prohibition on the nonconsensual use, disclosure, or access to customer proprietary network information. This exception allows carriers to disclose "call location information," without customer consent, to various emergency services providers and to family members in an emergency involving a risk of death or serious physical harm. 47 U.S.C. § 222(d)(4). Congress also clarified that, in the context of "call location information," consent for purposes of § 222(c)(1) means "express prior authorization." *Id.* § 222(f)(1).

Citing to the 1999 amendments and their legislative history, Verizon argues that these provisions show that Congress intended "location" in the definition of customer propriety network information to capture "call location information." Pet. Br. at 34 (quotation marks omitted). And it maintains that embracing the contrary interpretation would lead to nonsensical results, since it would mean that (1) Verizon may, without consent, disclose call-location information to emergency service providers or immediate family in a life-threatening emergency, but *not* device-location information, and (2) only "express prior authorization" counts as

consent for call-location information, but lesser forms of consent (e.g., a failure to opt out) could suffice for disclosing device-location information.

Even assuming that those results reflect contrary assumptions about the sensitivity of device-location data, Verizon's arguments about congressional intent just as easily cut in the other direction. "Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion," *Russello v. United States*, 464 U.S. 16, 23, 104 S.Ct. 296, 78 L.Ed.2d 17 (1983) (cleaned up), and the "negative implications raised by disparate provisions are strongest" when those provisions "were being considered simultaneously," *Lindh v. Murphy*, 521 U.S. 320, 330, 117 S.Ct. 2059, 138 L.Ed.2d 481 (1997). Had Congress wished to limit § 222's scope to call-location information, it could have used a term like "call location" in § 222(h)(1)(A)—just as it did in the other amended provisions—instead of affording protection more broadly to all "information that relates to the . . . location" of a service. 47 U.S.C. § 222(h)(1)(A). In any event, "[i]t is axiomatic that the plain meaning of a statute controls its interpretation." *Lee v. Bankers Tr. Co.*, 166 F.3d 540, 544 (1999). And since device-location data plainly "relates to the . . . location . . . of a telecommunications service," as § 222(h)(1)(A) requires, that alone is enough to defeat Verizon's remaining arguments about congressional intent. 47 U.S.C. § 222(h)(1)(A).

As for the second prong of the § 222(h)(1)(A) analysis, Verizon contends that device-location data is not customer proprietary network information because it is not obtained "solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1)(A). This argument is a close cousin of its first, since its effect would be to limit the definition of customer proprietary network information to data concerning voice plans. But once again, Verizon misses the mark.

The Communications Act subjects communications services "to different regulatory regimes depending on how they are classified." *N.Y. State Telecomms. Ass'n*, 101 F.4th at 140. Entities providing "telecommunications services" are regulated as common carriers under Title II of the Act. 47 U.S.C. § 153(51). By contrast, "information services" are exempt from common-carrier status. *See Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 975, 125 S.Ct. 2688, 162 L.Ed.2d 820 (2005) ("The Act regulates telecommunications carriers, but not information-service providers, as common carriers."). A parallel framework applies to mobile service providers: while entities that provide "commercial mobile services" are treated as common carriers, 47 U.S.C. § 332(c)(1)(A), those that offer "private mobile services" are not, *id.* § 332(c)(2). *See also*, *e.g.*, *Petitions for Declaratory Ruling on Regul. Status of Wireless Messaging Serv.*, 33 FCC Rcd. 12075, 12076-77 (2018) (discussing these parallel frameworks).

Against this backdrop, the crux of Verizon's argument is that the location data at issue here is not made available "solely by virtue of the carrier-customer

relationship" because Verizon can obtain it even if a customer is not using or has not purchased the sole common-carrier service that Verizon provides: its mobile-voice services. 47 U.S.C. § 222(h)(1)(A); *see also id.* §§ 153(51), 332(c)(1)(A). Indeed, as we have already explained, that data can be obtained from customers using Verizon's data services, which are classified as non-common-carrier services.[10]

This argument fails. Verizon provides wireless-voice services to its customers because they have chosen Verizon to be their provider of that voice service—in other words, they have a carrier-customer relationship. Verizon's voice customers, in turn, provide their device-location data to Verizon solely to use the services they purchase from it. Indeed, Verizon's voice services *require* this information to operate. As such, the carrier-customer relationship is the "sole[ ]" reason that Verizon's voice customers provide location data to Verizon. 47 U.S.C. § 222(h)(1)(A).

---

[10] Verizon's wireless data services—text messaging and Internet access—are presently regulated as non-common-carrier information services and private mobile services. *See Petitions for Declaratory Ruling on Regul. Status of Wireless Messaging Serv.*, 33 FCC Rcd. at 12082, 12090-94 (text messaging); *Restoring Internet Freedom*, 33 FCC Rcd. 311, 312, 322-34 (2018) (broadband Internet access). Although the FCC sought to reclassify broadband Internet access in 2024, *see Safeguarding & Securing the Open Internet Restoring Internet Freedom*, No. 24-52, 2024 WL 2109860, at *3-4 (F.C.C. May 7, 2024), the Sixth Circuit set aside the order earlier this year, *see In re MCP No. 185*, 124 F.4th 993, 1001, 1013 (6th Cir. 2025). *See also N.Y. State Telecomms. Ass'n*, 101 F.4th at 140-41 (discussing the prior reclassifications of broadband Internet access and its regulatory consequences).

The core problem with Verizon's argument is that it assumes that the scope of the "carrier-customer relationship" in § 222(h)(1)(A) is limited to its common-carrier services. Not so. At the outset, the "solely by virtue of" language does not ask whether the carrier obtained the customer proprietary network information solely through its *telecommunications service* (or its commercial mobile service). Instead, by its terms, it asks whether the carrier obtained the information through "the carrier-customer *relationship*." *Id.* (emphasis added). That relationship may encompass multiple services, such as information services. Indeed, where carriers sell voice and data services as part of a bundle, all those services are fairly encompassed within the carrier-customer relationship.

To be sure, the Communications Act treats regulated parties as common carriers only to the extent that they provide common-carrier services. *See id.* § 153(51) (stipulating that a party "shall be treated as a common carrier . . . only to the extent that it is engaged in providing telecommunications services"); *id.* § 332(c)(1)(A) (same "insofar as such person is . . . engaged" in providing a commercial mobile service); *see also Fed. Trade Comm'n v. AT&T Mobility LLC*, 883 F.3d 848, 860 (9th Cir. 2018) ("[A] company may be an interstate common carrier in some instances but not in others, depending on the nature of the activity which is subject to scrutiny." (quotation marks omitted)). But nothing in those provisions constrains the scope of the "carrier-customer relationship" in § 222(h)(1)(A). Section 222(h)(1)(A) uses the terms "carrier" and "customer" to identify the relevant parties via their

relationship to one another, not to cabin that relationship to common-carrier services.

In sum, we conclude that device-location data both "relates to the . . . location . . . of a telecommunications service" and is obtained "solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1)(A). It thus qualifies as customer proprietary network information and triggers the privacy protections set forth in § 222 of the Communications Act.

II. LIABILITY FINDING

In the alternative, Verizon contends that the FCC's determination that Verizon did not reasonably protect customers' location data was arbitrary and capricious. "However, an agency's decision is arbitrary and capricious only if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise." *Safe Haven Home Care, Inc. v. U.S. Dep't of Health & Hum. Servs.*, 130 F.4th 305, 323 (2d Cir. 2025) (cleaned up). That was not the case here.

Section 503(b) provides that a person shall be liable for forfeiture for "willfully or repeatedly fail[ing] to comply with any of the provisions of" the Communications Act or rules promulgated by the FCC. 47 U.S.C. § 503(b)(1)(B).[11] In the forfeiture order, the FCC

[11] For obligations under the Communications Act, "'willful', when used with reference to the commission or omission of any act,

determined that Verizon failed to reasonably protect customer proprietary network information before and after the Securus/Hutcheson disclosures, thereby violating § 222 and § 64.2010 of the agency's rules.

Verizon's challenge to this determination stems from its view that the Securus/Hutcheson disclosures were outlier occurrences that affected a small number of customers and do not speak to any broader systemic issues in its safeguards. Thus, Verizon argues, instead of reasonable measures, the FCC required perfect ones, imposing, without fair notice, a strict liability standard "contrary to the reasonableness standard" in the FCC rule. Pet. Br. at 40 (quotation marks omitted). At bottom, Verizon asks us to find that it was arbitrary and capricious for the FCC to refuse to infer the reasonableness of Verizon's safeguards based on the fact that only the Securus/Hutcheson breaches were publicly identified. But the Commission "reasonably considered the relevant issues and reasonably explained the decision" to reject that position. *Fed. Commc'ns Comm'n v. Prometheus Radio Project*, 592 U.S. 414, 423, 141 S.Ct. 1150, 209 L.Ed.2d 287 (2021).

As to the period before the Securus/Hutcheson disclosures, the FCC considered the safeguards that Verizon had in place and reasonably found them wanting. In reaching this decision, the agency explained that Verizon relied heavily on a chain of contractual arrangements to satisfy its statutory and regulatory obligations. And it observed that, to enforce its

---

means the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision" or FCC rule. 47 U.S.C. § 312(f)(l).

contractual safeguards, Verizon's efforts "apparently mainly consisted of analysis of unverified vendor-created consent records" (through Aegis). *Verizon Commc'ns*, 2024 WL 1905229, at *16 (quotation marks omitted). Specifically, Aegis's review consisted essentially of comparing the list of "location requests" provided by a location-based services provider with the list of purported "consent records" *also provided by the provider*, a system that "assumed that the location requests and consent records provided by the [providers] would be legitimate in the first instance" and could not detect if a provider fabricated the consent records. *Verizon Commc'ns*, 35 FCC Rcd. 1698, 1719 (2020). A 2017 internal report, which warned Verizon that "it is possible for [providers] with delegated consent to falsify consent records and obtain [Verizon] subscriber data without their consent," shows that the company was on notice of this possibility. *Verizon Commc'ns*, 2024 WL 1905229, at *4 (quotation marks omitted) (second alteration in original).

The FCC also emphasized that although allegedly designed to monitor customer consents, Verizon's system was incapable of detecting customers' lack of consent, since the Securus location requests expressly sought to obtain customer location data without customers' approval. This was, in the agency's view, a "significant loophole." *Id.* at *17. Verizon complains that its failure to identify the 11 customers whose data was improperly accessed by Hutcheson "hardly shows" the existence of any "significant loophole" in its

procedures. Pet. Br. at 5.[12] But even if the unauthorized disclosures themselves were not so numerous, it was appropriate for the FCC to consider, in assessing the reasonableness of Verizon's safeguards, that the Securus/Hutcheson requests did not raise *any* red flags despite the fact that they were submitting the opposite of consent records to a system whose central conceit was obtaining customer consent.

The FCC examined the relevant factors and spelled out a reasonable basis to support its conclusion: it considered the full gamut of Verizon's safeguards and found that Verizon lacked a reliable means to enforce compliance with its contractual safeguards. That is sufficient on review for arbitrary and capriciousness. *See Prometheus Radio Project*, 592 U.S. at 423, 141 S.Ct. 1150 (noting that "a court may not substitute its own policy judgment for that of the agency" on arbitrary and capricious review).

Second, and more importantly, as to Verizon's response to the Securus/Hutcheson breaches, Verizon again reiterates the measures it took in the wake of the *New York Times* article. But the FCC reasonably

---

[12] The FCC's briefing relies on numbers that seem to refer to disclosures *across carriers*. The Notice of Apparent Liability indicated that "at least 20 Verizon customers' location information was disclosed to Hutcheson, via Securus, without the customers' consent." *Verizon Commc'ns*, 35 FCC Rcd. at 1714. In response, Verizon argued that the evidence on which the FCC relied did not support that contention. The forfeiture order does not appear to reiterate the original number. But, consistent with Verizon's position, the record suggests that, although Hutcheson/ Securus may have made some 20 requests, the data of only 11 Verizon customers was improperly accessed.

found those measures to be insufficient as well. As the Commission observed, the breaches put Verizon on notice that the third parties' contractual promise to limit the use of location data alone failed to prevent its unauthorized use. And yet, Verizon continued to sell its customers' location data under effectively "the *same system*" to 58 entities for over six months and to another five for over 10 months. *Verizon Commc'ns*, 2024 WL 1905229, at *18.

The FCC acknowledged that Verizon immediately cut off 3Cinteractive and Securus, declined to allow access to location information for additional providers and use cases, and had Aegis review the vetting procedures and data analytics used. That said, the FCC observed that Verizon implemented only certain changes, requiring Aegis to "strengthen the trans-action verification process to identify any anomalies in the data relating to consent requests that could indicate a potential issue, such as multiple location requests within a 24-hour period or an increase in location requests that were out of the ordinary" for a particular location-based services provider. *Id.* at *19 (quotation marks omitted). And it explained that nothing in the record indicated that "those particular measures were likely to have identified the problem that enabled the Securus and Hutcheson breaches in the first place," including the failure to verify the validity of customer consent. *Id.*

The Commission identified "numerous steps that could have been taken to squarely address the proven vulnerability," including steps short of terminating the program. *Id.* These steps included immediately

suspending the access of LocationSmart, which was contractually obligated to monitor Securus and 3Cinteractive's access to Verizon customer data; meaningfully investigating whether the Securus incident was an isolated occurrence or indicative of a broader problem;[13] directly verifying customer consent; and, if Verizon determined it could not reasonably safeguard the customer location data that it sold access to, terminating the program. Thus, once again, the agency "considered the evidence, examined the relevant factors, and spelled out a satisfactory rationale for its action." *Env't Def. v. U.S. Env't Prot. Agency*, 369 F.3d 193, 201 (2d Cir. 2004).

Verizon's remaining arguments are unavailing. The FCC's decision to provide a 30-day "grace period," during which Verizon could have fixed the problems it identified or terminated the program without facing penalties, in no way belies its assertions regarding the seriousness of the flaws in Verizon's program. And the FCC order neither suggests that the only reasonable response would have been for Verizon to terminate the program within 30 days of learning of the *New York Times* article, nor otherwise imposes an "effective strict liability regime." Pet. Br. at 40. So Verizon cannot complain of lack of fair notice on either front.

---

[13] Verizon claims to have investigated the other service providers, and that neither it nor its third-party auditor identified any other service provider that improperly accessed customer location information. But it "fail[ed] to provide any details about the scope or strength of that investigation." *Verizon Commc'ns*, 35 FCC Rcd. at 1722.

Accordingly, we find that the FCC's liability finding was not arbitrary and capricious.

III. FORFEITURE AMOUNT

Verizon next asserts that the forfeiture order violates the Communication Act's statutory limit on forfeiture penalties. We disagree.

In authorizing the FCC to assess forfeitures, Congress set maximum forfeiture amounts. As applic-able here, the Communications Act caps the total per-violation forfeiture amount at approximately $200,000 for "each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed" approximately $2 million, as adjusted for inflation, "for any single act or failure to act" that violates the statute or FCC rules. 47 U.S.C. § 503(b)(2)(B); *see also* 47 C.F.R. § 1.80(b)(2), (b)(9)(ii) (2020); *Amend. of Section 1.80(b) of the Comm'n's Rules Adjustment of Civ. Monetary Penalties to Reflect Inflation*, 34 FCC Rcd. 12824, 12828 (2019). Thus, for any given continuing violation, the Act authorizes the FCC to impose a penalty of up to $200,000 for each successive day, so long as the aggregate penalty for any "single act or failure to act" does not exceed $2 million. 47 U.S.C. § 503(b)(2)(B); *Amend. of Section 1.80(b) of the Comm'n's Rules Adjustment of Civ. Monetary Penalties to Reflect Inflation*, 34 FCC Rcd. at 12828. In determining the amount of the forfeiture penalty, the FCC must consider "the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other

matters as justice may require." 47 U.S.C. § 503(b)(2)(E).

As previewed above, the FCC found that Verizon "engaged in [63] continuing violations—one for each ongoing relationship with a third-party . . . provider or aggregator that had access to Verizon customer location information more than 30 days after publication of the *New York Times* report—and that each violation continued until Verizon terminated the corresponding entity's access to customer location information." *Verizon Commc'ns*, 2024 WL 1905229, at *22. In challenging this result, Verizon and its amici contend that the FCC's findings support at most a "single act or failure to act" warranting a forfeiture: that, in maintaining "one set" of flawed policies, it "failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information." Pet. Br. at 42 (quotation marks omitted). In its view, the maximum forfeiture penalty the FCC could impose was about $2 million, *not* nearly $47 million.

At the outset, the parties disagree as to the applicable standard of review. Verizon and its amici suggest that, after *Loper Bright*, we must assess this matter *de novo*, because whether Verizon's failure to take reasonable protective measures constitutes a "single act or failure to act" or many acts or failures to act is a question of statutory interpretation. Pet. Br. at 42 (quoting 47 U.S.C. § 503(b)(2)(B)). The FCC, on the other hand, maintains that arbitrary-and-capricious review governs.

Rather than defer to an agency's interpretation of a statute, "courts must exercise independent judgment in determining the meaning of statutory provisions." *Loper Bright*, 603 U.S. at 394, 144 S.Ct. 2244. Of course, "[i]n a case involving an agency . . . the statute's meaning may well be that the agency is authorized to exercise a degree of discretion." *Id.* "When the best reading of a statute is that it delegates discretionary authority to an agency, the role of the reviewing court under the APA is, as always, to independently interpret the statute and effectuate the will of Congress subject to constitutional limits[,] . . . ensuring the agency has engaged in reasoned decisionmaking within [the] boundaries [of the authority delegated to it]." *Id.* at 395, 144 S.Ct. 2244 (quotation marks omitted).

Here, although Verizon and its amici are correct that determining Verizon's total number of violations involves a question of statutory interpretation, they misidentify the relevant question. The Communications Act does not specifically articulate what qualifies as a "single act or failure to act." Rather, the Act gives the Commission "the discretion" to determine when to issue a forfeiture penalty against a carrier. 47 U.S.C. § 503(b)(3)(A). And when the Commission does issue a penalty, the Act gives the Commission the discretion, within a statutory cap, to determine its amount. *Id.* § 503(b)(2)(B), (E). It also empowers the Commission to determine when someone has "willfully or repeatedly failed to comply with [the Communications Act]." *Id.* § 503(b)(1)(B). Those delegations of authority make sense in the context of the FCC's remedial scheme: because the agency is close to the facts, it is best positioned to determine what, under any given set of

circumstances, qualifies as a single violation. So the relevant statutory interpretation question is whether, under the Communications Act, the FCC has the discretion to determine, within reasonable "boundaries," *Loper Bright*, 603 U.S. at 395, 144 S.Ct. 2244, when a carrier has engaged in a single violation of the Act. Because the Communications Act explicitly grants the Commission the discretion to determine what qualifies as a violation of the Act, when to issue a forfeiture penalty for violations, and what the size of that forfeiture penalty would be, we conclude, on *de novo* review, that the agency has the authority to determine, within reasonable boundaries, what qualifies as a "single act or failure to act," for the purpose of remaining within the statutory cap. 47 U.S.C. § 503(b)(2)(B). In short, we are not deferring to the agency's interpretation of the statute. Instead, we conclude—based on our own independent analysis of the statute—that the Communications Act vests the agency with some discretion to select, from a reason-able range of possibilities, the unit of prosecution that can be considered a single violation of the Act under particular circumstances.

Still, that conclusion does not resolve whether the FCC's determination that Verizon committed 63 continuing violations is unlawful. As we have explained, when a statute "delegates discretionary authority to an agency," the role of the court, in addition to interpreting the statute, is to ensure that "the agency has engaged in reasoned decisionmaking" within the boundaries of the authority Congress has delegated to it. *Loper Bright*, 603 U.S. at 395, 144 S.Ct. 2244 (quotation marks omitted). We conclude that the FCC acted within those boundaries when it determined that

Verizon committed 63 continuing violations of the Communications Act.

Verizon may have had one overarching set of flawed policies, which insufficiently protected customer proprietary network information, but those policies were implemented through separate relationships with 63 different entities. Verizon approved and terminated each entity's participation separately. In the weeks following the Securus/Hutcheson disclosures, it had the choice of shoring up its demonstrably flawed safeguards or else cutting off access not just for Securus and 3Cinteractive but also for any one of the other entities that continued to receive customer location data without adequate safeguards. Its failure to take either of these paths means that each of its on-going relationships represented an additional risk of security breaches. That is enough to render Verizon's decision to continue selling location data to 63 entities under essentially the same system that produced the Securus/Hutcheson disclosures 63 individual "act[s] or failure[s] to act." 47 U.S.C. § 503(b)(2)(B). Thus, consistent with the FCC's conclusion, Verizon committed 63 continuing violations of § 222 of the Communications Act and § 64.2010 of the FCC's rules.

Verizon and its amici complain that the FCC's interpretation of the statute leads to absurd results. But it's Verizon's approach that makes little sense. In the course of securing customers' data, a regulated party will make many decisions, which will in turn have various ramifications on any number of sub-decisions and any number of potential victims. As we have explained, Verizon made a series of decisions that had various

consequences. For example: Verizon relied on a chain of contractual arrangements to satisfy its statutory and regulatory obligations, rather than satisfying those obligations directly itself. It insufficiently validated customer consent records and did not have a system in place that could detect a lack of customer consent. And it took few additional measures after the Securus/ Hutcheson breach to remedy the shortcomings in its data protection systems. *See supra* [App. 19a-23a]. Considering that set of circumstances, we have little trouble concluding that the FCC acted within the boundaries of the discretion that Congress delegated to it when it concluded that Verizon committed 63 continuing violations.

Moreover, the purpose of the FCC's forfeiture penalties is to meaningfully deter and punish violations of the statute. Indeed, in setting the forfeiture amount, the FCC must consider several factors that "concern culpability, deterrence, and recidivism," *Sec. & Exch. Comm'n v. Jarkesy*, 603 U.S. 109, 123-24, 144 S.Ct. 2117, 219 L.Ed.2d 650 (2024), such as the "gravity of the violation," "the degree of culpability," and "any history of prior offenses," 47 U.S.C § 503(b)(2)(E). Forfeitures are also "payable into the Treasury of the United States," which further confirms their deterrent and punitive, as opposed to remedial, function. *Id.* § 504(a). Section 503's legislative history supports this conclusion as well. *See Commission's Forfeiture Pol'y Statement & Amend. of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines (Forfeiture Pol'y Statement)*, 12 FCC Rcd. 17087, 17097 (1997). And yet, interpreting the statutory cap to insulate systemic privacy failures from anything more than a single capped

penalty would do little to deter or punish telecommunications giants like Verizon, even with the maximum, approximately $2 million penalty. Given that Congress directed the Commission to consider a violator's "ability to pay" in calculating the forfeiture amount, 47 U.S.C. § 503(b)(2)(E), we doubt that it intended such a result.[14]

Verizon and its amici's complaints of absurdity stem largely from the FCC's claim that the agency's approach was not only lawful but also "eminently *conservative*," as it could have chosen to calculate the number of violations based on "the total number of Verizon subscribers"—"tens of millions"—"whose highly sensitive location information was made vulnerable by Verizon." *Verizon Commc'ns*, 2024 WL 1905229, at *26. But the legality of this methodology is not before us. And, in any event, finding in favor of the FCC here does not mean countenancing the imposition of a penalty in the hundreds of trillions.

To the extent amici also rely on *United States v. WIYN Radio, Inc.*, 614 F.2d 495 (5th Cir. 1980), that decision does not bind our Court. But even if it did, the FCC's interpretation does not run counter to its holding. Indeed, that case focuses on the distinction between single and continuing violations and does not address when or whether the FCC might impose penalties for various continuing violations. *See id.* at 497

---

[14] While the FCC also claims that its interpretation is "[c]onsistent with established practice" of treating "systemic privacy failings as 'significantly more than a single violation,'" it points to a single non-final decision in support of that position. Resp. Br. at 45 (citing *In re TerraCom, Inc.*, 29 FCC Rcd. 13325, 13343 ¶ 50 (2014)).

(holding that a licensee's failure to provide the required notice of a personal attack on a broadcast was not a repeated violation for which successive daily penalties could be exacted because the rule at issue imposed a "single, pointed duty" that "admitt[ed] of only a single dereliction" once the week-long period to give notice elapsed). Thus, we find that the FCC acted within the limits of its authority when it determined that Verizon engaged in 63 separate failures to implement a reasonable data-security regime in violation of § 222 of the Communications Act and § 64.2010 of the FCC's rules.

Finally, we conclude that Verizon forfeited on appeal any challenge to the FCC's upward adjustment of the forfeiture order amount. Before the Commission, Verizon brought a second objection to the size of the penalty imposed. It argued that the agency's 50% upward adjustment on top of the base forfeiture amount was unwarranted. *See Verizon Commc'ns*, 2024 WL 1905229, at *23. But "we rely on the parties to frame the issues for decision" on appeal. *United States v. Sineneng-Smith*, 590 U.S. 371, 375, 140 S.Ct. 1575, 206 L.Ed.2d 866 (2020) (quoting *Greenlaw v. United States*, 554 U.S. 237, 243, 128 S.Ct. 2559, 171 L.Ed.2d 399 (2008)). And an appellant—or petitioner —who fails to raise an argument in his opening brief generally "forfeits" that argument. *Tripathy v. McKoy*, 103 F.4th 106, 118 (2d Cir. 2024).

Verizon did not mention the upward adjustment in its opening or reply briefs before this Court, and it did not raise any challenge to the upward adjustment at oral argument. Even after we ordered supplemental

briefing about the upward adjustment, Verizon did not explain *why* it had failed to raise the issue beforehand. It only tacitly conceded that failure. *See* Pet. Supp. Br. at 1 (claiming the upward adjustment furnishes "*another reason*" why the Commission's forfeiture order is "unlawful" (emphasis added)). Verizon has therefore forfeited any challenge to the upward adjustment here. Although we may consider a forfeited issue if it is "purely legal" or if "necessary to avoid a manifest injustice," neither discretionary exception counsels a different result. *See Readco, Inc. v. Marine Midland Bank*, 81 F.3d 295, 302 (2d Cir. 1996).

While we note that the D.C. Circuit considered and rejected other carriers' similar challenges to their large penalty amounts, *see Sprint Corp. v. Fed. Commc'ns Comm'n*, No. 24-1224, ––– F.4th –––, –––, 2025 WL 2371009, at *15 (D.C. Cir. Aug. 15, 2025), those challenges were affirmatively raised before that court, *see* Pet. Br. at 67-69, *Sprint Corp.*, 2025 WL 2371009, (No. 24-1224), 2024 WL 5097079, at *67-69. We thus decline to reach Verizon's here.

IV. SEVENTH AMENDMENT

Verizon and its amici lastly contend that the FCC's decision to levy a forfeiture by way of its § 503(b)(4) enforcement procedures violated Verizon's Seventh Amendment rights. Even assuming for the sake of argument that the Seventh Amendment applies in this context, we determine that Verizon waived its right to a jury trial.

The Seventh Amendment provides that, "[i]n 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. Verizon and its amici's arguments that the FCC violated this constitutional mandate rest on the Supreme Court's recent decision in *Securities & Exchange Commission v. Jarkesy*. There, the Court held that the Securities and Exchange Commission (SEC) could not, consistent with the Seventh Amendment, adjudicate securities fraud claims seeking civil penalties "in-house" before an ALJ "rather than before a jury in federal court." *See Jarkesy*, 603 U.S. at 115, 144 S.Ct. 2117. "The Seventh Amendment," the Court explained, "extends to a particular statutory claim if the claim is 'legal in nature,'" which requires examining the cause of action and the remedy it provides. *Id.* at 122-23, 144 S.Ct. 2117 (quoting *Granfinanciera, S.A. v. Nordberg*, 492 U.S. 33, 53, 109 S.Ct. 2782, 106 L.Ed.2d 26 (1989)). And, the Court found, because the SEC's action in *Jarkesy* was "legal in nature," it required a jury trial. *Id.* at 126, 144 S.Ct. 2117.

We may assume for the sake of argument that Verizon has a Seventh Amendment right to trial by jury on the charges here. Nevertheless, there is no Seventh Amendment problem here, because Verizon could have gotten such a trial. The remedial structure of the Communications Act differs significantly from the securities statutes that the Supreme Court considered in *Jarkesy*. *See* 603 U.S. at 115-18, 144 S.Ct. 2117 (explaining the remedial structure imposed by the three securities fraud statutes that were relevant to the disposition of the case). When the FCC imposes a forfeiture under § 503(b)(4) of the Communications Act, the statute directs that the penalty "shall be recoverable pursuant to Section 504(a)." 47 U.S.C. § 503(b)(4). And

§ 504(a), in turn, requires the government to enforce any penalty in a "trial de novo" in federal district court. *Id.* § 504(a). Thus, Verizon could have declined to pay the forfeiture and preserved its opportunity for a *de novo* jury trial if the government sought to collect. Instead, it chose to pretermit any § 504(a) enforcement action and seek immediate review in our Court. *Cf. Westchester Day Sch. v. Vill. of Mamaroneck*, 504 F.3d 338, 356 (2d Cir. 2007) (discussing the waiver of the jury-trial right).

Verizon and its amici protest that the prospect of a § 504(a) trial does not satisfy the Seventh Amendment's demands because by the time of trial, "the Commission would have already adjudged a carrier guilty of violating section 222 and levied fines." *AT&T, Inc. v. Fed. Commc'ns Comm'n*, No. 24-60223, ––– F.4th ––– –, ––––, 2025 WL 2426855, at *9 (5th Cir. Aug. 22, 2025). That argument is misplaced. Verizon essentially complains that, whereas, after *Jarkesy*, the SEC must file a civil complaint in federal district court to seek civil penalties for securities fraud, the FCC will begin a § 504(a) trial not with allegations of wrongdoing, but with a determination of liability. But the problem in *Jarkesy* was that the SEC could "siphon" its securities fraud claims away from Article III courts and compel payment without a jury trial. 603 U.S. at 135, 144 S.Ct. 2117. The FCC's forfeiture order, however, does not, by itself, compel payment. The government needs to initiate a collection action to do that. *See* 47 U.S.C. §§ 503(b)(4), 504(a). Against this backdrop, the agency's proceedings before a § 504(a) trial create no Seventh Amendment injury. *Cf. Cap. Traction Co. v. Hof*, 174 U.S. 1, 4, 45-46, 19 S.Ct. 580, 43 L.Ed. 873 (1899)

(holding that an initial tribunal may lawfully enter judgment without a full jury trial if the law permits a subsequent "trial [anew] by jury, at the request of either party, in the appellate court").

Verizon and its amici also assert that a § 504(a) trial falls short of the Seventh Amendment's guarantee because Verizon would have needed to wait up to five years for the FCC to bring a collection action, during which time Verizon would suffer reputational and practical harms. *See* 28 U.S.C. § 2462 (establishing a five-year statute of limitations). Verizon emphasizes, for example, that under FCC policy, the agency may "us[e] the underlying facts of a prior violation that shows a pattern of non-complaint behavior against a licensee in a subsequent renewal, forfeiture, transfer, or other proceeding." *Forfeiture Pol'y Statement*, 12 FCC Rcd. at 17103. While we share Verizon's concerns regarding these "real-world impacts," *AT&T*, ––– F.4th at –––, 2025 WL 2426855, at *9, we fail to see how they implicate the Seventh Amendment, which requires a jury trial only upon an effort to collect payment of monetary damages, *see Jarkesy*, 603 U.S. at 123, 144 S.Ct. 2117.[15] In fact, if the FCC had instituted § 503(b)(4) proceedings, issued a Notice of Apparent Liability, and ultimately chosen to admonish Verizon instead of imposing a forfeiture, Verizon would equally experience collateral consequences. But, crucially, the civil penalties—the thing that *Jarkesy* tells us is most important for

[15] To the extent Verizon's complaints might implicate due process or some other constitutional matter, Verizon has waived such claims by failing to raise them in its brief. *See JP Morgan Chase Bank v. Altos Hornos de Mexico, S.A. de C.V.*, 412 F.3d 418, 428 (2d Cir. 2005).

assessing whether the Seventh Amendment applies—would not exist. And ultimately, if the government declined to pursue the collection action within five years, Verizon would be under no obligation to pay and would suffer no Seventh Amendment injury.

Verizon and its amici's final challenge to the constitutional sufficiency of a § 504(a) trial concerns the scope of the trial itself. Relying primarily on the Fifth Circuit's decision in *United States v. Stevens*, Verizon objects that defendants in § 504(a) trials cannot challenge the FCC's legal interpretations or raise constitutional challenges. 691 F.3d 620, 622-24 (5th Cir. 2012). In brief, that is not the law of this Circuit. For one, we think that § 504(a) "says what it means and means what it says." *Oklahoma v. Castro-Huerta*, 597 U.S. 629, 642, 142 S.Ct. 2486, 213 L.Ed.2d 847 (2022) (quotation marks omitted). Textually speaking, "trial de novo" plainly indicates that the parties would start afresh in federal court, and consequently that Verizon would be able to challenge both the factual and legal bases of the FCC's forfeiture order. 47 U.S.C. § 504(a). Indeed, a "trial de novo" means "[a] new trial on the entire case—that is, on both questions of fact and issues of law—conducted as if there had been no trial in the first instance." *Trial de novo*, BLACK'S LAW DICTIONARY (12th ed. 2024). In any given trial, the parties can raise questions of law by debating what should be included in the jury instructions. The parties can then appeal any determinations that the district court makes on those instructions, which the Court of Appeals would review *de novo*. *See United States v. Estevez*, 961 F.3d 519, 526-27 (2d Cir. 2020). Nothing in the Communication Act's guarantee of a "trial de novo" suggests that a

§ 504(a) trial would not follow that same course. 47 U.S.C. § 504(a). We therefore disagree with the Fifth Circuit's holding in *Stevens*.

Moreover, given the Supreme Court's recent decision in *McLaughlin Chiropractic Associates, Inc. v. McKesson Corp.*, 606 U.S. 146, 145 S.Ct. 2006, ––– L.Ed.2d ––– (2025), it is questionable whether *Stevens* remains good law at all. In *Stevens*, the Fifth Circuit reasoned that the district court lacked jurisdiction to consider legal challenges to the validity of a forfeiture order in a § 504(a) trial because § 402(a), by reference to the Hobbs Act, vests courts of appeals with "'exclusive jurisdiction . . . to determine the validity of' final FCC forfeiture orders." 691 F.3d at 623 (quoting 28 U.S.C. § 2342). *McLaughlin*, however, teaches that "[t]he Hobbs Act does not preclude district courts in enforcement proceedings from independently assessing whether an agency's interpretation of the relevant statute is correct," so it may well abrogate *Stevens*. 606 U.S. at 152, 145 S.Ct. 2006.[16] But even if that were not the case, we would not find *Stevens'* reasoning persuasive. While § 402(a), the Communication Act's general

[16] That *Stevens* remained good law when Verizon was deciding whether to pay the forfeiture and seek judicial review in a court of appeals or to forgo payment until the government brought a § 504(a) enforcement action is, for our purposes, immaterial. True, the FCC could have pursued a collection action in a Circuit that follows the *Stevens* rule because Verizon is subject to nationwide venue under § 504(a). *See* 47 U.S.C. § 504(a) (providing that a § 504(a) action may be "brought in the district where the . . . carrier has its principal operating office or in any district through which the line or system of the carrier runs"). But if that had been the case, then it would have been up to Verizon to raise its Seventh Amendment challenge before that Circuit, as it has done here.

review provision, vests such exclusive jurisdiction in the courts of appeals, "[i]t is a commonplace of statutory construction that the specific governs the general." *Nat'l Labor Rels. Bd. v. SW Gen., Inc.*, 580 U.S. 288, 305, 137 S.Ct. 929, 197 L.Ed.2d 263 (2017) (quotation marks omitted). And here, § 504(a) creates a specific "exception to [the] general rule" for government actions for the recovery of forfeiture penalties. *AT&T Corp.*, 323 F.3d at 1084. In other words, despite its protestations, Verizon waived any right it had to the same kind of trial the SEC's enforcement targets have post-*Jarkesy*.

Accordingly, we conclude that, assuming Verizon has a Seventh Amendment right to a trial by jury, those rights were not violated because it had, but chose to forgo, an opportunity for a § 504(a) trial.

CONCLUSION

For the foregoing reasons, the petition for review is **DENIED**.

APPENDIX B

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	File No.: EB-TCD-
	)	18-00027698
Verizon Communications	)	NAL/Acct. No.:
	)	202032170006
	)	FRN: 0003257094

FORFEITURE ORDER

[FCC 24-41]

Adopted: April 17, 2024 Released: April 29, 2024

By the Commission: Chairwoman Rosenworcel issuing a statement; Commissioners Carr and Simington dissenting and issuing separate statements.

TABLE OF CONTENTS

Paragraph

I. INTRODUCTION 1
II. BACKGROUND 2
A. Legal Background 2
B. Factual Background 8
III. DISCUSSION 21
A. Location Information is CPNI 22
B. Verizon Had Fair Notice That its LBS Practices Were Subject to Enforcement Under the Communications Act 35

C. Verizon Failed to Take Reasonable Steps to Protect CPNI 42
1. Verizon's Customer Location Disclosures to Securus Were Unauthorized and Violated Section 222 43
2. Verizon's Protection of Customer Location Information Was Unreasonable Both Before and After the Securus/Hutcheson Disclosures 46
3. Verizon Bore the Burden of Production.. 59
D. The Forfeiture Amount is Lawful and Consistent with FCC Precedent..... 66
1. Verizon Willfully Violated the Act and the Commission's Rules..... 69
2. The Commission Did Not Need to Find Unauthorized Access to CPNI During the Limitations Period..... 73
3. The Commission Reasonably Found that Verizon Engaged in 65 Continuing Violations..... 77
4. The Commission Will Reduce the Forfeiture Amount by $1,417,500 83
5. The Upward Adjustment is Permissible and Warranted..... 87
E. Section 503(b) Is Employed Here Consistent With the Constitution..... 90
IV. CONCLUSION 101
V. ORDERING CLAUSES..... 102

I. INTRODUCTION

1. On February 28, 2020, the Commission issued a Notice of Apparent Liability for Forfeiture and Admonishment (*NAL*) against Verizon Communications (Verizon or Company).[1] In the *NAL*, the Commission admonished Verizon for apparently disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it, and proposed to fine Verizon $48,318,750 for failing to take reasonable steps to protect its customers' location information. After reviewing the Company's response to the *NAL*,[2] we find no reason to cancel or withdraw the proposed penalty. However, pursuant to additional factual evidence provided in Verizon's NAL Response that is relevant to the forfeiture calculation, we reduce the proposed penalty by $1,417,500, and therefore impose a penalty of $46,901,250 against Verizon.

II. BACKGROUND

A. Legal Background

2. As set forth fully in the *NAL*,[3] carriers are required to protect the confidentiality of certain customer data related to the provision of telecommunications service. This includes location information, which is customer proprietary network information (CPNI) pursuant to section 222 of the Communications Act

---

[1] *Verizon Communications*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1698 (2020) (*NAL*).

[2] *Verizon Communications*, Response to Notice of Apparent Liability for Forfeiture and Admonishment (filed May 7, 2020) (on file in EB-TCD-18-00027698) (NAL Response or Response).

[3] *See generally NAL.*

(Act).[4] The Commission has advised carriers that this duty requires them to take "every reasonable precaution" to safeguard their customers' information.[5] Section 222(a) of the Act imposes a general duty on telecommunications carriers to "protect the confidentiality of proprietary information" of "customers."[6] Section 222(c) establishes specific privacy requirements for "customer proprietary network information" or CPNI, namely information relating to the "quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[7] The Commission has promulgated regulations implementing section 222 (CPNI Rules), which require, among other things, that carriers employ "reasonable

---

[4] 47 U.S.C. § 222.

[5] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007) (*2007 CPNI Order*).

[6] 47 U.S.C. § 222(a).

[7] 47 U.S.C. § 222(c), (h)(1)(A) (emphasis added). "Telecommunications service" is defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(53). The mobile voice services provided by Verizon are "telecommunications services." *See* 47 U.S.C. § 332(c)(1); H.R. Conf. Rep. No. 104-458 at 125 (1996) ("This definition [of 'telecommunications service'] is intended to include commercial mobile service.").

measures to discover and protect against attempts to gain unauthorized access to CPNI."[8]

3. *Customer Consent to Disclose CPNI*. With limited exceptions, a carrier may only use, disclose, or permit access to CPNI with customer approval.[9] Generally, carriers must obtain a customer's "opt-in approval" before disclosing that customer's CPNI.[10] This means that a carrier must obtain the customer's "affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request . . . ."[11]

4. This opt-in requirement has been in place since 2007, when the Commission amended its rules in the *2007 CPNI Order* after finding that once carriers disclosed CPNI to third parties, including joint venturers and independent contractors, that information was out of the control of the carrier and had a higher risk of being improperly disclosed.[12] Accordingly, among

---

[8] *See* 47 CFR § 64.2001 *et seq.*; *id.* § 64.2010(a). The CPNI Rules are a subset of, and are thus included within, the Commission's rules.

[9] 47 U.S.C. § 222(c)(1) ("Except as required by law *or with the approval of the customer*, a telecommunications carrier that receives or obtains [CPNI] by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.") (emphasis added).

[10] 47 CFR § 64.2007(b).

[11] 47 CFR § 64.2003(k).

[12] *2007 CPNI Order*, 22 FCC Rcd at 6947-53, paras. 37-49. Prior to the *2007 CPNI Order* the Commission's rules had allowed carriers

other things, this opt-in requirement was meant to allow individual consumers to determine if they wanted to bear the increased risk associated with sharing CPNI with such third parties.[13] In the Commission's view, obtaining a customer's express consent in these circumstances is particularly important, because a carrier cannot simply rectify the harms resulting from a breach by terminating its agreement with such a third party, "nor can the Commission completely alleviate a customer's concerns about the privacy invasion through an enforcement proceeding."[14] The Commission further concluded that contractual safeguards between a carrier and such a third party do not obviate the need for explicit customer consent, as such safeguards do not eliminate the increased risk of unauthorized CPNI disclosures that accompany information that is provided by a carrier to such a third party.[15] Thus, the Commission determined that, with limited exceptions, a carrier may only use, disclose, or permit access to CPNI with the customer's opt-in approval.[16]

5. *Reasonable Measures to Safeguard CPNI*. The Commission has also recognized that an opt-in requirement alone is not enough to protect customer CPNI, especially in light of tactics like "pretexting," where a

---

to share CPNI with joint venture partners and independent contractors on an opt-out basis for the purpose of marketing communications-related services to customers. *Id.* at 6931-32, para. 8.

[13] *2007 CPNI Order*, 22 FCC Rcd at 6950, para. 45.

[14] *2007 CPNI Order*, 22 FCC Rcd at 6949, para. 42.

[15] *2007 CPNI Order*, 22 FCC Rcd at 6952, para. 49.

[16] *See* 47 CFR § 64.2007(b).

party pretends to be a particular customer or other authorized person in order to illegally obtain access to that customer's information (thus circumventing opt-in requirements).[17] Therefore, the Commission adopted rules requiring carriers to "take reasonable measures to *discover* and *protect* against attempts to gain unauthorized access to CPNI."[18] To provide some direction on how carriers should protect against tactics like pretexting, the Commission included in its amended rules customer authentication requirements tailored to whether a customer is seeking in-person, online, or over-the-phone access to CPNI.[19] It also adopted password and account notification requirements.[20]

6. The Commission made clear that the specific customer authentication requirements it adopted were "minimum standards" and emphasized the Commission's commitment "to taking resolute enforcement action to ensure that the goals of section 222 [were] achieved."[21] Although carriers are not expected to eliminate every vulnerability to the security of CPNI, they must employ "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[22] They must also take reasonable measures to protect the confidentiality of CPNI—a permanent and

---

[17] *See* 2007 CPNI Order, 22 FCC Rcd at 6928, para. 1 & n.1.

[18] 47 CFR § 64.2010(a) (emphasis added).

[19] *See* 47 CFR § 64.2010(b)-(d).

[20] *See* 47 CFR § 64.2010(e)-(f).

[21] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[22] 47 CFR § 64.2010(a).

ongoing obligation to police disclosures and ensure proper functioning of security measures.[23] As the Commission stated in the *NAL*, several government entities provide guidance and publish best practices that are intended to help companies evaluate the strength of their information security measures.[24]

---

[23] *See 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 ("We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.").

[24] For example, the National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. NIST publishes cybersecurity and privacy frameworks which feature instructive practices and guidelines for organizations to reference. The publications can be useful in determining whether particular cybersecurity or privacy practices are reasonable by comparison. The model practices identified in the NIST and other frameworks, however, are not legally binding rules, and we do not consider them as such here. The Federal Trade Commission (FTC), the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), and the Cybersecurity & Infrastructure Security Agency (CISA) also offer guidance related to managing data security risks. *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (NIST Cybersecurity Framework); NIST, The NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 (Jan. 16, 2020), https://nvlpubs. nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf; FTC, Start with Security: A Guide for Business, Lessons Learned from FTC Cases (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Communications Security, Reliability and Interoperability Council, CSRIC Best Practices, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data; CISA,

7. *Section 217.* Finally, the Act makes clear that carriers cannot disclaim their statutory obligations to protect their customers' CPNI by delegating such obligations to third parties. Section 217 of the Act provides that "the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person."[25]

B. Factual Background

8. *Customer Location Information and Verizon's Location-Based Services Business Model.* Verizon provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on Verizon's wireless network.[26] As part of its business, Verizon ran a Location-Based Services (LBS) program until March 2019. Through the LBS program, Verizon sold access to its customers' location information to companies known as "location information aggregators," who then resold access to such information to third-party location-based service providers or in some cases to intermediary companies who then resold access to such information to location-based

---

Cross-Sector Cybersecurity Performance Goals and Objectives (last visited Aug. 17, 2022), https://www.cisa.gov/cpgs.

[25] 47 U.S.C. § 217.

[26] *See* Verizon Communications, 2021 Annual Report, https://www.verizon.com/about/sites/default/files/2021-Annual-Report-on-Form-10-K.pdf.

service providers.[27] Verizon had arrangements with two location information aggregators: LocationSmart and Zumigo (the Aggregators). Each Aggregator, in turn, had arrangements with location-based service providers. In total, Verizon sold access to its customers' location information (directly or indirectly) to 67 third-party entities (including the two Aggregators).[28]

9. The Verizon LBS program was largely governed via contractual provisions that vested Verizon with oversight authority over the Aggregators. Verizon entered into contracts with the Aggregators, and the Aggregators then entered into their own contracts with various LBS providers. Verizon asserts that its LBS program was subject to a number of safeguards and that both the LBS providers and Aggregators had to satisfy various requirements, which were memorialized in and governed by contract provisions with the Aggregators.[29] According to Verizon, these provisions included various information security requirements, including implementing and maintaining multiple types of security controls, preventing unauthorized disclosures of Verizon's data, and compliance with consumer protection and data privacy laws and industry best practices.[30] Beyond these security provisions, which Verizon required the Aggregators to likewise

---

[27] The *NAL* includes a more complete discussion of the facts and history of this case and is incorporated herein by reference. *See NAL*, 35 FCC Rcd at 1703-12, paras. 11-38.

[28] *See NAL*, 35 FCC Rcd at 1703-04, paras. 12-13.

[29] *See NAL*, 35 FCC Rcd at 1704-05, paras. 14-16.

[30] *See NAL*, 35 FCC Rcd at 1705, para. 15; NAL Response at 18.

hold the LBS providers to, the Aggregator-LBS provider contracts included provisions obligating the LBS providers to provide Verizon's customers with clear disclosure of the way their location information would be "accessed, used, copied, stored, or disclosed" by the location-based service provider and obtain "affirmative, opt-in consent" from Verizon customers or users "prior to accessing, using, storing or disclos-ing location information."[31] This arrangement meant that it was typically the LBS providers who were obligated "to provide notice and obtain consent" from consumers—not the Aggregators or Verizon.[32] Verizon had broad authority under its contracts to "terminate its relationship with each Aggregator for any material breach of contract terms, and it could terminate any arrangement that failed to meet Verizon's standards."[33]

10. While Verizon did not have contracts with the LBS providers, each provider was required to submit an application that described, among other things, the "Use Case" or purposes for which it would use the location information, as well as the process it would use for providing notice and obtaining opt-in consent from a Verizon customer for use and sharing of the

---

[31] *See NAL*, 35 FCC Rcd at 1705, para. 14 (citing Response to Supplemental Letter of Inquiry from Verizon to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 8, Response to Question 4 (June 5, 2019) (on file in EB-TCD-18-00027698) (Supplemental LOI Response)).

[32] *See NAL*, 35 FCC Rcd at 1704-05, para. 14 (citing Supplemental LOI Response at 8, Response to Question 4).

[33] *NAL*, 35 FCC Rcd at 1705, para. 16 (citations omitted).

customer's location information.[34] Verizon claims that it only approved applications for one of six specific types of Use Cases: "'call routing, roadside assistance, proximity marketing, transportation and logistics, fraud mitigation/identity management, and mobile gaming/lottery.'"[35]

11. Verizon's approval process and ongoing monitoring involved a third-party Auditor, Aegis Mobile, LLC (Aegis).[36] According to Verizon, Aegis would "perform background checks on companies seeking access to location information before those companies were allowed to obtain it," and also "validate and reconcile the records of consent events and the records of each access to a subscriber's location on a daily basis."[37] Validation and reconciliation of requests for customer location information with the corresponding record of consumer consent was not always successful in the initial processing of data, and could vary greatly depending on which LBS provider was being checked (e.g., in a five and a half month time period, more than 50% of one LBS provider's transaction could not be reconciled

---

[34] *See NAL*, 35 FCC Rcd at 1705-06, para. 17 (citing Response to Letter of Inquiry from Verizon to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 2, Response to Question 1 (Oct. 15, 2018) (on file in EB-TCD-18-00027698) (LOI Response)).

[35] *NAL*, 35 FCC Rcd at 1706, para. 17 (quoting LOI Response at 2, Response to Question 1).

[36] *See NAL*, 35 FCC Rcd at 1706-08, paras. 18-24.

[37] *NAL*, 35 FCC Rcd at 1706, paras. 18 & 19 (citations omitted).

in the first instance).[38] Verizon claimed that this was only the initial step of the consent validation process and that Aegis would follow-up "with the Aggregators or their [LBS] provider customers" and correct "misalignments in the data or performing other data operations," resulting in matching "99.95% of all records of location requests to the corresponding consent record," followed by a spot-check of the remaining 0.05% records.[39]

12. Verizon also asserted that Aegis's "broader oversight program" had additional components, including looking at trends in data to identify larger areas of concern and using various methods "to ensure that the Aggregators (and their location-based service provider customers) were complying with their contractual obligations."[40] According to Verizon, Aegis "applied fraud analytics techniques to refine its ability to broadly identify potential issues going forward"—but Verizon offered no examples of issues identified and addressed via such data analysis.[41] Verizon also claims that Aegis reviewed LBS providers to make sure they were in compliance with their use case, notice, and consent

---

[38] *See NAL*, 35 FCC Rcd at 1707, para. 20 (citing LOI Response at VZ-0000873, Response to Request for Documents No. 6).

[39] *NAL*, 35 FCC Rcd at 1707, para. 21 (citing Declaration of John A. Bruner, Jr., Aegis Mobile, LLC, paras. 5-6 (Feb. 21, 2020) (on file in EB-TCD-18-00027698) (Bruner Decl.)).

[40] *NAL*, 35 FCC Rcd at 1707-08, paras. 22-23 (citing Supplemental LOI Response at 4, 22, Response to Questions 1, 13; Bruner Decl. at para. 7).

[41] *NAL*, 35 FCC Rcd at 1707-08, para. 22.

requirements.[42] In addition, Verizon says it reviewed and/or addressed "'discrete issues as they were raised by Aegis or otherwise.'"[43] For example, Verizon described an investigation into an allegation that a bail bonds company had obtained unauthorized access to Verizon consumers' location data.[44] According to Verizon, the investigation concluded that the company was likely a rejected applicant to its LBS program and that the company was not receiving location information, but that "it is possible for [LBS] program companies with delegated consent to falsify consent records and obtain [Verizon] subscriber data without their consent."[45] As the *NAL* explained, the "report made no recommendations for adopting additional methods to mitigate the risk of approved location-based service providers falsifying consent records to obtain Verizon customer location information without their consent."[46]

13. *Unauthorized Access and Use of Customer Location Information.* On May 10, 2018, the *New York Times* published an article that detailed security breaches involving Verizon's (and other carriers') practice of selling access to customer location information.[47] The

---

[42] *See* NAL, 35 FCC Rcd at 1708, para. 23 (citing Supplemental LOI Response at 22, Response to Question 13).

[43] *NAL*, 35 FCC Rcd at 1708, para. 24 (quoting Supplemental LOI Response at 12, Response to Question 5).

[44] *See NAL*, 35 FCC Rcd at 1708, para. 24 (citing Supplemental LOI Response at 13, Response to Question 5).

[45] *NAL*, 35 FCC Rcd at 1708, para. 24 (citations omitted).

[46] *NAL*, 35 FCC Rcd at 1708, para. 24.

[47] See Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018),

NAL includes a more detailed summary of the article and its findings, but essentially the breaches involved a location-based service provider (Securus Technologies, Inc., or Securus) that offered a location-finding service to law enforcement and corrections officials that allowed such officials to access customer mobile device location *without* that device owner's knowledge or consent.[48] Not only was Securus's location-finding service outside the scope of its approved "Use Case" or any agreement with either Aggregator (and thus had not been reviewed and approved by Verizon), but despite Securus's claims that the program required appropriate "legal authorization," it did not verify such authorizations and its program was used and abused by a (now former) Missouri Sheriff (Cory Hutcheson) for non-law enforcement purposes and in the absence of any such legal authorization.[49] Securus obtained location services from a company called 3Cinteractive, and

---

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

[48] *See NAL*, 35 FCC Rcd at 1708-09, paras. 25-26 (citing Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018) https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html).

[49] *See NAL*, 35 FCC Rcd at 1708-09, paras. 25-26 (citing Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018) https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html; Doyle Murphy, *Ex-Missouri Sheriff Cory Hutcheson Sentenced to 6 Months in Prison*, Riverfront Times (Apr. 29, 2019), https://www.riverfronttimes.com/newsblog/2019/04/29/ex-missouri-sheriff-cory-hutcheson-sentenced-to-6-months-in-prison).

3Cinter-active obtained Verizon consumers' location information pursuant to a contract with the Aggregator Location-Smart.[50] Verizon conceded that its regular audits "did not reveal that Securus was using this data in ways that differed from its approved use case with LocationSmart."[51]

14. The Department of Justice's U.S. Attorney's Office for the Eastern District of Missouri charged Hutcheson with, among other things, wire fraud and illegally possessing and transferring the means of identification of others, and Hutcheson pleaded guilty on November 20, 2018.[52] The Department of Justice's investigation of Hutcheson's actions included an examination of how the Securus location-finding service operated. Once Hutcheson became an authorized user of Securus's LBS software, he was able to obtain the location of specific mobile telephone devices.[53] In order

---

[50] *See NAL*, 35 FCC Rcd at 1709, para 27 (citing Supplemental LOI Response at 15, Response to Question 7).

[51] *NAL*, 35 FCC Rcd at 1709, para. 29 (citing LOI Response at 12, Response to Question 8).

[52] *See* Press Release, U.S. Attorney's Office Eastern District of Missouri, *Mississippi County Sheriff Pleads Guilty to Fraud and Identity Theft, Agrees to Resign* (Nov. 20, 2018), https://www.justice.gov/usao-edmo/pr/mississippi-county-sheriff-pleads-guilty-fraud-and-identity-theft-agrees-resign.

[53] *See* Government's Sentencing Memorandum at 3, *United States v. Corey Hutcheson*, Case No. 1:18-CR-00041 JAR, Doc. No. 65 (E.D. Mo. Apr. 23, 2019) (Hutcheson Sentencing Memo), https://storage.courtlistener.com/recap/gov.uscourts.moed.160663/gov.uscourts.moed.160663.65.0.pdf.; *see also NAL*, 35 FCC Rcd at 1708-09, paras. 25-26.

to do so, users (including Hutcheson) were required to input the telephone number of the device they wanted to locate, and then "upload a document manually checking a box, the text of which stated, '[b]y checking this box, I hereby certify the attached document is an official document giving permission to look up the location on this phone number requested.'"[54] As soon as Hutcheson (or any other authorized user) submitted his request and uploaded a document, the Securus LBS platform would *immediately* provide the requested location information (regardless of the adequacy of the uploaded document).[55] Rather than "uploading the required legal process," Hutcheson instead "routinely uploaded false and fraudulent documents . . . , each time representing that the uploaded documents were valid legal process authorizing the location requests the defendant made."[56] Those "false and fraudulent documents" included "his health insurance policy, his auto insurance policy, and pages selected from Sheriff training materials."[57] Hutcheson "submitted thousands of Securus LBS requests and obtained the location

---

[54] Hutcheson Sentencing Memo at 3; *see also NAL*, 35 FCC Rcd at 1708-09, para. 25.

[55] *See* Hutcheson Sentencing Memo at 3-4; *see also NAL*, 35 FCC Rcd at 1708-09, para. 25.

[56] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1709, para. 26.

[57] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1709, para. 26.

data of hundreds of individual phone subscribers without valid legal authorization."[58]

15. *Verizon's Response to the Securus Disclosures.* Verizon directed LocationSmart to terminate Securus's and 3Cinteractive's access to Verizon customer location information on May 11, 2018.[59] Following this termination, Verizon stated that it "undertook a review to better understand how [the Securus and Hutcheson breaches] could occur despite the contractual, auditing, and other protections" in had in place to protect customer location data."[60] Verizon says it determined that its auditing did not identify Securus's unauthorized program because Securus used the profile of its approved Use Case, the number of Securus requests appeared normal, and nothing in Securus's background check changed such that the auditor would question Securus's credibility.[61] Verizon also claimed to conduct a broader investigation, which the Company said "did not uncover any new incidents in which a Location Aggregator (or its customer) mispresented that it had customer consent."[62] However, through this

---

[58] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1709, para. 26.

[59] *See NAL*, 35 FCC Rcd at 1709, para. 28 (citing Supplemental LOI Response at 16, Response to Question 7).

[60] *NAL*, 35 FCC Rcd at 1709, para. 29 (citing LOI Response at 12, Response to Question 8).

[61] *See NAL*, 35 FCC Rcd at 1710, para. 29 (citing LOI Response at 12, Response to Question 8).

[62] *NAL*, 35 FCC Rcd at 1710, para. 30 (citing LOI Response at 12, Response to Question 8).

investigation Verizon learned of a vulnerability whereby a cybersecurity researcher gained access "to Verizon customer data through LocationSmart's website via a demonstration page for prospective [LocationSmart] customers."[63] Though Verizon claims that the cybersecurity research only attempted location queries for individuals who had consented, it nonetheless suggested "that it was not aware of LocationSmart's use of Verizon customer location information for this purpose before the investigation and state[d] that it 'directed both Location-Smart and Zumigo to not use Verizon customer data in any demonstration site going forward.'"[64]

16. On June 12, 2018, Verizon notified the two Aggregators that it intended to terminate their contracts under the LBS program as soon as possible.[65] However, it was not until November 30, 2018, that Verizon terminated all arrangements with Zumigo, and terminated all but four arrangements with LocationSmart (the four exceptions being arrangements with companies that provided location-based roadside assistance).[66] Per Verizon, during the more than five intervening months it had "(1) stopped authorizing any new uses of

---

[63] *NAL*, 35 FCC Rcd at 1710, para. 31 (citing LOI Response at 13, Response to Question 10).

[64] *NAL*, 35 FCC Rcd at 1710, para. 31 (citing LOI Response at 13, Response to Question 10).

[65] *NAL*, 35 FCC Rcd at 1710, para 32 (citing LOI Response at 9, Response to Question 6).

[66] *See NAL*, 35 FCC Rcd at 1710, para. 34 (citing Supplemental LOI Response at 2, Response to Question 1).

location information by the Aggregators or the sharing of such information with any new customers of the Aggregators, and (2) strengthened its transaction verification process to identify anomalies in consent requests that might be indicative of a problem (e.g., multiple location requests in a 24-hour period or an increase in location requests that are out of the ordinary).[67]

17. While Verizon was phasing out its relationships with the Aggregators, it started a "Direct Location Services" program as an alternative, under which Verizon itself would obtain consent from its customers to share their location information with particular LBS providers.[68] Verizon obtained affirmative consent by sending its customer a text message and only sharing location information with an LBS provider if the Verizon customer responded affirmatively to the text message request.[69]

18. Eventually, Verizon completely exited the location-based services business. On April 5, 2019, Verizon announced it would terminate its in-house Direct Location Services program by the end of July 2019.[70] As far

---

[67] *NAL*, 35 FCC Rcd at 1710, para 32 (citing LOI Response at 10, Response to Question 6).

[68] *See NAL*, 35 FCC Rcd at 1710-11, para. 33 (citing LOI Response at 9, Response to Question 6; Supplemental LOI Response at 3, Response to Question 1).

[69] *See NAL*, 35 FCC Rcd at 1711, para. 33 (citing Supplemental LOI Response at 3, 9, Response to Questions 1, 4).

[70] *See NAL*, 35 FCC Rcd at 1711, para. 36 (citing Supplemental LOI Response at 5, Response to Question 1).

as its LBS Aggregator program, Verizon stopped providing LocationSmart and its four remaining LBS providers access to Verizon customer location information on March 30, 2019.[71] In other words, Verizon did not finally terminate its location-based service program until March 30, 2019, or 324 days from when the *New York Times* first reported on the Securus location-finding service, as well as the abuse of that service by Hutcheson.

19. *Notice of Apparent Liability*. On February 28, 2020, the Commission issued the *Verizon NAL* proposing a $48,318,750 fine against Verizon for its apparent willful and repeated violation of section 222 of the Act and section 64.2010 of the Commission's CPNI Rules for failing to have reasonable protections in place to prevent unauthorized access to customer location information. In the *Verizon NAL*, the Commission also admonished Verizon for apparently disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it.

20. On May 7, 2020, Verizon filed a response to the *NAL*.[72] Verizon makes a number of arguments as to why the *NAL* should be withdrawn and cancelled. Verizon argues that location information is not CPNI and thus is not subject to the Act and the Commission's CPNI Rules, and that even if it was, the Company did

---

[71] *See NAL*, 35 FCC Rcd at 1711, para. 35 (Supplemental LOI Response at 2, Response to Question 1).

[72] *Verizon Communications*, Response to Notice of Apparent Liability for Forfeiture and Admonishment (filed May 7, 2020) (on file in EB-TCD-18-00027698) (NAL Response or Response).

not have fair notice that it would be classified as CPNI.[73] Verizon also argues that it acted reason-ably both pre-and post-publication of the *New York Times* article. The Company claims that the LBS program had reasonable protections in place before the *New York Times* article, and that the Company's response to the article, including its months-long continuation of the LBS program, was likewise reasonable.[74] Verizon argues that the forfeiture amount is arbitrary and capricious.[75] Finally, Verizon contends that the forfeiture amount is incorrect insofar as the *NAL* miscounts the number of LBS providers and the number of days in the forfeiture calculation.[76]

III. DISCUSSION

21. The Commission proposed a forfeiture in this case in accordance with section 503(b) of the Communications Act of 1934, as amended (Act),[77] section 1.80 of the Commission's rules,[78] and the Commission's *Forfeiture Policy Statement*.[79] When we assess forfeit-

---

[73] NAL Response at 5-6, 9-11, 32-39.

[74] NAL Response at 39-40, 44-54.

[75] NAL Response at 8-9, 56-59.

[76] NAL Response at 58, Exh. A (Supplemental Declaration of John A. Bruner, Aegis Mobile, LLC, para. 12 (May 6, 2020)), Exh D.

[77] 47 U.S.C. § 503(b).

[78] 47 CFR § 1.80.

[79] *The Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, Report and Order, 12 FCC Rcd 17087 (1997) (*Forfeiture Policy Statement*), *recons. denied*, Memorandum Opinion and Order, 15 FCC Rcd 303 (1999).

tures, section 503(b)(2)(E) requires that the Commission take into account the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[80] We have fully considered Verizon's NAL Response, which includes a variety of legal and factual arguments. With one exception, we find none of Verizon's arguments persuasive. Upon review of Verizon's NAL Response and a further review of the evidence in the record, we will adjust the forfeiture calculation to account for updated evidence related to the non-participation of two entities in Verizon's LBS program that had been included in the original forfeiture calculation. We therefore reduce the $48,318,750 forfeiture proposed in the *NAL* by $1,417,500, and impose a penalty of $46,901,250.

A. Location Information is CPNI

22. As the *NAL* explained in more detail, the customer location information disclosed in Verizon's LBS program is CPNI under the Act and our rules.[81] Section 222 defines CPNI as "information that relates to the quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[82] The customer location information used in

---

[80] 47 U.S.C. § 503(b)(2)(E).

[81] *See NAL*, 35 FCC Rcd at 1712-14, paras. 41-48.

[82] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

Verizon's LBS program falls squarely within this definition. Verizon's arguments to the contrary[83] are largely reiterations of arguments the Commission considered and found unpersuasive in the *NAL*. Consistent with the analysis of location data found in the *NAL*, we remain persuaded that the location data at issue here constitute CPNI.

23. *First*, the customer location information at issue here relates to the location of a telecommunications service—i.e., Verizon's commercial mobile service.[84] As fully explained in the *NAL*:

> A wireless mobile device undergoes an authentication and attachment process to the carrier's network, via the closest towers. After a mobile device is authenticated and logically attached to a wireless network, it may be (1) connected (sending/receiving data/voice) or (2) idle. In either state, the carrier must be aware of and use the device's location in order for it to enable customers to send and receive calls. Verizon is therefore providing telecommunications service to these customers whenever it is enabling the customer's device to send and receive calls—regardless of whether the device is actively in use for a call.[85]

---

[83] *See* NAL Response at 5-6, 9-11, 32-39.

[84] *See* 47 U.S.C. § 332(c)(1) (providing that "a person engaged in the provision of a service that is a commercial mobile service shall, insofar as such person is so engaged, be treated as a common carrier for purposes of this chapter"), (d)(1) (defining "commercial mobile service").

[85] *See NAL*, 35 FCC Rcd at 1712, para. 43.

24. We conclude that the location information at issue here meets the first prong of the CPNI definition under either of two alternative interpretations. For one, we believe that the relevant statutory language is best read as referring to "information that relates to the . . . location, . . . of a telecommunications service . . . ."[86] That interpretation accords with the "rule of the last antecedent," which suggests that the term "of use" in section 222(h)(1)(A) modifies only "amount," as opposed to the preceding terms such as "location."[87] Our interpretation also better squares with the broader operation of section 222. If the language "of use" modified every term in the preceding list, it would lead to apparently anomalous results. For instance, although the phrase "amount of use of a telecommunications service" plainly refers at least to the number and length of telephone calls, it is not clear what "technical configuration of use" would mean. And our interpretation squares more readily with section 222(d)(1), which preserves carriers' ability to use CPNI to "initiate" service[88]—an event that, aspects of which, ordinarily occur before the service is in "use."

25. The location information at issue here readily fits within that interpretation of the first prong of the CPNI definition. Verizon's customers can access the

---

[86] 47 U.S.C. § 222(h)(1)(A).

[87] *See, e.g., Lockhart v. United States*, 577 U.S. 347, 351 (2016) (the rule of the last antecedent "provides that 'a limiting clause or phrase . . . should ordinarily be read as modifying only the noun or phrase that it immediately follows'").

[88] 47 U.S.C. § 222(d)(1).

commercial mobile service to which they subscribe over a broad geographic area, and their location at a given point in time—and the fact of Verizon's ability to use its network to determinate that location—is reasonably understood as associated with or a reference to the location of the Verizon telecommunications service.[89] Consequently, consistent with our assessment in the *NAL*,[90] we find this to be information that "relates to" the location of Verizon's telecommunications service within the meaning of the first prong of the CPNI definition.[91]

26. In the alternative, even if the term "of use" modified "location," we still conclude the information at issue fits within the first prong of the definition of CPNI.

---

[89] *See*, *e.g.*, *NAL*, 35 FCC Rcd at 1703, para. 11 ("Verizon provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on Verizon's wireless network.")

[90] *See*, *e.g.*, *NAL*, 35 FCC Rcd at 1712-14, paras. 43, 46.

[91] *See*, *e.g.*, *Collins Concise Dictionary*, Third Ed., at 1129 (HarperCollins Pub. 1995) (defining "relate" as, among other things, "establishing association (between two or more things) or (of something) to have relation or reference (to something else)"); *American Heritage Dictionary*, Third Ed., at 695 (Dell Pub. 1994) (defining "relate" as, among other things, "To bring into logical or natural association," "To establish or demonstrate a connection between," or "To have connection, relation, or reference"); *Merriam-Webster's Collegiate Dictionary*, Tenth Ed., at 987 (Merriam-Webster Pub. 1994) (defining "relate" as, among other things, "to show or establish logical or causal connection between"); *The Oxford Paperback Dictionary & Thesaurus*, at 636 (Oxford Univ. Press 1997) (defining "relate" as, among other things, "connect in thought or meaning" or "have reference to").

Verizon does not dispute the *NAL*'s explanation that customers' devices and Verizon's network regularly exchange information as necessary for customers to send and receive calls.[92] To the extent that Verizon contends that this does not represent use of the telecommunications service because it merely enables the provision of that service, Verizon does not demonstrate why that is a fair characterization or why it would represent a meaningful distinction in any case. Consistent with the reasoning of the *NAL*,[93] we believe that Verizon's customers subscribe to its commercial mobile service to enable them to receive and transmit calls. When customers' devices are exchanging communications with Verizon's network, and thereby ensuring that they can receive incoming calls and place outgoing calls, we think that 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.[94]

---

[92] *NAL*, 35 FCC Rcd at 1712-13, para. 43.

[93] *See*, *e.g.*, *NAL*, 35 FCC Rcd at 1712-14, paras. 43, 46.

[94] Definitions of "use" appear sufficiently broad to encompass our understanding of the term in this scenario. *See*, *e.g.*, *Collins Concise Dictionary*, Third Ed., at 1483 (HarperCollins Pub. 1995) (defining "use," among other things, to mean "to put into service or action; employ for a given purpose"); *American Heritage Dictionary*, Third Ed., at 884 (Dell Pub. 1994) (defining "use," among other things, to mean "To put into service; employ" and "To avail oneself of; practice"); *Merriam-Webster's Collegiate Dictionary*, Tenth Ed., at 1301 (Merriam-Webster Pub. 1994) (defining "use," among other things, to mean "to put into action or service: avail oneself of"); *The Oxford Paperback Dictionary & Thesaurus*, at 853 (Oxford Univ. Press 1997) (defining "use," among other things, to mean "cause to act or

27. Nor do Verizon's arguments about the source and intended purpose of the location data at issue here persuade us to reach a contrary result. Verizon contends that the location data at issue here, while generated using "the same network functionality as the normal-course operational pinging that occurs between cell sites and customer devices to facilitate Verizon services," nonetheless "occurred separately from that normal-course operation—and was done specifically for the purpose of facilitating the third-party location-based services."[95] Thus, Verizon says, it obtained such location data with the intent of using it for purposes of its LBS initiative, rather than Verizon's provision of commercial mobile service.[96] But nothing in the text of the first prong of the CPNI definition turns on the carriers' stated intent in collecting it. So long as the information "relates to" one or more of the specified criteria, the other factors raised by Verizon do not matter. And as noted above, the information at issue here "relates to" the location of the telecommunications service (or to the location of use of that service), regardless of how Verizon obtained the information and how it planned to use the information.

28. We also are unpersuaded by Verizon's arguments that the location information covered by the first prong of the definition of CPNI is limited to call location information for voice calls based on what Verizon gleans

---

serve for purpose; bring into service" and "exploit for one's own ends").

[95] NAL Response at 34.

[96] NAL Response at 34-35.

from other language in section 222.[97] In addition to the *NAL*'s responses in this regard,[98] we conclude that the use of "location" in (h)(1)(A) as opposed to "call location information" in (d)(4) and (f)(1) must be given some significance:[99] All *location* information is protected as CPNI under (h)(1)(A). But carriers can disclose *call location* information for 911 purposes under (d)(4), which makes sense because 911 calls are *calls*. Nor would it have been irrational for Congress to expressly require opt-in consent for call location information in section 222(f)(1) if the definition of CPNI encompasses other forms of location information, as well. At the time the provision was enacted in 1999, Congress might reasonably have viewed call location information as obviously sufficiently sensitive to necessitate opt-in approval requirements while leaving it to the Commission's discretion whether to require opt-in approval for other location information, just as for other information falling within the definition of CPNI more generally. In

---

[97] *See*, *e.g.*, NAL Response at 5, 32-34.

[98] *NAL*, 35 FCC Rcd at 1714, para. 47.

[99] This interpretive approach is consistent with how the Commission has approached the interpretation of section 222 in other contexts in the past. *See*, *e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8084-85, para. 32 (1998) (distinguishing the interpretation of different language in section 222(a), (c)(1), and (d)(1), given that, "[u]nder well-established principles of statutory construction, 'where Congress has chosen different language in proximate subsections of the same statute,' we are 'obligated to give that choice effect' ").

addition, the Commission's references to "calls" in a prior order that was focused in significant part on data regarding customers' calls—and which did not purport to exhaustively address the application of section 222 to mobile wireless service—cannot reasonably be read as setting forth the outer bounds of the Commission's understanding of section 222.[100]

29. *Second*, the location information at issue was obtained by Verizon solely by virtue of its customer-carrier relationship. The *NAL* explains this in more detail, but the crux of the matter is that:

> Verizon provides wireless telephony services to the affected customers because they have chosen Verizon to be their provider of telecommunications service—in other words, they have a carrier-customer relationship. . . . Verizon's customers provided their wireless location data to Verizon because of their customer-carrier relationship with Verizon, . . .[101]

In sum, although Verizon might also provide non-common-carrier services to the same customer, the customer provided the relevant data "solely by virtue of the carrier-customer relationship."[102]

30. The *NAL* did not specify with precision the standard for applying the second prong of the CPNI

---

[100] *See generally Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609 (2013) (*2013 CPNI Declaratory Ruling*).

[101] *NAL*, 35 FCC Rcd at 1713, para. 44.

[102] *NAL*, 35 FCC Rcd at 1714, para. 46.

definition, and although we elaborate further on some of its contours here, we likewise need not resolve that question with specificity because we find that prong met here under a range of possible approaches. We begin by observing that the second prong of the CPNI definition is focused on a "relationship"—namely, the "carrier-customer relationship."[103] A relationship presumes associations involving at least two parties, and we conclude that it must be understood with that context in mind, rather than focused single-mindedly on one side of the relationship. Our accounting for the customer's viewpoint is also supported by the statutory text's focus on whether the information "is made available to the carrier by the customer"— rather than "obtained by the carrier"—"solely by virtue of the carrier-customer relationship."[104] Thus, although Verizon

[103] 47 U.S.C. § 222(h)(1)(A).

[104] 47 U.S.C. § 222(h)(1)(A). Insofar as Verizon disputes whether "the location information that Verizon obtains" is "obtained solely by virtue of Verizon's provision of telecommunications service," *see*, *e.g.*, NAL Response at 36, the focus on Verizon's "telecommunications service" neither reflects the statutory text regarding prong two of the CPNI definition nor does it appropriately account for these concepts underlying the statutory focus on a customer-carrier "relationship." To be sure, section 222(c)(1) is limited in scope to "a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service." 47 U.S.C. § 222(c)(1). But in that provision, the required nexus is just that the carrier receive or obtain the CPNI "by virtue" (not "solely by virtue") of its provision of a telecommunications service. In its NAL Response, Verizon disputes whether the location information at issue meets the statutory definition of CPNI in section 222(h)(1)(A), *see* NAL Response at 34-36, but does not contend that, if it does meet that definition, section 222(c)(1) nonetheless should not be interpreted to apply here.

suggests that its acquisition of the location information at issue here is in some sense distinct from, or does not depend exclusively on, the carrier-customer relationship,[105] we find that belied by the technical and marketplace realities here, as experienced by Verizon customers.

31. As the *NAL* explains, when a customer subscribes to Verizon's commercial mobile service, Verizon "enables the connection of a customer's device to its network for the purpose of sending and receiving calls, and the customer has no choice but to reveal that location to the carrier."[106] Verizon does not dispute that the carrier-customer relationship fully enables Verizon to obtain the location data at issue here. Verizon contends that while it obtained location data for its LBS program using the same mechanism as it did to provide other services, its acquisition of location information nonetheless "occurred separately from that normal-course operation—and was done specifically for the purpose of facilitating the third-party location-based services."[107] However, Verizon does not claim that a customer, having subscribed to its commercial mobile service, entered a separate agreement with Verizon for the provision of that location information—or that Verizon's voice customers had any way to avoid providing that information if they wanted to subscribe to Verizon's commercial mobile service. Under circumstances such as these, we conclude that the location

---

[105] *See*, *e.g.*, NAL Response at 9, 34-36.

[106] *NAL*, 35 FCC Rcd at 1713, para. 45.

[107] NAL Response at 34.

information at issue from Verizon's commercial mobile service customers was "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[108]

32. Although we find that reasoning sufficient to resolve the application of the second prong of the CPNI definition, we independently conclude that the same decision is warranted even if we parse the matter more finely. For example, in its NAL Response, Verizon has argued that the location information as issue in this matter should not be considered CPNI because the "same equipment-to-device communication occurs for customers using data services . . . as it does for customers making phone calls" and that the "vast majority of traffic on Verizon's network . . . is data traffic."[109] But we are not persuaded that Verizon's provision of multiple services to its telecommu-nications customers (including SMS text messaging and internet service) takes the resulting *relationship* outside the scope of the "carrier-customer" relationship for the specific purposes of the CPNI definition. Nothing dissuades us that the purchase of telecommunications service alone was sufficient to obligate Verizon's customers to make their location informa-tion available to Verizon,[110] and

---

[108] 47 U.S.C. § 222(h)(1)(A).

[109] NAL Response at 9.

[110] Consequently, this is not a situation where we are relying on a theory that the carrier-customer relationship was merely one of a "confluence of multiple factors"—including relationships beyond the carrier-customer relationship itself—that collectively were required for Verizon to obtain the location information at issue here. *Bostock v. Clayton Cty.*, 140 S. Ct. 1731, 1739 (2019) (In contrast to the statute

in evaluating the second prong of the CPNI definition in the past, the Commission has noted that a carrier's "unique position with respect to its customers" when the carrier pre-configures a mobile device to collect information can satisfy "the 'carrier-customer relationship' element of the definition of CPNI."[111] Verizon points out[112] that section 153(51) of the Act provides that "[a] telecommunications carrier shall be treated as a common carrier under [the Act] only to the extent that it is engaged in providing telecommunications services."[113] But we are far from that scenario here, given the many necessary links to Verizon's telecommunications services for the CPNI definition to apply.[114] For one, the protections of section 222(c) only apply with respect to "information that relates to" certain characteristics of "a telecommunications service subscribed to by any customer of" Verizon.[115] And the information must have

---

at issue there, Congress "could have added 'solely' to indicate that actions taken 'because of 'the confluence of multiple factors do not violate the law."); *cf. id.* (observing that "[o]ften, events have multiple but-for causes"). By contrast, information that carriers obtain independently from public records, for example, would not be information that the customer provided to the carrier solely by virtue of the carrier-customer relationship.

[111] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para 23.

[112] *See* NAL Response at 36 n.28.

[113] 47 U.S.C. § 153(51).

[114] For similar reasons, we reject the suggestion that our approach regulates Verizon under section 222 based on the mere fact that it has the status of a telecommunications carrier, rather than being linked to its specific offering of telecommunications services. *See* NAL Response at 32-36.

[115] 47 U.S.C. § 222(h)(1)(A).

been provided by consumers in a manner that reflects the statutorily required nexus to Verizon's telecommunications service.[116] Our interpretation and application of section 222 thus accords with the text of both section 222 and section 153 of the Act, even if it does not reflect the policy that Verizon would prefer.

33. Finally, we reject Verizon's argument that because it also gathered location information from consumers who only subscribed to information services (e.g., tablets) and did not partake of telecommunications services, *none* of the location information has been gathered solely by virtue of the customer-carrier relationship.[117] Against the backdrop of the analysis above, that only bears on the status of the information from those specific, non-voice, customers. The *NAL*'s proposed forfeitures turn not on specific effects on specific customers individually but on Verizon's corporate practices as a whole with respect to the entities that received LBS data.[118] Verizon does not contend that

---

[116] 47 U.S.C. § 222(h)(1)(A).

[117] *See* NAL Response at 35-36.

[118] In particular, the *NAL* did not propose forfeitures based on unauthorized disclosure of CPNI associated with particular customers—it proposed forfeitures based on allegations that Verizon failed to take reasonable steps to protect its customers' location information, with forfeitures proposed not on a per-customer basis but on the basis of the days in which Verizon allegedly did not have a reasonable policy in place for particular entities that received LBS data. *See*, *e.g.*, *NAL*, 35 FCC Rcd at 1726-27, para. 87. And while *FTC v. AT&T Mobility LLC*, 883 F.3d 848 (9th Cir. 2018) (en banc), concluded that the common-carrier limitation on the FTC's authority is activities-based, rather than status-based, it also recognized that "there may be some overlap between the agencies' jurisdiction when the

the LBS data that it provided, directly or indirectly, to any of the entities associated with the proposed forfeitures in the *NAL* was limited exclusively to data from non-voice customers. Thus, the Verizon practices that formed the basis of the proposed forfeitures in the *NAL* included information from voice customers, which falls within the definition of CPNI for the reasons explained above.

34. The Commission therefore affirms its finding from the *NAL* that the location information at issue in the LBS program is CPNI.

B. Verizon Had Fair Notice That its LBS Practices Were Subject to Enforcement Under the Communications Act

35. We reject Verizon's claim that it lacked fair notice that its practices involving customer location information were subject to the Communications Act and potential penalties thereunder.[119] The language of section 222 makes clear that customer location information is CPNI; Verizon's practices involving CPNI, including customer location information, unquestionably are regulated under the Act and the Commission's CPNI Rules; and Verizon's failure to comply with the requirements of the Act and our rules, including the "reasonable measures" mandate of section 64.2010,

---

FCC's regulations of common carriers affect the non-common-carrier activities of those entities," observing that "[i]n the administrative context, two cops on the beat is nothing unusual." *Id.* at 862. Thus, our interpretation of section 222 is not at odds with the court's decision in *FTC v. AT&T Mobility*.

[119] *See* NAL Response at 38-39.

foreseeably makes the Company liable for a forfeiture penalty under section 503 of the Act.

36. Verizon argues that if the Commission wishes to classify location information as CPNI, "it must do so on a prospective basis through a rulemaking or declaratory ruling."[120] But the Commission is not limited to these options. When, as in this case, a carrier's conduct falls within an area subject to regulation by the Commission, it is well established that enforcement action is also a proper vehicle to adjudicate the specific bounds of what is lawful and what is not, subject to principles of fair notice.[121]

37. Contrary to Verizon's assertion, the Commission is not "impos[ing] retroactive liability on a carrier that

---

[120] NAL Response at 38. As discussed more fully in this section, contrary to Verizon's argument, Verizon could have reasonably ascertained that the location information at issue here would be found to meet the definition of CPNI and Verizon would be subject to forfeiture penalties for failing to protect that customer location information as required under section 222 and the CPNI Rules.

[121] *See, e.g.*, *City of Arlington, Texas v. FCC*, 569 U.S. 290, 307 (2013) (affirmatively stating that "Congress has unambiguously vested the FCC with general authority to administer the Communications Act through rulemaking and adjudication"); *Neustar, Inc. v. FCC*, 857 F.3d 886, 894 (D.C. Cir. 2017); *Chisholm v. FCC*, 538 F.2d 349, 365 (D.C. Cir. 1976) (reiterating that "the choice whether to proceed by rulemaking or adjudication is primarily one for the agency regardless of whether the decision may affect agency policy and have general prospective application") (citing *N.L.R.B. v. Bell Aerospace Co.*, 416 U.S. 267, 291-95 (1974); *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947) (stating that "the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency").

did not have adequate notice . . . ."[122] As the D.C. Circuit has explained, "[t]he fair notice doctrine, which is couched in terms of due process, 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.'"[123] And, in general, fair notice principles require that a regulated party be able to identify, with ascertainable certainty, the standards with which the agency expects parties to conform.[124]

38. Here, the Commission previously explained in the *2013 Declaratory Ruling* that it would not "set out a comprehensive list of data elements that pertain to a telecommunications service and satisfy the definition of CPNI and those data elements that do not."[125] Thus, Verizon cannot reasonably have assumed that the fact

---

[122] NAL Response at 38.

[123] *Mississippi Comm'n on Envtl. Quality v. EPA*, 790 F.3d 138, 186 (D.C. Cir. 2015) (quoting *United States v. Chrysler Corp.*, 158 F.3d 1350, 1354 (D.C. Cir. 1998)); *see also United States v. Thomas*, 864 F.2d 188, 195 (D.C. Cir. 1988) ("statutes cannot, in reason, define proscribed behavior exhaustively or with consummate precision").

[124] *Star Wireless, LLC v. FCC*, 522 F.3d 469, 473 (D.C. Cir. 2008) ("In assessing forfeitures against regulated entities, the Commission is required to provide adequate notice of the substance of the rule. . . . The court must consider whether by reviewing the regulation and other public statements issued by the agency, a regulated party acting in good faith would be able to identify, with ascertainable certainty, the standards with which the agency expects parties to conform.") (internal quotations and citations omitted).

[125] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

a given scenario had not been expressly addressed by Commission rules and precedent meant it fell outside the scope of CPNI and the associated protections of section 222 and the Commission's implementing rules. To the contrary, the Commission has stated that "implicit in section 222 is a rebuttable presumption that information that fits the definition of CPNI contained in section 222([h])(1) is in fact CPNI."[126] Moreover, even while declining to comprehensively identify CPNI, including in the case of location information, the Commission emphasized that "location information in particular can be very sensitive customer information."[127] In addition, notwithstanding the fair notice claims it makes now, Verizon asserted to the Commission that it treated customer location information in an essentially equivalent manner to CPNI.[128]

---

[126] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14495-96, para. 167 (1999). Although the Commission was responding, in part, to a request for clarification from MCI regarding "laundering" of CPNI by virtue of transfers to affiliated or unaffiliated entities, it was not limited just to that scenario alone. *See*, *e.g.*, *id.* at 14495, para. 166 (describing the MCI request for clarification being addressed as, among other things, "seek[ing] clarification that there is a rebuttable presumption that customer-specific information in a carrier's files was received on a confidential basis or through a service relationship governed by section 222").

[127] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[128] *See* NAL Response at 40. Verizon concedes that ". . . even if the information used in Verizon's aggregator program were CPNI or even 'call location information,' Verizon would have satisfied either of

39. Further, our conclusion that the location data at issue here fall within the definition of CPNI flows from the text of section 222 is consistent with the Commission's approach to interpreting that provision as laid out in prior precedent. As noted, CPNI is defined by statute, in relevant part, to include "information that relates to . . . the location . . . of a telecommunications service."[129] That definition further directs us to evaluate whether the relevant information "is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[130] Our interpretation of those provisions above relies on the statutory text, interpreted consistent with ordinary tools of statutory interpretation, and is consistent with prior Commission precedent.

40. Finally, Verizon had fair notice of its obligations with respect to CPNI under section 64.2010 of the Commission's rules. In pertinent part, that rule provides that "[t]elecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[131]

Section 222's consent requirements because Verizon required affirmative, opt-in customer consent — the highest level of consent that Section 222 contemplates — before third parties were permitted to access customer location information." *Id.*

[129] 47 U.S.C. § 222(h)(1)(A); *see also*, *e.g.*, *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para. 22 n.48 (citing section 222(h)(1)(A) as "defining CPNI to include 'information that relates to the . . . location . . . of a telecommunications service subscribed to by any customer of a telecommunications carrier'").

[130] 47 U.S.C. § 222(h)(1)(A).

[131] 47 CFR § 64.2010(a).

Beyond "requir[ing] carriers to implement the specific minimum requirements set forth in the Commission's rules," to comply with section 64.2010, the Commission "further expect[s] carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier."[132] The Commission granted carriers flexibility to incorporate the specific measures and practices that are consistent with their otherwise-existing "technological choices."[133] In the *2007 CPNI Order*, the Commission also explained, for example, that "a carrier that practices willful blindness" regarding unauthorized disclosure of CPNI likely "would not be able to demonstrate that it has taken sufficient measures" to discover and protect against such conduct.[134] And in the same order, the Commission likewise identified the limitations of relying on "contractual safeguards" to address risks once CPNI has been disclosed outside the covered carrier.[135] Ultimately, while providing guidance regarding compliance with section 64.2010, the Commission also recognized that it was necessary to guard against providing bad actors "a 'roadmap' of how to obtain CPNI without authorization."[136] This provides

---

[132] *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

[133] *Id.* at 6959-60, para. 65; *see also*, *e.g.*, *id.* at 6945-46, para. 34 ("we permit carriers to weigh the benefits and burdens of particular methods of possibly detecting pretexting," which "will allow carriers to improve the security of CPNI in the most efficient manner").

[134] *Id.* at 6946, para. 35.

[135] *Id.* at 6952-53, para. 49.

[136] *Id.* at 6959-60, para. 65.

sufficient direction for Verizon to understand its obligations under the rule as relevant here.

41. Thus, Verizon could reasonably have ascertained that (1) any enumeration of CPNI data elements set out by the agency was not exhaustive; (2) the customer location information at issue would be found to meet the definition of CPNI; and (3) Verizon would be subject to forfeiture penalties for failing to protect that customer location information as required under section 222 and the Commission's rules.[137]

C. Verizon Failed to Take Reasonable Steps to Protect CPNI

42. Verizon violated section 222 of the Act and section 64.2010 of our rules by failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information.[138] While our rules recognize that companies cannot prevent all data breaches, the rules require carriers to take reasonable steps to safeguard their customers' CPNI and discover attempts to gain access to their customers' CPNI. Further, as noted below, where an unauthorized disclosure has occurred—as here—the burden of production shifts to the carrier to offer evidence that it did have reasonable measures in place.

---

[137] Accordingly, we reject Verizon's argument that "[n]o carrier "acting in good faith" could have identified "with 'ascertainable certainty'" the NAL's expansive view of CPNI." NAL Response at 38.

[138] 47 CFR § 64.2010(a); *see also 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 ("We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.").

Once the carrier offers some evidence of those safeguards, the rebuttable presumption falls away, and the Commission bears the burden of persuasion and must find by a preponderance of the evidence that the carrier's safeguards were unreasonable in order to find a violation of 47 CFR § 64.2010(a). Verizon contends that the Securus disclosures to Hutcheson did not constitute legal violations of section 222, disputes the timing and scope of those disclosures, and contends that finding a violation of section 222 and the Commission's rules otherwise is unjustified with regard to those disclosures.[139] Verizon then claims that it acted reasonably to protect its customers' location information both before and after the Securus disclosure came to light.[140] Verizon also argues that the Commission improperly shifted the burden of proving that such protections were reasonable to Verizon.[141] We find Verizon's arguments unpersuasive.

1. Verizon's Customer Location Disclosures to Securus Were Unauthorized and Violated Section 222

43. As an initial matter, we conclude that it was not just disclosures to Hutcheson that were unauthorized. Rather, Securus's entire location-finding service[142] (as

---

[139] *See* NAL Response at 19-22, 28-30.

[140] *See* NAL Response at 39-40, 44-56.

[141] *See* NAL Response at 40-44.

[142] *See NAL*, 35 FCC Rcd at 1708-09, paras. 25-26 (citing Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018) https://

detailed in paragraphs 13-14, above) was predicated on unauthorized disclosures.[143] Consistent with Verizon's own description of events, the program was outside the scope of not only its approved use case, but also beyond any agreement with either Aggregator (and thus had not been reviewed by Verizon).[144] Verizon conceded that it was unable to distinguish location requests unrelated to the authorized use case (which involved an inmate collect-calling service) and that the practice did not trigger any review by Aegis.[145] And, to be clear, none of the records submitted in connection with the location-finding service evinced a consumer's actual opt-in consent. Therefore, every time Securus submitted a request for location information under the guise of its approved use case (a use case that required consumer consent) and Verizon provided the requested location information, a separate, unauthorized disclosure occurred.

44. Verizon attempts to avoid this conclusion by: (1) concentrating only on the disclosures made to

---

www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html).

[143] Verizon states that "the NAL does not claim that Verizon disclosed information to Hutcheson—it claims that Securus did." NAL Response at 28. But it was Verizon CPNI that was disclosed, and as the *NAL* explained, "Verizon is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred." *NAL*, 35 FCC Rcd at 1715, para. 52.

[144] *See* LOI Response at 11-12, Response to Question 8; *NAL*, 35 FCC Rcd at 1709, para. 27; *see also*, *e.g.*, NAL Response at 19-21.

[145] *See NAL*, 35 FCC Rcd at 1709-10, 1715, paras. 27-29, 51.

Hutcheson, not on the overall Securus location-finding program;[146] and (2) trying to use section 222(c)(1)'s exception for disclosures that are required by law to shield itself.[147] This misses the larger point. Whether or not there was a legitimate law enforcement request for the information is irrelevant if Verizon did not satisfy its own obligations under section 222. Verizon provided the location information to Securus under Securus's false pretenses, and Verizon only did so because it took Securus at its word that Securus had obtained opt-in consumer consent.[148] This means that Verizon did not review any law enforcement requests and likewise did not provide the information pursuant to a law enforcement request because Verizon did not know there were any law enforcement requests in the

---

[146] *See* NAL Response at 19-22 (raising arguments based on the number of identified disclosures to Hutcheson and the time periods at issue in those identified disclosures); *id.* at 48 (disputing "that the fact that Securus was able to share with Hutcheson the information for a small number of Verizon customers without authorization is evidence that Verizon's program safeguards were inadequate").

[147] *See* NAL Response at 20 n.17 (relying on 47 U.S.C. § 222(c)(1), which allows disclosure of CPNI "as required by law").

[148] As the *NAL* explained, "[t]o the extent that the third parties were *not* acting on behalf of the carrier, the carrier itself would have provided those third parties with access to its customers' CPNI without obtaining for themselves the approval required by section 222(c)(1)—thus violating federal law." *NAL*, 35 FCC Rcd at 1716, para. 54 n.145. Although the *NAL* noted that "Verizon does not appear to argue that situation is present here," *id.*, the totality of the record persuades us that this is, in fact, the import of the facts and Verizon's arguments here.

first place — legitimate or otherwise.[149] Separately and independently, there is no indication that the law enforcement requests were properly reviewed by Securus, as evidenced by the ready success of Hutcheson's thinly veiled ruse.[150] Thus, the disclosures made

---

[149] *See* LOI Response at 11-12, Response to Question 8; *NAL*, 35 FCC Rcd at 1709, para. 27; NAL Response at 19-21. *See also NAL*, 35 FCC Rcd at 1708-09, paras. 25-26 (citing Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018) https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html; Doyle Murphy, *Ex-Missouri Sheriff Cory Hutcheson Sentenced to 6 Months in Prison*, Riverfront Times (Apr. 29, 2019), https://www.riverfronttimes.com/newsblog/2019/04/29/ex-missouri-sheriff-cory-hutcheson-sentenced-to-6-months-in-prison). It is not reasonable to interpret Verizon as having been relying on a third party to disclose information as required by law where Verizon neither knew nor approved of the third party doing so.

[150] *See* Hutcheson Sentencing Memo at 3-4 (explaining that after uploading documents that were blatantly not legal authorizations, location information was immediately transmitted with no intervening time for any documents to be reviewed for validity); *NAL*, 35 FCC Rcd at 1709, para. 26 (describing Hutcheson's uploading of documents that were blatantly not legal authori-zations in order to obtain location information). As the *NAL* explained, "Verizon does not deny the existence of the Securus location-finding service nor the abuse of that system by Hutcheson." *NAL*, 35 FCC Rcd at 1709, para. 27. Verizon likewise does not dispute here that Hutcheson was, as a general matter, able to access location data by providing documents that were blatantly not legal authorizations as described in the *NAL* and confirmed in the Hutcheson Sentencing Memo. It at most asserts that there conceivably might have been legal authorizations associated with the specifically-identified Verizon customers, *see* NAL Response at 20 n.17, but does provide any reason to believe that Securus (let alone Verizon) could have or would have made that assessment before providing the location data.

to Hutcheson were doubly unauthorized under section 222(c)(1). First, Securus used the façade of their approved use case to hide the true purpose and destination of the request, resulting in Verizon's unauthorized disclosure of location information to Securus. Second, Hutcheson likewise submitted blatantly fake requests to Securus under the guise of law enforcement, resulting in Securus's unauthorized disclosure of location information to Hutcheson.[151] Despite Verizon's arguments, the Company is clearly not "required by law" to disclose location information based on any and every pretense or unsupported request. Therefore, consistent with the *NAL*, we find that the Securus disclosures, including those made to Hutcheson, were unauthorized.

45. We thus conclude that Verizon was appropriately admonished in relation to such disclosures.[152] In objecting to the admonishment, Verizon criticizes the approach of finding a violation of section 222 when there is an unauthorized disclosure of CPNI as in-consistent with the limits of carriers' practical ability to prevent

---

[151] *See* Hutcheson Sentencing Memo at 3-4 (Hutcheson "uploaded legally defective search warrants that either did not authorize the acquisition of location data, were unsigned, or had no connection to the targeted phone user" and in "most of these instances . . . even notarized his own signature."); *see also NAL*, 35 FCC Rcd at 1709, para. 26.

[152] Among other things, Verizon argues that it would not have satisfied the willfulness requirement that is a prerequisite for a forfeiture under section 503(b) of the Act. *See* NAL Response at 28-29. Given that we do not impose a forfeiture for that conduct here, we need not address Verizon's arguments in that regard.

all unauthorized disclosures,[153] and as "contrary to the current CPNI rules, which enshrine a reasonableness approach to CPNI issues."[154] But Verizon fails to grapple with the text of the restriction on unauthorized use or disclosure in section 222(c)(1) of the Act and section 64.2007(b) of the Commission's rules.[155] Rather than incorporating some kind of *de minimis* exception or reasonableness standard, section 222(c)(1)'s statutory restriction on use and disclosure is unequivocal, as likewise reflected in section 64.2007(b) of the Commission's rules.[156] Against that backdrop, we also are not persuaded that the admonishment causes unfair surprise to Verizon, even assuming *arguendo* that such a standard applied to an admonishment here.

2. Verizon's Protection of Customer Location Information Was Unreasonable Both Before and After the Securus/Hutcheson Disclosures

46. The Commission affirms the *NAL* and finds that Verizon failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information. As fully laid out in the *NAL*, the record not only shows that Verizon did not have reasonable protections in place prior to 2018 *New York Times* article detailing the

---

[153] *See* NAL Response at 29.

[154] NAL Response at 29-30 (citing 47 CFR § 64.2010(a)).

[155] 47 U.S.C. § 222(c)(1); 47 CFR § 64.2007(b).

[156] We note that Verizon does not contend that it literally would not have been possible to avoid the disclosures, so our interpretation does not demand the impossible of Verizon or any other carrier.

Securus/Hutcheson breaches,[157] but also that Verizon failed to promptly address its demonstrably inadequate CPNI safeguards after Securus/Hutcheson disclosure.[158]

47. Verizon attempts to excuse its unreasonable practices by cataloging the steps it did take before and after the *New York Times* article. Verizon argues that, prior to the Securus disclosure, its efforts conformed to the CTIA Guidelines for ensuring customer consent to the use of location data.[159] Specifically, Verizon states that its safeguards included: "vetting and conducting ongoing monitoring of third-party program participants; limiting the sharing of information to certain, preapproved use cases; imposing information security requirements and adherence to industry best practices; reviewing notice and consent language; requiring production of consent records on a daily basis; and retaining Aegis to review those consent records, analyze

---

[157] *See NAL*, 35 FCC Rcd at 1717-21, paras. 58-73. Verizon disputes the relevance of the reasonableness of Verizon's procedures prior to the Securus and Hutcheson breaches, *see* NAL Response at 45 n.37, but Verizon neglects the fact that its post-breach procedures largely consist of those very same procedures, with only limited changes of potential relevance here.

[158] *See NAL*, 35 FCC Rcd at 1721-24, paras.74-82.

[159] *See* NAL Response at 54. To the extent that Verizon seeks to defend its actions by claiming that it attempted to ensure consumers provided opt-in consent, *see* NAL Response at 39-40, that aspiration is meaningful here only insofar as Verizon employed reasonable procedures to carry that out. Consistent with the *NAL*, and for the reasons explained below, we conclude that it did not.

program data to find any potential issues, and otherwise monitor the program."[160]

48. The safeguards that Verizon had in place before the Securus disclosure were not reasonable. The CTIA guidelines focus on best practices for notice and consent by location-based service providers—but they do not include best practices recommendations for carriers that sell access to their customers' location information to location-based service providers.[161] For example, they do not offer guidance to carriers on how to assure that location-based service providers comply with a contractual obligation to access location information only after furnishing proper notice and receiving customer consent (which was at issue here). Further, to enforce the safeguards Verizon did use, the Company's efforts "apparently mainly consisted of analysis of unverified vendor-created consent records,"[162] and we agree with the *NAL* regarding those efforts' shortcomings.[163] Although Verizon criticizes aspects of the analysis in the *NAL* and states that it also "used methods for discovering and addressing falsified transaction and consent records in connection

---

[160] NAL Response at 46. The *NAL* also explained that the fact that Verizon provided access to "coarse" location data does not render its procedures reasonable. *NAL*, 35 FCC Rcd at 1720-21, para. 71. We agree with that assessment, which Verizon does not appear to dispute here.

[161] *See* CTIA, Best Practices and Guidelines for Location Based Services, https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services.

[162] *See NAL*, 35 FCC Rcd at 1721, para.72.

[163] *NAL*, 35 FCC Rcd at 1718-20, paras. 64-67.

with the location aggregator program that were *not* reliant only on the accuracy of what third parties submitted,"[164] we nonetheless conclude that the resulting measures employed were not reasonable. Critically, as explained in the *NAL*:

> The unauthorized service did not collect consents from Verizon's customers—just the opposite. When working as intended, Securus's unauthorized program collected electronic copies of legal process asserting a right to obtain location information *without the knowledge or consent of the Verizon customer*. A system allegedly designed to monitor customer consents but that is incapable of detecting its opposite is not a "reasonable measure" to detect unauthorized uses of or access to CPNI.[165]

Whatever risks Verizon's measures might have guarded against in other respects,[166] we conclude that measures with such a significant loophole are unreasonable under section 64.2010(a).

49. Given our finding of significant shortcomings in the measures Verizon employed, we reject Verizon's other criticisms of the analysis in the *NAL*. For one, Verizon seeks to characterize the Securus and Hutcheson breaches as outliers,[167] contending "[t]he fact that

---

[164] NAL Response at 47.

[165] *NAL*, 35 FCC Rcd at 1720, para. 70.

[166] *See* NAL Response at 48 (observing that "the NAL also expressly acknowledges instances in which Verizon's program safeguards identified and addressed other potential issues.").

[167] *See* NAL Response at 48-50.

Verizon's safeguards evidently prevented any unauthorized access by any other program participant or any impact on any other customer demonstrates that those safeguards were both reasonable and effective."[168] Verizon also criticizes the Commission's consideration of an internal Verizon analysis of its safeguards in the *NAL*,[169] characterizing that internal analysis as having identified a merely theoretical risk "that program participants . . . could have submitted falsified location requests or consent records" while seeking to rely on the report's assertion that "'[i]t is unlikely any current program companies are performing fraudulent activities to obtain [Verizon] subscriber information without their consent due to the program management processes and oversight that is in place today.'"[170] Notably, however, Verizon's measures were not what identified the unauthorized disclosures in the case of Securus and Hutcheson. Thus, in the face of what we see as the failing in a fundamental aspect of Verizon's safeguards, we reject the theory that the reasonableness of those measures can be inferred from the fact that even more unauthorized disclosures have not been publicly identified.

50. Verizon also contends that the *NAL* misinterpreted information about what were merely preliminary results of the Aegis record reconciliation program, and that this misinterpretation led the Commission to question what those results signified for the

---

[168] NAL Response at 50.

[169] *See* NAL Response at 46-47.

[170] NAL Response at 47.

effectiveness of Verizon's measures.[171] But the *NAL* made clear that it understood the relevant results flowed just from Aegis' "initial attempts to match the consent and access records," and recognized that, as an effort 'to track down how well the Location Aggregators were fulfilling their record-keeping obligations,'" it provided reason for concern.[172] Verizon's contention that Aegis ultimately could, with enough time and additional investigation, identify supporting consent records where it looked for them,[173] does not undermine the questions about the reliability of the LBS providers in following the contractual requirement—or of the strength of those contractual requirements—for ensuring that prior customer notice and consent was provided and obtained.[174] While Verizon's explanation makes the case that its measures did provide some protection as to some potential risks, viewed in its totality we nonetheless find Verizon's measures unreasonable for the reasons described here.

51. And to the extent that Verizon raises broader objections to the process for developing the record, particularly before the issuance of the *NAL*, those claims

---

[171] *See* NAL Response at 48 n.39.

[172] *NAL*, 35 FCC Rcd at 1719-20, para. 68.

[173] *See* NAL Response at 15-16. In a small number of cases, Aegis relied on sampling rather than comprehensively looking for supporting consent records. *See* NAL Response at 16.

[174] *See*, *e.g.*, *NAL*, 35 FCC Rcd at 1719-20, para. 68 (noting that there could be significant variation in the initial results among different LBS providers and that Verizon itself looked to the results of Aegis' initial attempts to verify consent to identify whether there was cause for concern).

do not alter our analysis either.[175] Verizon had ample opportunity to present evidence and arguments in response to the *NAL*, and our conclusions here are based on what we know about the measures Verizon employed—not based on questions or uncertainty about how those safeguards operated.

52. Likewise, Verizon's safeguards after the Securus disclosure were also unreasonable. Verizon should have been keenly aware of the inadequacy of its safeguards after the May 2018 *New York Times* article. Nonetheless, Verizon did not and cannot demonstrate that its safeguards were made reasonable in the months that followed the 2018 *New York Times* article. In fact, rather than promptly implementing reasonable safeguards, Verizon continued to sell access to its customers' location information under (for all intents and purposes) the *same system* that was exploited by Securus and Hutcheson.[176]

53. We reject Verizon's attempt to dispute that the reports of the Securus and Hutcheson breaches should have made Verizon aware of the need for greater safeguards beyond cutting off Securus.[177] In particular, Verizon cites its theory that the location information is not CPNI and its view that the Securus/Hutcheson disclosures was a limited, outlier situation that did not raise broader questions about the efficacy of its safeguards.[178] As explained above, however, the location

---

[175] *See* NAL Response at 26, 48 n.39.

[176] *See NAL*, 35 FCC Rcd at 1721, para.74.

[177] *See* NAL Response at 50-52.

[178] *See* NAL Response at 50-52.

information is, in fact, CPNI.[179] And as explained earlier in this section, the Securus and Hutcheson breaches revealed fundamental shortcomings in Verizon's safeguards, rather than only demonstrating the sort of narrow, limited problems that Verizon claims. We therefore conclude that Verizon should have known of the inadequacies in its safeguards and the need for significant changes after the May 2018 *New York Times* article. Indeed, notwithstanding its arguments here, Verizon itself did, in fact, recognize the need to take steps in the wake of that article, ultimately including ending its location-based services initiative.[180]

54. Although Verizon explored implementing an enhanced direct notice and consent mechanism, this approach did not extend beyond the exploratory stage.[181] Likewise, Verizon touts the fact that after the May 2018 *New York Times* article "Verizon actually did decide within 30 days to terminate the program entirely," although it took a longer period of time to effectuate that decision.[182] But the mere fact that Verizon was

---

[179] *See supra* section III.A.

[180] *See* NAL Response at 21-25.

[181] *See* NAL Response at 53.

[182] NAL Response at 51. Verizon argues that "the Commission never before set out specific requirements that a carrier must take in response to a third party's unauthorized access to location data, much less announced a hard-and-fast 30-day deadline by which any specific action must be taken." *Id.* at 8. The 30-day period cited in *NAL* was not a deadline but a grace period during which the Commission used its discretion and did not assess a fine. However, Verizon's existing data security practices were unreasonable both before and after the May 2018 article—the article merely exposed those unreasonable

working on possible alternative processes or had not-yet-implemented plans to end its location aggregator initiative is not sufficient to satisfy its obligation to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[183] Until the new measures actually are in place, or the initiative actually terminated, they cannot enable a carrier to "discover and protect against" the harms that are the target of that rule—and thus, they cannot be relied upon to satisfy that rule. Nor does the time and effort involved in Verizon's work on the exploratory processes or on terminating the location aggregator initiative render the procedures that remained in place in the meantime "reasonable" under that rule, given their glaring weaknesses.

55. We also are unpersuaded that the steps Verizon did take were reasonable. Verizon cut off 3CI and Securus and declined to allow access to location information for additional LBS providers and use cases,[184] but those actions did not improve the safeguards for consumers whose location information could be disclosed under the location data sharing arrangements that remained in place. Verizon also contends that it had Aegis review the vetting procedures and data

---

practices. As such, the Commission could have assessed a fine *for every single day* such unreasonable practices were in place (both before and after the Securus/Hutcheson disclosures)—the 30 days provided Verizon with a grace period to either end the program or reform its practices.

[183] 47 CFR § 64.2010(a).

[184] *See*, *e.g.*, NAL Response at 21, 24, 51.

analytics used.[185] But the only changes Verizon claims actually were implemented were having Aegis "strengthen the transaction verification process to identify any anomalies in the data relating to consent requests that could indicate a potential issue, such as multiple location requests within a 24-hour period or an increase in location requests that were out of the ordinary for a particular LBS provider."[186] But nothing Verizon has said, nor anything in the record, gives the Commission any reason to believe that those particular measures were likely to have identified the problem that enabled the Securus and Hutcheson breaches in the first place. In particular, Verizon identified reasons why Aegis' regular auditing did not identify the Securus and Hutcheson breaches,[187] and we are not persuaded that the newly implemented measures would have remedied those shortcomings. Further, Verizon does not identify the timing of when those

---

[185] *See* NAL Response at 52-53; NAL Response, Exh. A, Brunner Supplemental Decl. at para. 11.

[186] NAL Response at 52.

[187] Verizon explained, for example, that Aegis' regular auditing "likely did not alert Aegis to a potential problem because: (i) Securus was using its profile for the approved use case to access location information for unauthorized purposes; (ii) nothing changed in the background check that Aegis maintained for Securus that would have prompted Aegis to question Securus's credibility about following approved use cases; (iii) the number of location requests from Securus was consistent with the number that Aegis would expect from it (i.e., there were no spikes in data to raise a red flag); and (iv) the number of impacted Verizon customers was so small (and apparently only within two relatively limited time spans)." NAL Response at 22 (emphasis in original).

measures were implemented, and while other steps were considered the record does not reveal whether or when they ultimately were implemented at all. Thus after considering all of the data security measures that Verizon implemented in response to the Securus disclosure[188] we conclude that these measures were inadequate.

56. Verizon further argues that the Commission fails to appropriately account for the fact that many location-based services are "beneficial services that Verizon's customers affirmatively wanted."[189] We disagree. The issue here is not whether there are any beneficial services offered by LBS providers, but whether Verizon reasonably protected its customers' location information. In any event, because of the sensitive personal information involved, the benefits of LBS must be weighed against the risks; here, the risks were grave, particularly because Verizon did not have a reliable way of confirming customer consent. The Commission considered Verizon's arguments, but finds they are outweighed by these risks.

57. The *NAL* listed numerous steps that could have been taken to squarely address the proven vulnerability, up to and including deploying enhanced measures to verify consumer consent (even directly verifying consumer consent) and shutting down the LBS program.[190] Rather than taking definitive steps to remedy the obvious LBS program issues, Verizon instead took

---

[188] *See* NAL Response at 21-25, 50-54.

[189] NAL Response at 51.

[190] *See NAL*, 35 FCC Rcd at 1721-23, paras. 75-79.

piecemeal steps. Moreover, the steps Verizon took did not rectify the systemic vulnerabilities at the heart of its LBS program—including relying on third parties to obtain customer consent for the disclosure of location information and failing to verify the validity of that consent.

58. Verizon's attempts to characterize the Commission as relying on an extreme strict liability-type approach fall short, as well.[191] We agree with Verizon that section 64.2010 of the Commission's rules requires only reasonable measures—not perfect ones—but that is not enough to help Verizon here.[192] Contrary to Verizon's suggestion, this is not a situation where the Commission is relying on 20/20 hindsight after a breach to find a violation of section 64.2010(a) of the rules based on any shortcoming in a carrier's measures, no matter how small, that results in a strict liability approach that is contrary to the reasonableness standard reflected in that rule.[193] Rather, we have carefully examined Verizon's procedures, including the fundamental flaw that while Verizon's "system allegedly designed to monitor customer consents [it was] incapable of detecting its opposite."[194] Our assessment under section 64.2010(a) thus is a straightforward evaluation of reasonableness, consistent with the text of the rule.

---

[191] *See* NAL Response at 46, 48-50, 54-56.

[192] *See* NAL Response at 49, 54-55.

[193] *See* NAL Response at 54-55.

[194] *NAL*, 35 FCC Rcd at 1720, para. 70.

3. Verizon Bore the Burden of Production

59. As an initial matter, the Commission notes that for the reasons discussed above and the analysis contained in the *NAL*, the preponderance of the evidence shows that Verizon did not use reasonable safeguards throughout the period of the violation.[195] As such, while the *NAL* discussed Verizon's burden of production to demonstrate that its protection of customer CPNI was reasonable,[196] that burden-shifting is not necessary given the preponderance of the evidence. Nonetheless, even if unnecessary to prove Verizon's violations in this matter, the *NAL* properly shifted the burden of production to Verizon.

60. *First*, as the *NAL* explained[197] and consistent with the *2007 CPNI Order*, where there is evidence of an unauthorized disclosure, the Commission will infer from that evidence that a carrier's practices were unreasonable unless the carrier offers evidence demonstrating that its practices were reasonable.[198] In the

---

[195] *See NAL*, 35 FCC Rcd at 1717-24, paras.58-82.

[196] *See NAL*, 35 FCC Rcd at 1701-02, 1717, 1722, paras. 8, 59, 60, 76.

[197] *See NAL*, 35 FCC Rcd at 1701-02, para. 8.

[198] *See 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 63 (noting that where there is evidence of an unauthorized disclosure, the Commission "will infer . . . that the carrier did not sufficiently protect that customer's CPNI" and that "[a] carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue").

NAL, the Commission found that Verizon failed to demonstrate that its safeguards were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018.[199]

61. Verizon acknowledges that the *NAL* based its approach on the *2007 CPNI Order*,[200] explaining that "where an unauthorized disclosure has occurred . . . the responsible carrier then shoulders the burden of proving the reasonableness of its measures to protect consumer data."[201] However, Verizon is incorrect when it asserts that the *2007 CPNI Order* cannot support the burden-shifting approach in cases outside of the pretexting context.[202] The *2007 CPNI Order* afforded adequate notice of the application of burden-shifting in this case. The order did not expressly limit burden-shifting to the pretexting context, instead applying more broadly to unauthorized disclosures of CPNI. The rationale applies with equal force to the kind of disclosure at issue here, where a fundamental issue is whether Verizon had reasonable measures to ensure that its customers had in fact consented to the disclosure of their CPNI. Indeed, the breach in the instant case is analogous to pretexting in that it involved fraud

---

[199] *See NAL*, 35 FCC Rcd at 1717-24, paras. 58-82.

[200] *See* NAL Response at 43 (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*)).

[201] *NAL*, 35 FCC Rcd at 1717, para. 59.

[202] *See* NAL Response at 43.

in order to obtain access to CPNI.[203] Broadly, in relation to Securus's entire unauthorized location-finding service, Securus used the pretext that it was requesting location information from Verizon for its approved use case and that it had explicit customer opt-in consent for the disclosure. Likewise, Hutcheson used the pretext that he had legal authorization or consumer consent when requesting location information from Securus.[204] Therefore, applying the burden-shifting to this case is appropriate even to the extent that the disclosures here could be said not to have been pretexting of the same form described in the *2007 CPNI Order*.

62. *Second*, Verizon admits that an evidentiary presumption is valid if the circumstances (here, a breach of CPNI) giving rise to that presumption make it "more likely than not" that the presumed fact (here, that CPNI safeguards were unreasonable) exists.[205] The Commission finds that the unauthorized disclosure in this case gave rise to a rebuttable presumption that Verizon did not reasonably protect customer location

---

[203] The breach at issue here arguably falls within the letter of criminal pretexting. *See* 18 U.S.C. § 1039.

[204] As explained in the *NAL*, "Hutcheson submitted thousands of unauthorized location requests via the Securus service between 2014 and 2017, in some cases 'upload[ing] entirely irrelevant documents including his health insurance policy, his auto insurance policy, and pages selected from Sheriff training manuals" in lieu of genuine legal process.'" *NAL*, 35 FCC Rcd at 1709, para. 26; *see also supra* para. 14 (citing Hutcheson Sentencing Memo).

[205] *See* NAL Response at 42.

information from unlawful access.[206] As already discussed, the entire Securus location-finding program was based upon unauthorized disclosures. Though the disclosures to Hutcheson were particularly egregious (given they were essentially doubly unauthorized), *all* of the Securus requests made under the false guise of the approved use case and Verizon's resultant disclosures of consumer location information were unauthorized. Verizon's existing safeguards and oversight failed to notice and (absent the *New York Times* article) may have never realized that the unauthorized Securus location-finding program existed. Nonetheless, Verizon argues that the Commission cannot use the Securus and Hutcheson breaches to support shifting the burden of production to Verizon to provide evidence of the reasonableness of their post-May 2018 security practices.[207] Specifically, Verizon asserts that because no provider can achieve perfection, "a single unauthorized disclosure of CPNI is a manifestly poor predictor of the reasonableness of a carrier's measures to safeguard CPNI," thus undercutting the reasonableness of any burden shifting here.[208] We disagree.

---

[206] *See 2007 CPNI Order*, 22 FCC Rcd at 6929, 6959, paras. 3, 63. A presumption is only permissible if there is "a sound and rational connection between the proved and inferred facts," and when "proof of one fact renders the existence of another fact so probable that it is sensible and timesaving to assume the truth of [the inferred] fact . . . until the adversary disproves it." *Chemical Mfrs. Ass'n v. Department of Transp.*, 105 F.3d 702, 705 (D.C. Cir. 1997) (quoting *NLRB v. Curtin Matheson Scientific, Inc.*, 494 U.S. 775, 788-89 (1990)) (internal citation and quotation marks removed).

[207] *See* NAL Response at 42-44.

[208] NAL Response at 43.

63. In the *NAL*, we found that Verizon apparently violated section 222(c) of the Act and section 64.2007(b) of our rules in connection with its un-authorized disclosures of CPNI to Hutcheson.[209] This is further bolstered by the Department of Justice's case against Hutcheson.[210] And though the Commission opted to admonish Verizon only for the unauthorized disclosures made to Hutcheson, it would have been appropriate to admonish Verizon for all the disclosures it made to Securus in relation to the unauthorized location-finding service. In the *NAL*, we clearly explained that, pursuant to section 217 of the Act,[211] carriers cannot disclaim their obligationsto protect customer CPNI by delegating those obligations to third parties.[212] In its NAL Response, Verizon does not dispute that a "third-party LBS provider in the location aggregator program breached its contractual obligations and—without Verizon's knowledge or approval—apparently shared Verizon customer location data with an unauthorized party

---

[209] *See NAL*, 35 FCC Rcd at 1714, para. 49. "The evidence reflects that Hutcheson used the Securus service to obtain the location information of Verizon customers. Verizon shared the information with LocationSmart, which the shared it with 3Cinteractive, which then shared it with Securus . . . ." *Id.* at 1714, para. 50.

[210] *See*, *e.g.*, Hutcheson Sentencing Memo.

[211] 47 U.S.C. § 217.

[212] *See NAL*, 35 FCC Rcd at 1702, para. 9. Under section 217, "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 § 217.

for an unauthorized purpose" in providing location data to Hutcheson.[213] We reiterate here that "Verizon is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred."[214] Further, section 222(c)(1) of the Act[215] makes the responsibility for avoiding unauthorized disclosures a carrier obligation and prohibits use and disclosure except in certain narrow circumstances, without any reasonableness criterion. Verizon should, therefore, be able to justify any unauthorized disclosure. Given that multiple breaches occurred here and that the "reasonable measures" obligation is a *continuing* obligation, the Commission's application of an evidentiary presumption based upon

---

[213] *See* NAL Response at 18. Verizon argues that Hutcheson's unauthorized location lookups, which they concede apparently violated Securus's legal obligations including safeguarding its customers' CPNI, did not violate the Act or the Commission's rules insofar as the information was shared as required by law under section 222(c)(1). *Id.* at 20 n.17. We find Verizon's argument unavailing. Although Verizon speculates that some of the lookups may have had a law enforcement basis, those lookups were certainly not submitted through the appropriate channels for law enforcement requests, and Verizon cannot now claim that they were "required by law" when it did not treat them as such in the first place. Further, as explained in the *NAL*, "Securus did not . . . assess the adequacy of the purported legal authorizations submitted by users of its location-finding service." *NAL*, 35 FCC Rcd at 1708, para.25.

[214] *See NAL*, 35 FCC Rcd at 1715, para.52; *see also id.* at 1716, para. 54 n.145 (explaining that where a carrier makes disclosures to a third party where the third party is not acting on behalf of the carrier to fulfill the relevant responsibilities of the carrier under section 222, the carrier's disclosure of CPNI to the third party would be unauthorized in violation of section 222(c)(1)).

[215] 47 U.S.C. § 222(c)(1).

the disclosures involving Hutcheson and the imposition of a burden to produce evidence of reasonable protections during the relevant violations period was reasonable—particularly because, as discussed, those safeguards did not materially change in the interim timeframe.

64. *Third*, Verizon misinterprets the *NAL* when it argues that the Commission improperly shifted the burden of persuasion to the Company.[216] To the contrary, the Commission properly (and consistent with APA precedent) shifted only the burden of *production*, and not the burden of *persuasion*, to Verizon. The unauthorized disclosure at issue gave rise to a rebuttable presumption that Verizon did not adequately protect customer information from unlawful access. The burden of production then shifted to Verizon to offer evidence that it had reasonable safeguards in place.

65. Rather than taking reasonable steps to safeguard its customers' location information after the Securus/Hutcheson disclosures were reported,[217] Verizon placed its customers' location information at continuing risk of unauthorized access through its failure to terminate its program or impose reasonable safeguards to protect its customers' location information. For these reasons, we conclude that Verizon failed in its obligation under section 222 and our rules to have reasonable measures in place to discover and protect

---

[216] *See* NAL Response at 40-42.

[217] Many of the possible reasonable steps were enumerated in the *NAL*. *See NAL*, 35 FCC Rcd at 1721-23, paras. 75-79.

against attempts to gain unauthorized access to its customers' CPNI.

D. The Forfeiture Amount is Lawful and Consistent with FCC Precedent

66. After considering the evidence in the record, the relevant statutory factors, the Commission's *Forfeiture Policy Statement*, and the arguments advanced by Verizon in the NAL Response, we find that Verizon is liable for a total forfeiture of $46,901,250 for its violations of section 222 of the Act and section 64.2010 of the Commission's rules—a reduction of $1,417,500 from the $48,318,750 forfeiture proposed in the *NAL*.[218] As explained in the *NAL*, this figure resulted from applying a base forfeiture of $40,000 for the first day of each such violation and a $2,500 forfeiture for the second and each successive day the violations continued (excluding the 30-day grace period granted by the Commission).[219] The Commission found in the *NAL* that Verizon apparently engaged in 65 continuing violations—one for each ongoing relationship with a third-party LBS provider or aggregator that had access to Verizon customer location information more than 30 days after publication of the *New York Times* report—and that each violation continued until Verizon terminated the corresponding entity's access to customer

---

[218] Any entity that is a "Small Business Concern" as defined in the Small Business Act (Pub. L. 85-536, as amended) may avail itself of rights set forth in that Act, including rights set forth in 15 U.S.C. § 657, "Oversight of Regulatory Enforcement," in addition to other rights set forth herein.

[219] *NAL*, 35 FCC Rcd at 1726, para. 86.

location information.[220] Using this meth-odology, the Commission found Verizon apparently liable for a total base forfeiture of $32,215,500. Upon considering the nature of the violations and the risk of harm they posed to consumers, the Commission then applied a 50% upward adjustment to the base forfeiture amount, resulting in a total proposed forfeiture of $48,318,750.[221]

67. Verizon challenges these forfeiture calculations with five principal arguments. *First*, Verizon asserts that it did not engage in any "willful" violations and suggests that any forfeiture penalty should take such non-willfulness into account.[222] *Second*, Verizon claims that it would be arbitrary and capricious to impose a forfeiture under section 222 when there had been no unauthorized disclosures during the limitation period.[223] *Third*, Verizon argues that the NAL describes at most a single continuing violation, not a separate violation for each of the 65 entities participating in Verizon's LBS program. As such, according to Verizon, the forfeiture exceeds the applicable statutory maximum.[224] *Fourth*, Verizon argues that even if the Commission could calculate the forfeiture based upon the number of LBS providers and how long they had access to customer location information, the proposed forfeiture relies upon incorrect facts and therefore is

---

[220] *NAL*, 35 FCC Rcd at 1726, para. 87.

[221] *NAL*, 35 FCC Rcd at 1727-28, paras. 90-93.

[222] NAL Response at 56.

[223] NAL Response at 56-57.

[224] NAL Response at 57-587.

calculated incorrectly. Specifically, Verizon states that a number of LBS program participants ceased accessing Verizon customer location information before the dates identified in the *NAL*, and two of them never actually participated in the program in the first place.[225] *Fifth* and finally, Verizon challenges the Commission's application of a 50% upward adjustment to the base forfeiture, claiming both that it rests upon a misunderstanding of an internal Verizon document and that it impermissibly cites to the same factors used for determining the base forfeiture amount.[226]

68. As we discuss below, to account for the non-participation in Verizon's LBS program of two entities that were included in the original forfeiture calculation, we reduce the forfeiture proposed in the *NAL* by $1,417,500. However, we are not persuaded by any of Verizon's other arguments and decline to cancel or further reduce the forfeiture proposed in the *NAL*.

1. Verizon Willfully Violated the Act and the Commission's Rules

69. According to Verizon, the *NAL* does not establish that it engaged in "willful" violations of section 222 and the Commission's rules. Verizon asserts that because it took steps to safeguards its customers' information and "did not consciously or deliberately fail to act to protect CPNI," it cannot be said to have "willfully" violated any requirement.[227] Thus, Verizon

---

[225] NAL Response at 57-58.

[226] NAL Response at 57-58.

[227] NAL Response at 56.

maintains, the *NAL* in actuality bases the penalty on section 503(b)'s "repeated" prong, and any forfeiture should reflect that.

70. These arguments lack merit. The term "willful," as used in section 503(b) of the Act, does not have the restrictive meaning that Verizon would assign to it. As the Commission has previously stated:

> . . . the word "willfully", as employed in Section 503(b), does not require a showing that the [party] knew he was acting wrongfully; it requires only that the Commission establish that the licensee knew that he was doing the acts in question — in short, that the acts were not accidental (such as brushing against a power knob or switch).[228]

71. Verizon's invocation of *Telrite*, which provides that a violation is "willful" if it involves "'the conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate' the law,"[229] does not persuade us otherwise. As *Telrite* provides, the issue is not whether Verizon *intended* to violate the law, but whether it deliberately engaged in the acts or omissions that the Commission found to have constituted an apparent violation of the law. Verizon does not dispute that it designed, implemented, and operated its LBS

---

[228] *Midwest Radio-Television Inc.*, *Memorandum Opinion and Order*, 40 F.C.C. 163, 167, para. 11 (1963). *See also Playa Del Sol Broadcasters*, Order on Review, 28 FCC Rcd 2666, 2667-68, paras. 4, 6 (2013); *USA Teleport, Inc.*, Memorandum Opinion and Order, 26 FCC Rcd 6431, 6434, para. 9 (EB 2011).

[229] NAL Response at 28 (citing *Telrite Corp.*, Notice of Apparent Liability for Forfeiture & Order, 23 FCC Rcd 7231, para. 12 (2008) (quoting 47 U.S.C. § 312(f)(1)) (alteration in original)).

program or that it is responsible for that program's structure and performance. Therefore, because the Commission found that the safeguards that Verizon had in place for customer location information—as consciously and deliberately implemented by Verizon—did not meet the requirements of section 222 of the Act and section 64.2010 of the Commission's rules, then Verizon "willfully" violated those provisions.

72. Furthermore, as Verizon acknowledges, section 503(b) applies when a carrier "willfully *or* repeatedly" fails to comply with an applicable requirement,[230] and does not require that both prongs of the clause be met. Thus, even if Verizon had not engaged in "willful" violations, a forfeiture penalty under section 503(b) still would be appropriate. But, as discussed, Verizon's failure to have reasonable protections in place for customer location information was "willful" for purposes of section 503. And, by continuing to operate its LBS program in the absence of reasonable safeguards, Verizon both willfully and repeatedly[231] violated section 222 of the Act and section 64.2010 of the Commission's rules.

2. The Commission Did Not Need to Find Unauthorized Access to CPNI During the Limitations Period

---

[230] 47 U.S.C. § 503(b)(1)(B) (emphasis added).

[231] For the purposes of section 503, "repeated" only requires that a party acted (or failed to act) more than once or, if the act or failure to act is continuous, for more than one day. *See*, *e.g.*, *Playa Del Sol Broadcasters*, Order on Review, 28 FCC Rcd 2666, 2668, para. 4 (2013).

73. Verizon challenges as arbitrary and capricious the imposition of a forfeiture penalty for when there has been no "actionable unauthorized disclosure" and claims that, at a minimum, the Commission should have taken this into account when setting the base forfeiture.[232] Verizon also contends that the base forfeiture amounts of $40,000 for the first day of a violation and $2,500 for the second and each successive day that the violation continued are so excessive as to be arbitrary and capricious given that, among other considerations, no unauthorized disclosure occurred during the limitations period.[233]

74. We reject this argument. The forfeiture here is based not upon any unauthorized disclosures (which, in the case of Hutcheson, occurred outside the limitations period) but rests upon Verizon's subsequent conduct—namely, how "[a]fter learning of Hutcheson's practices, Verizon placed its customers' location information at continuing risk of unauthorized access through its failure to expeditiously terminate its program or impose reasonable safeguards to protect its customers' location information."[234]

75. Moreover, with respect to the specific amounts chosen for the base forfeiture, these figures were neither excessive nor arbitrary and capricious, but reflected the Commission's careful consideration of the relevant statutory factors. Section 503 of the Act requires the Commission to ". . . take into account the

---

[232] NAL Response at 56-57.

[233] NAL Response at 56-57.

[234] *NAL*, 35 FCC Rcd at 1724, para. 82.

nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[235] The plain language of the statute provides the Commission with broad discretion to assess proposed penalties based on the statutory factors, up to the statutory maximum.

76. In selecting the base forfeitures that it did, the Commission explained that the chosen amounts "(1) . . . provide a meaningful distinction between the violations in this case and those of other cases involving less egregious facts; and (2) . . . provide consistency with other consumer protection cases involving serious harm to consumers."[236] The Commission also found that "this base forfeiture appropriately deters wrongful conduct and reflects the increased risk consumers face when their information is not secured in a timely manner."[237] Given the broad discretion afforded to the Commission under section 503, as well as the *NAL*'s examination of how the relevant statutory factors intersected with the facts of this case, we reject Verizon's claim that the Commission acted arbitrarily or capriciously in setting the base forfeiture amount.

3. The Commission Reasonably Found that Verizon Engaged in 65 Continuing Violations

---

[235] 47 U.S.C. § 503(b).

[236] *NAL*, 35 FCC Rcd at 1726, para. 86.

[237] *NAL*, 35 FCC Rcd at 1726, para. 86.

77. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against Verizon of up to $204,892 for each day of a continuing violation, up to a statutory maximum of $2,048,915 "for any single act or failure to act."[238] The Commission found that, because Verizon permitted 65 separate entities to access its customers' location information in the apparent absence of reasonable safeguards, the Company engaged in 65 continuing violations of section 222 of the Act and section 64.2010 of the Commission's rules. Verizon challenges this methodology, arguing that "[e]ither Verizon took reasonable measures with respect to the location aggregator program, or it did not," and contends that "the number of entities is irrelevant to that analysis."[239] Verizon therefore asserts that there could have been at most one continuing violation (subject to the $2,048,915 penalty cap) and the *NAL*'s finding of 65 separate continuing violations (one for each LBS provider or Aggregator) constitutes an impermissible attempt to circumvent the statutory maximum.[240]

78. We reject this argument. Neither section 503(b) nor the forfeiture guidelines in section 1.80 of the Commission's rules speak to the application of the phrase

---

[238] *See* 47 U.S.C. § 503(b)(2)(B); 47 CFR § 1.80(b)(2). These amounts reflect inflation adjustments to the forfeitures specified in section 503(b)(2)(B) ($100,000 per violation or per day of a continuing violation and $1,000,000 per any single act or failure to act). *See Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 19-1325 (EB 2019).

[239] NAL Response at 57.

[240] NAL Response at 58.

"single act or failure to act," or otherwise to the calculation of the number of violations, in the CPNI or data security context.[241] Moreover, in calculating a proposed penalty under section 222, the Commission previously applied a methodology under which a systemic failure to protect customer information constituted significantly more than a single violation. In *TerraCom*, the Commission stated that "[e]ach document containing [[[proprietary information] that the Companies failed to protect constitutes a separate violation for which a forfeiture may be assessed."[242] The Commission further observed that "[e]ach un-protected document constitutes a continuing violation that occurred on each of the 81 days [until] the date that the Companies remedied the failure . . . ."[243]

79. The Commission in *TerraCom* elected to ground its forfeiture calculation in the number of unprotected documents (which it "conservatively estimate[ed]" as more than 300,000),[244] but that approach was not mandated under section 503, section 222, or the Commission's rules. Similarly, in this case, the Commission reasonably exercised its authority to find that each unique relationship between Verizon and an LBS

---

[241] 47 U.S.C. § 503(b); 47 CFR § 1.80(b).

[242] *TerraCom*, 29 FCC Rcd at 13343, para. 50.

[243] *TerraCom*, 29 FCC Rcd at 13343, para. 50.

[244] *TerraCom*, 29 FCC Rcd at 13343, para. 52. The Commission's investigation into apparent violations of consumer privacy requirements in *TerraCom* was resolved by a consent decree in which the companies admitted to violating sections 201(b) and 222(a) of the Act. *See TerraCom, Inc. and YourTel America, Inc.*, Order and Consent Decree, 30 FCC Rcd 7075, 7084, at para. 20 (EB 2015).

provider or aggregator represented a distinct failure to reasonably protect customer CPNI and therefore a separate violation of section 222 of the Act and section 64.2010 of the Commission's rules. Each such relationship relied upon a distinct and unique contractual chain (from Verizon to the Aggregator, then from the Aggregator to the LBS provider) and was premised to involve a specific, individually-approved "Use Case" that had been reviewed and authorized by Verizon. Treating these separate channels for the disclosure of location information—each of which, although unique, suffered from the same fundamental vulnerabilities discussed in the *NAL* and above—as separate violations was thus rational and properly within the Commission's discretion.

80. The approach taken in the *NAL* was not only reasonable, it was—contrary to Verizon's claim that it exceeded the statutory maximum—eminently *conservative*. As described in the *NAL*, Verizon's practices placed the sensitive location information of *all* of its customers at unreasonable risk of unauthorized disclosure. As such, the Commission could well have chosen to look to the total number of Verizon subscribers when determining the number of violations (and under that analysis, the violations presumably would have continued until the very last LBS provider's access to customer location information was cut off).[245] Using that

[245] Although it involved a data breach—and not, as in this case, an ongoing failure to maintain reasonable safeguards such that customer data was placed at unreasonable risk of unauthorized disclosure—*TerraCom* supports applying a customer-centric forfeiture calculation that takes into account the number of customers whose

methodology—and taking into account the tens of millions of consumers whose highly sensitive location information was made vulnerable by Verizon —would have resulted in a significantly higher forfeiture than what was proposed in the *NAL*.

81. Furthermore, even under the framework applied in the *NAL*, the Commission could have calculated the proposed forfeiture based upon every single entity with access to Verizon customer location information up to the statutory maximum ($204,892 per day up to $2,048,915 for each and every LBS provider). That would have resulted in a far higher fine than the approach that was taken (applying a $40,000 forfeiture for the first day of the violation and a $2,500 forfeiture for each successive day the violation continued). Instead, the Commission took a conservative approach, giving Verizon a 30-day grace period with no fines assessed, limiting the number of continuing violations to every day that each related LBS provider operated in the apparent absence of reasonable measures to protect CPNI and therefore left Verizon customers' CPNI vulnerable to unlawful disclosure, and assessing a far lower fine per day for the continuing violations than it could have. This approach recognized the Commission's need to show that such violations are serious and ensured the proposed forfeiture amounts act as a powerful deterrent for future failures to reasonably protect CPNI.

82. We also reject any claim that Verizon's due process rights were violated because it lacked fair notice

---

data was inadequately protected. *See TerraCom*, 29 FCC Rcd at 13343, para. 50.

that its LBS practices would potentially make it liable for a penalty in excess of the $2,048,915 statutory maximum for a single continuing violation. Consistent with our earlier discussion of Verizon's fair notice claims,[246] we find that this argument lacks merit. Customer location information is CPNI that is subject to protection under section 222 of the Act and section 64.2010 of the Commission's rules. Verizon knew, or should have known, that failing to reasonably protect CPNI carries with it significant potential penalties that may be associated with more than one violation. Indeed, the Commission has in the past proposed penalties for what could be viewed as a system-wide violation on a more granular basis that would yield higher penalties that would result from treating the violation as a single continuing violation.[247] Indepen-dently, we observe that the penalties at issue here are governed by section 503 of the Act, with which we fully comply in our decision.[248] As the D.C. Circuit has recognized, where a statute specifies maximum penalties, the statute itself provides fair notice of all penalties within that limit.[249]

4. The Commission Will Reduce the Forfeiture Amount by $1,417,500

---

[246] *See supra* [App. 94a-96a].

[247] *See*, *e.g.*, *TerraCom*, 29 FCC Rcd at 13343, paras. 51-52.

[248] 47 U.S.C. § 503.

[249] *Pharon v. Bd. of Gov. of the Fed. Reserve*, 135 F.3d 148, 157 (D.C. Cir. 1998) (applying *BMW of North Am. v. Gore*, 517 U.S. 559 (1996), to a penalty assessed by the Board and concluding that the relevant statutory maximum penalty provisions provided adequate notice).

83. Verizon asserts that even if the Commission's forfeiture methodology is permissible, the calculations in the *NAL* are based on incorrect facts. Specifically, for the 65 entities whose ongoing access to customer location information factored into the forfeiture amount, the *NAL* cites two separate termination dates (one for 60 of the entities and the other for the remaining 5).[250] According to Verizon, "a number of those third parties actually ceased accessing any location information before those dates."[251] Verizon's claim is supported by a Declaration and Exhibit that purport to show the "Date of Last Location Access/Request" for each LBS entity, a number of which fall upon dates prior to those listed in the *NAL*.[252]

84. We are not persuaded that this merits a reduction in the forfeiture amount. The calculations in the *NAL* were not based on when Verizon actually transmitted customer location information to particular LBS providers. Rather, it was those entities' *ability* to access location information at the time of their choosing, and in the apparent absence of reasonable safeguards, that the forfeiture calculation was based upon. The fact that certain providers may not have exercised that ability (which they retained until the termination dates set forth in the *NAL*) does not affect our analysis.

85. Verizon also contends that two of the entities whose participation in the LBS program factored into the forfeiture calculation "never actually participated

---

[250] *NAL*, 35 FCC Rcd at 1726, para. 86.

[251] NAL Response at 58.

[252] NAL Response, Exhibits A and D.

in the program in the first place."[253] Verizon explains that "[t]wo of the entities identified in VZ's LOI Responses . . . applied to and were approved for participation in the Verizon location aggregator program and, therefore, were included on customer / participant lists, but did not fully integrate to the location platform and never received any subscriber location data in connection with the program."[254]

86. In developing the *NAL*, the Commission relied upon the information furnished to it by Verizon, including a listing of LBS program participants, and reasonably expected that information to be accurate and complete. Nonetheless, in light of the additional details provided by Verizon in the NAL Response, we now exercise our discretion to reduce the forfeiture amount to reflect the fact that two of the 65 entities cited in the *NAL* did not actually participate in the program (and therefore did not have access to customer location information). The *NAL* assigned a base forfeiture of $472,500 for each of those two entities ($40,000 for the first day of the continuing violation and $2,500 for each of the subsequent 173 days, or $40,000 plus $432,500, totaling $472,500). The combined base forfeiture for the two providers is therefore $945,000. The *NAL* applied a 50% upward adjustment to that amount, or an additional $472,500, for a total associated forfeiture of $1,417,500. Accordingly, we now reduce the total forfeiture proposed in the *NAL* by $1,417,500.

---

[253] NAL Response at 58.

[254] NAL Response, Exhibit D, n. 5.

5. The Upward Adjustment is Permissible and Warranted

87. Verizon argues that the Commission impermissibly based the 50% upward adjustment to the forfeiture amount proposed in the *NAL* on the same factors that were considered in setting the base forfeiture.[255] Verizon also contends that, in determining the amount of the upward adjustment, the Commission misconstrued the significance of an internal Verizon document and the record-matching reports provided by Aegis and erred in describing the severity of the risk that Verizon's LBS program posed to the Company's customers.[256]

88. We reject these arguments and maintain the 50% upward adjustment proposed in the *NAL*. With regard to the upward adjustment, section 503 of the Act requires the Commission to ". . . take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[257] The plain language of the statute provides the Commission with broad discretion to assess proposed penalties based on the statutory factors, up to the statutory maximum. Moreover, section 1.80 of the Commission's rules provides a list of possible factors the Commission may use when making a determination to adjust upward or adjust downward the base forfeiture.[258] These

---

[255] NAL Response at 59.

[256] NAL Response at 58-59.

[257] 47 U.S.C. § 503(b).

[258] 47 CFR § 1.80(b)(10), Table 3.

factors include, importantly, "egregious misconduct," "substantial harm," "repeated or continuous violation," and "ability to pay/relative disincentive," among others.[259]

89. The Commission weighed these factors when making the determination that the base forfeiture in this case merited a substantial upward adjustment. Verizon's conduct was egregious; the *NAL* detailed how Verizon failed to respond to indications that its consent record audit process, as well as its overall system for obtaining customer consent for the disclosure of location information, was faulty.[260] Further, revelations in the press about Securus' hidden location information program led to a public outcry and prompted inquiries from members of Congress concerned about carriers' apparent lack of control over highly sensitive location information.[261] Its failure to adequately

---

[259] *Id.*

[260] For the reasons discussed earlier, we reject Verizon's claim that the Commission drew the wrong conclusions from the Aegis audit and consent-matching materials discussed in the *NAL*. *See supra* III.C.1-2.

[261] *See e.g.*, Letter from Sen. Ronald L. Wyden, Senator, U.S Senate, et al., to Joseph J. Simons, Chairman, Federal Trade Commission, and Ajit Pai, Chairman, Federal Communications Commission (Jan. 24, 2019) (on file in EB-TCD-18-00027704) (this Congressional was signed by 15 United States senators); Letter from Rep. Frank J. Pallone, Jr., Chairman, U.S. House of Representatives Committee on Energy and Commerce, to Ajit Pai, Chairman, Federal Communications Commission (Jan. 11. 2019) (on file in EB-TCD-18-00027704); Maria Dinzeo, *Class Claims AT&T Sold Their Real-Time Locations to Bounty Hunters*, Courthouse News Service (July 16, 2019), https://www.courthousenews.com/class-claims-att-sold-

protect CPNI for a protracted amount of time caused substantial harm by making it possible for "malicious persons to identify the exact locations of Verizon subscribers who belong to law enforcement, military, government, or other highly sensitive positions—thereby threatening national security and public safety"—a threat illustrated by reports that Hutcheson used location information to obtain the precise location of multiple Missouri State Highway Patrol officers on numerous occasions.[262] The violations were continuous over an extended period of time and repeated with two Aggregators and multiple LBS providers. Finally, the Commission took into account Verizon's status as a

---

their-real-time-locations-to-bounty-hunters/; Brian Barrett, *A Location-Sharing Disaster Shows How Exposed You Really Are*, Wired (May 19, 2018), https://www.wired.com/story/locationsmart-securus-location-data-privacy/; Press Release, *New America's Open Technology Institute, Privacy Advocates Call on FCC to Hold Wireless Carriers Accountable for Selling Customer Location Information to Third Parties Without Consent* (June 14, 2019), https://www.newamerica.org/oti/press-releases/privacy-advocates-call-fcc-hold-wireless-carriers-accountable-selling-customer-location-information-third-parties-without-consent/ (announcing that New America's Open Technology Institute, the Center on Privacy & Technology at Georgetown Law, and Free Press had filed a complaint with the FCC regarding the sale and disclosure of customer location information by Verizon, AT&T, T-Mobile, and Sprint).

[262] *NAL*, 35 FCC Rcd at 1728, para. 91. Verizon argues that it was not possible under its LBS program for a third party to identify customers' "exact locations." NAL Response at 59. We do not intend to quibble over the precision of the location-finding that Verizon's program had enabled. There is no question that it allowed for determining the location of law enforcement personnel, including whether they were in a certain area or vicinity. It is not difficult to imagine how this capability is susceptible to abuse.

major telecommunications provider to determine what penalty, when applied, would adequately provide Verizon with the necessary disincentive to engage in similar conduct again in the future. These considerations, taken into account as the Commission lawfully exercised its statutory authority to weigh the relevant factors, justify the resulting upward adjustment. Verizon's arguments to the contrary do not defeat Congress's decision to grant the FCC the power to weigh the factors and make such adjustments "as justice may require."[263] Nor do Verizon's arguments persuade us that the 50% upward adjustment, which is in line with upward adjustments in other cases involving consumer harms,[264] was unwarranted.

E. Section 503(b) Is Employed Here Consistent With the Constitution

90. We reject Verizon's supplemental constitutional objections that: (1) the FCC combines investigatory, prosecutorial, and adjudicative roles in violation of

---

[263] 47 U.S.C. § 503(b).

[264] *See*, *e.g.*, *Scott Rhodes*, Forfeiture Order, 36 FCC Rcd 705, 728, at para. 54 (2021) (upward adjustment equaling 100% of base forfeiture amount on robocaller/spoofer who made targeted robocalls designed to harass victims); *John C. Spiller, et al.*, Forfeiture Order, 36 FCC Rcd 6225, 6257, at para. 59 (2021) (upward adjustment equaling 50% of base forfeiture amount imposed on robocaller who engaged in illegal spoofing for robocall telemarketing activities); *Adrian Abramovich*, Forfeiture Order, 33 FCC Rcd 4663, 4671, at para. 25, 4674, at para. 33 (2018) (upward adjustment equaling 50% of base forfeiture amount imposed on robocaller who engaged in illegal spoofing for robocall tele-marketing activities).

constitutional due process requirements;[265] (2) the issuance of a forfeiture order by the Commission would violate Article III and the Seventh Amendment;[266] and (3) the Commission's ability to choose a procedural approach to enforcement under section 503(b) of the Act is an unconstitutional delegation of legislative power.[267] Verizon's arguments are premised on misunderstandings regarding the relevant statutory framework, the nature of the Commission's actions, and relevant precedent.

91. As a threshold matter, Verizon neglects key aspects of the statutorily-mandated enforcement process applicable here. Pursuant to section 504 of the Act, after the Commission issues a forfeiture order, Verizon is entitled to a trial *de novo* in federal district court before it can be required to pay the forfeiture.[268] Verizon's objection to the combination of investigatory, prosecutorial, and adjudicative roles in the FCC ignores that statutory entitlement to a trial *de novo* in federal district court to ultimately adjudicate its obligation to pay a

---

[265] Letter from Scott H. Angstreich, counsel to Verizon, to Michael Epshteyn and Rosemary Cabral, Enforcement Bureau, FCC, EB-TCD-18-00027698, at 2 (filed June 22, 2023) (Verizon June 22, 2023 Supplemental NAL Response).

[266] Verizon June 22, 2023 Supplemental NAL Response at 2.

[267] Verizon June 22, 2023 Supplemental NAL Response at 2-3.

[268] 47 U.S.C. § 504(a); *see also*, *e.g.*, *Ill. Citizens Comm. for Broadcasting v. FCC*, 515 F.2d 397, 405 (D.C. Cir. 1974) (noting that "a jury trial was available" in an action to collect a forfeiture). That Verizon theoretically might elect to pay the forfeiture voluntarily does not diminish its statutory right to a trial *de novo* in federal district court.

forfeiture.[269] Likewise, Verizon's claim that a forfeiture order issued under section 503(b) of the Act does not provide it a decision by an Article III court, including via a trial by jury, ignores Verizon's statutory right to a trial *de novo* before it can be required to pay the forfeiture.[270] The statutory right to a trial *de novo* provided for by section 504 of the Act is itself sufficient grounds to reject those two constitutional claims.

92. Independently, there are sufficient grounds to reject Verizon's arguments for other reasons, as well. We discuss each of these in turn below.

93. *Combination of Functions*. With respect to Verizon's claimed due process violation,[271] Verizon fails to demonstrate sufficient grounds for concluding that a combination of functions in the Commission's enforcement process here renders it constitutionally

---

[269] *See, e.g.*, *Concrete Pipe & Prods. of Cal. v. Construction Lab. Pension Trust for S. Cal.*, 508 U.S. 602, 618 (1993) ("Where an initial determination is made by a party acting in an enforcement capacity, due process may be satisfied by providing for a neutral adjudicator to 'conduct a *de novo* review of all factual and legal issues.'").

[270] *Cf. Executive Benefits Insurance Agency v. Arkinson*, 573 U.S. 25, 38-40 (2014) (where a claim raised before a bankruptcy court implicates the judicial power under Article III of the constitution, the bankruptcy court can make proposed findings of fact and conclusions of law for *de novo* review by a federal district court, and even if a bankruptcy court adjudicates such a claim itself, *de novo* review of that decision by a federal district court resolved any Article III concern); *Crowell v. Benson*, 285 U.S. 22, 50-65 (1932) (even in the case of private rights, an agency can make factual findings and render an initial decision of law subject to *de novo* review of issues of jurisdictional fact and of law in an Article III court).

[271] Verizon June 22, 2023 Supplemental NAL Response at 2.

suspect, even apart from Verizon's failure to account for the trial *de novo* under section 504 of the Act. It is true that "a 'fair trial in a fair tribunal is a basic requirement of due process,'" but objections in that regard premised on the combination of functions in an agency "must overcome a presumption of honesty and integrity in those serving as adjudicators."[272] To overcome that presumption requires "a showing of conflict of interest or some other specific reason for disqualification."[273]

---

[272] *Withrow v. Larkin*, 421 U.S. 35, 46, 47 (1975); *see also*, *e.g.*, *id.* at 47-48 (discussing *FTC v. Cement Institute*, 333 U.S. 683 (1948), where the Court found no due process violation based on the adjudicators' prior investigations, including stated opinions about the legality of certain pricing systems, because "[t]he fact that the Commission had entertained such views as the result of its prior ex parte investigations did not necessarily mean that the minds of its members were irrevocably closed on the subject of the respondents' basing point practice" and in the adjudication at issue "members of the cement industry were legally authorized participants in the hearings" and submit evidence and arguments in defense of their positions); *In re Zdravkovich*, 634 F.3d 574, 579 (D.C. Cir. 2011) ("In *Withrow v. Larkin*, the Supreme Court expressly rejected the claim that due process is violated where '[t]he initial charge or determination of probable cause and the ultimate adjudication' are made by the same agency."); *Ethicon Endo-Surgery v. Covidien*, 812 F.3d 1023, 1029-30 (Fed. Cir. 2016) (observing that "[l]ower courts have also rejected due process challenges to systems of adjudication combining functions in an agency," and collecting illustrative cases).

[273] *Schweiker v. McClure*, 456 U.S. 188, 195 (1982); *see also*, *e.g.*, *Caperton v. A.T. Massey Coal*, 556 U.S. 868, 881 (2009) (the due process inquiry is "whether the average judge in his position is 'likely' to be neutral, or whether there is an unconstitutional 'potential for bias'").

94. Verizon fails to demonstrate a concern specific to the Commission's forfeiture order here sufficient to overcome the presumption of honesty and integrity. Insofar as Verizon notes the existence of pending due process claims premised on the combination of functions involving another agency, we are not persuaded to treat those still-pending unadjudicated arguments as warranting the conclusion that there is a genuine due process concern here.[274]

95. Verizon also expresses concern that "the Commission performs its own investigations of alleged violations, prosecutes them by taking enforcement action and issuing an NAL, and adjudicates the merits of any challenges to the NAL in imposing a forfeiture."[275] But these broad-brush objections do not identify specific reasons that a reasonable adjudicator in the Commission's position would be biased in this proceeding—certainly not one sufficient to overcome the background presumption of honesty and integrity on the part of agency adjudicators. To the contrary, finding a due process violation based simply on those would, in large part, turn that background presumption on its head by a requiring a presumption of bias whenever the Commission issued an NAL. Such an understanding would be at odds with the range of scenarios where courts have found no due process concerns with adjudication

---

[274] *See* Verizon June 22, 2023 Supplemental NAL Response at 2 (citing the pending constitutional challenge involving the FTC underlying *Axon Enterprise v. FTC*, 143 S. Ct. 890 (2023)).

[275] Verizon June 22, 2023 Supplemental NAL Response at 2.

by individuals despite earlier involvement in a matter.[276]

96. Nor are we otherwise persuaded that due process concerns are present here. The potential to adopt forfeitures—even substantial forfeitures—that would be paid into the U.S. Treasury does not create a risk of financial bias on the part of reasonable adjudicators in the Commission's position.[277] We also are not

---

[276] For example, the Supreme Court in *Withrow v. Larkin* observed that "judges frequently try the same case more than once and decide identical issues each time, although these issues involve questions both of law and fact," and "the Federal Trade Commission cannot possibly be under stronger constitutional compulsions in this respect than a court," noting also that "a hearing examiner who has recommended findings of fact after rejecting certain evidence as not being probative was not disqualified to preside at further hearings that were required when reviewing courts held that the evidence had been erroneously excluded." *Withrow v. Larkin*, 421 U.S. at 48-49 (internal quotation marks omitted). The Court's willingness to accept continued adjudicator participation even where final—not merely preliminary—decisions previously had been made by the adjudicators strongly supports our analysis here.

[277] *See*, *e.g.*, *Ward v. Village of Monroeville*, 409 U.S. 57, 59-61 (1972) ("[T]he test is whether the [decisionmaker's] situation is one 'which would offer a possible temptation to the average man as a judge to forget the burden of proof required to convict the defendant, or which might lead him not to hold the balance nice, clear, and true between the state and the accused . . . ,'" and due process was violated where a mayor acted as an adjudicator and also obtained a portion of the fees and costs he imposed in that role, whereas due process was not violated where a mayor acted as an adjudicator but "the Mayor's relationship to the finances and financial policy of the city was too remote to warrant a presumption of bias toward conviction in prosecutions before him as judge."); *Brucker v. City of Doraville*, 38 F.4th 876, 884 (11th Cir. 2022) ("The fact that a judge works for a government, which gets a significant portion of its revenues from

persuaded that the Commission's decision to issue an NAL proposing even a significant forfeiture is likely to create the risk of bias in the Commission's subsequent decision regarding a forfeiture order. Although the Supreme Court has stated in the context of criminal prosecutions that "there is an impermissible risk of actual bias when a judge earlier had significant, personal involvement as a prosecutor in a critical decision regarding the defendant's case," we find even a significant proposed forfeiture materially distinguishable from the imposition of criminal penalties—particularly the death penalty.[278] For example, we are not persuaded that the Commission's decision to propose a forfeiture in an NAL creates the same degree of risk of an adjudicator becoming "psychologically wedded" to that proposal as in the case of a prosecutor's decision to authorize prosecutors to seek the death penalty, nor does Verizon provide evidence that is the case here.[279] We also do not find that the NAL-initiated enforcement process presents the risk of adjudicators acting on the basis of extra-record information or impressions of the respondent that the Court found of concern in the case of a criminal prosecutor then serving as a

---

fines and fees, is not enough to establish an unconstitutional risk of bias on the part of the judge.").

[278] *Williams v. Pennsylvania*, 579 U.S. 1, 8 (2016) (finding a due process violation where the judge previously had been involved as a prosecutor in authorizing the prosecution to seek the death penalty).

[279] *See Williams v. Pennsylvania*, 579 U.S. at 9 (identifying this concern in the case of a prosecutor that authorized the prosecution to seek the death penalty).

judge.[280] In particular, section 503(b) requires a Commission NAL to "set forth the nature of the act or omission charged . . . and the facts upon which such charge is based,"[281] and Verizon has not identified concerns about the decision here being premised on extra-record evidence obtained by the Commission or commissioners in the development of the *NAL*.

97. *Trial By Jury*. We also reject Verizon's contention that adjudication of the violations at issue here may not constitutionally be assigned to a federal agency.[282] The Seventh Amendment preserves "the right of trial by jury" in "Suits at common law, where the value in controversy shall exceed twenty dollars,"[283] but the Seventh Amendment applies only to suits litigated in Article III courts, not to administrative adjudications conducted by federal agencies.[284] In determining whether an adjudication involves an exercise of

---

[280] *See Williams v. Pennsylvania*, 579 U.S. at 9-10 (identifying this concern in the case of a prosecutor that authorized the prosecution to seek the death penalty and also citing *In re Murchison*, 349 U.S. 133, 138 (1955), which involved an individual acting in the role of both a grand jury and judge where similar concerns arose); *see also*, *e.g.*, *Withrow v. Larkin*, 421 U.S. at 54 (explaining that "Murchison has not been understood to stand for the broad rule that the members of an administrative agency may not investigate the facts, institute proceedings, and then make the necessary adjudications").

[281] 47 U.S.C. § 503(b)(4).

[282] AT&T June 22, 2023 Supplemental NAL Response at 2-3.

[283] U.S. Const. amend. VII.

[284] *See*, *e.g.*, *Oil States Energy Services v. Greene's Energy Group*, 138 S. Ct. 1365, 1379 (2018); *Atlas Roofing Co. v. Occupational Safety & Health Review Commission*, 430 U.S. 442, 455 (1977).

judicial power vested in the federal courts under Article III of the constitution, the Supreme Court has distinguished between "public rights" and "private rights."[285] Congress has broad authority to "assign adjudication of public rights to entities other than Article III courts."[286] Examples of "public rights" litigation involving "cases in which the Government sues in its sovereign capacity to enforce public rights created by statutes within the power of Congress to enact" include enforcement of federal workplace safety requirements,[287] "adjudicating violations of the customs and immigration laws and assessing penalties based thereon,"[288] adjudicating "whether an unfair labor practice had been committed and of ordering backpay where appropriate,"[289] and the grant or reconsideration of a grant of a patent.[290] That precedent confirms the constitutionality validity of FCC adjudication of violations of the Communications Act, even setting aside the reality that Verizon does, in fact, have the right of a trial *de novo* under section 504 of the Act here. Through section 222 of the Communications Act, Congress "created new statutory obligations"[291] designed to protect consumer privacy even as the communications marketplace

---

[285] *Oil States*, 138 S. Ct. at 1373 (citation omitted).

[286] *Id.*

[287] *Atlas Roofing*, 430 U.S. at 450, 461.

[288] *Id.* at 451.

[289] *Id.* at 453.

[290] *Oil States*, 138 S. Ct. at 1373.

[291] *Atlas Roofing*, 430 U.S. at 450.

became more open to competition,[292] analogous to those previously identified as involving public rights. Congress further "provided for civil penalties" for violations of those obligations, and constitutionally could entrust to the Commission "the function of deciding whether a violation has in fact occurred" when deciding whether to issue a forfeiture order, bringing it well within the "public rights" framework of existing Supreme Court precedent.[293]

98. Relying principally on the Supreme Court's decision in *Tull v. United States* and the Fifth Circuit's decision in *Jarkesy*, Verizon contends that the forfeiture at issue here should fall within the "private rights" framework—requiring adjudication in an Article III court, with the right to a trial by jury.[294] In *Tull*, the

---

[292] *See, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8064, para 1 (1998) ("Congress recognized, . . . that the new competitive market forces and technology ushered in by the 1996 Act had the potential to threaten consumer privacy interests. Congress, therefore, enacted section 222 to prevent consumer privacy protections from being inadvertently swept away along with the prior limits on competition.").

[293] *Atlas Roofing*, 430 U.S. at 450.

[294] Verizon June 22, 2023 Supplemental NAL Response at 2-3 (citing *Tull v. United States*, 481 U.S. 412 (1987) and *Jarkesy v. SEC*, 34 F.4th 446 (5th Cir. 2022)). Verizon also cites Justice Thomas' concurrence in *Axon*. *Id.* (citing *Axon*, 143 S. Ct. at 911 (Thomas, J., concurring)). However, as relevant here, Justice Thomas was critiquing existing Supreme Court precedent insofar as it had allowed agency adjudication subject to only deferential appellate court review. *Axon*, 143 S. Ct. at 906-09 (Thomas, J., concurring). We are

government was pursuing a claim in federal district court seeking penalties and an injunction under the Clean Water Act and the district court had denied the defendant's request for a jury trial.[295] But as the Supreme Court also has made clear, Congress can assign matters involving public rights to adjudication by an administrative agency "even if the Seventh Amendment would have required a jury where the adjudication of those rights is assigned to a federal court of law instead."[296] Thus, *Tull* does not address the question of whether Congress can assign the adjudication of a given matter to an administrative agency—it speaks only to the Seventh Amendment implications of a matter that is assigned to an Article III court. To the extent that the Fifth Circuit in *Jarkesy* treated *Tull* as standing for the proposition that causes of action analogous to common-law claims would, as a general matter, need to be adjudicated in Article III courts with a right to trial by jury, we are unpersuaded. As the Supreme Court has held in a post-*Tull* decision, "Congress may fashion causes of action that are closely analogous to common-law claims and place them beyond the ambit of the Seventh Amendment by assigning their resolution to a forum in which jury trials are

---

not persuaded to alter our analysis based on one Justice's non-controlling opinion, and we therefore continue to apply existing Supreme Court precedent as it bears on our analysis here.

[295] *Tull*, 481 U.S. at 414-15.

[296] *Atlas Roofing*, 430 U.S. at 455.

unavailable."[297] We thus are unpersuaded by Verizon's reliance on *Tull* and *Jarkesy*.[298]

99. *Nondelegation*. Finally, contrary to Verizon's contention,[299] the choice of enforcement processes in section 503(b) of the Act does not constitute an unconstitutional delegation of legislative power. Section 503(b)(3) and (4) of the Act gives the Commission a choice of two procedural paths when pursuing forfeitures: either the NAL-based path most commonly

---

[297] *Granfinanciera v. Nordberg*, 492 U.S. 33, 52 (1989) (emphasis omitted). We also are unpersuaded by the Fifth Circuit's decision in *Jarkesy* insofar as it interpreted *Granfinanciera* as establishing an additional prerequisite for a public right—namely, "when Congress passes a statute under its constitutional authority that creates a right so closely integrated with a comprehensive regulatory scheme that the right is appropriate for agency resolution." *Jarkesy*, 34 F.4th at 453. But *Granfinanciera* involved a dispute between two private parties, rather than an enforcement action commenced by the government. *Granfinanciera*, 492 U.S. at 51. The *Granfinanciera* Court explained that it had previously applied the public-rights doctrine to sustain "administrative factfinding" in cases "where the Government is involved in its sovereign capacity," but the Court distinguished such cases from "[w]holly private" disputes. *Id.* (citation omitted). It was in the context of private disputes—*i.e.*, "in cases not involving the Federal Government"—where the Court considered whether Congress "has created a seemingly 'private' right that is so closely integrated into a public regulatory scheme as to be a matter appropriate for agency resolution." *Granfinanciera*, 492 U.S. at 54. The Fifth Circuit in *Jarkesy* thus took that holding out of context when it applied it to claims where (as here) the government is involved in its sovereign capacity.

[298] The government has petitioned for certiorari in the *Jarkesy* case. Petition for a Writ of Certiorari, SEC v. Jarkesy, No. 22-859 (filed Mar. 8, 2023).

[299] Verizon June 22, 2023 Supplemental NAL Response at 2-3.

employed by the Commission—which we have used here—or a formal adjudication in accordance with section 554 of the Administrative Procedure Act before the Commission or an administrative law judge.[300] Contrary to Verizon's suggestion, this choice involves the exercise not of legislative power but of executive power. The choice of enforcement process reflected in section 503(b) does not require the Commission to establish general rules governing private conduct of the sort that might implicate potential concerns about unauthorized lawmaking, but instead involves the exercise of enforcement discretion that is a classic executive power.[301]

100. We also are unpersuaded by Verizon's reliance on the Fifth Circuit decision in *Jarkesy* to support its nondelegation concerns. In addition to questions about the merits of the Fifth Circuit's approach in that

---

[300] 47 U.S.C. § 503(b)(3), (4).

[301] *See, e.g.*, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2207 (2021) ("[T]he choice of how to prioritize and how aggressively to pursue legal actions against defendants who violate the law falls within the discretion of the Executive Branch."); *cf. Heckler v. Chaney*, 470 U.S. 821, 832 (1985) (noting that a federal prosecutor's decision not to indict a particular defendant "has long been regarded as the special province of the Executive Branch, inasmuch as it is the Executive who is charged by the Constitution to 'take Care that the Laws be faithfully executed' ") (citation omitted); *United States v. Batchelder*, 442 U.S. 114, 121, 124, 126 (1979) (no violation of the nondelegation doctrine when Congress enacted two criminal statutes with "different penalties for essentially the same conduct" and gave prosecutors "discretion to choose between" the two statutes given that Congress had "informed the courts, prosecutors, and defendants of the permissible punishment alternatives available under each [statute]," and thereby "fulfilled its duty").

regard,[302] even on its own terms, *Jarkesy* involved a scenario where the court found that "Congress offered *no guidance* whatsoever" regarding the statutory decision at issue.[303] That is not the case here, however. Although section 503(b) alone does not expressly provide guidance regarding the choice of enforcement process, section 4(j) of the Act directs as a general matter that "[t]he Commission may conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to the ends of justice."[304] Nothing in section 503(b) precludes the applicability of these considerations to guide the Commission's choice of enforcement process there, and the Commission has interpreted section 4(j) as informing its decision regarding the procedural protections required in adjudicatory proceedings in other contexts in the past.[305] The circumstances here therefore are distinct from those in

---

[302] As discussed above, Supreme Court precedent supports our contrary analysis here, and as previously noted, the government has petitioned for certiorari in the *Jarkesy* case. *See supra* note 298.

[303] *Jarkesy*, 34 F.4th at 462.

[304] 47 U.S.C. § 154(j).

[305] *See*, *e.g.*, *Procedural Streamlining of Administrative Hearings*, EB Docket No. 19-214, Report and Order, 35 FCC Rcd 10729, 10734, para. 14 (2020) (looking to the standards in section 4(j) to guide the decision regarding the conduct of adjudicatory proceedings on the basis of a written record without live testimony); *id.* at 10735-36, para. 18 (looking to the standards in section 4(j) to guide the decision regarding whether an adjudication should be heard by the Commission, one or more commissioners, or an ALJ).

Jarkesy where "Congress offered *no guidance* whatsoever."[306]

IV. CONCLUSION

101. Based on the record before us and in light of the applicable statutory factors, we conclude that Verizon willfully and repeatedly violated section 222 of the Act[307] as well as section 64.2010 of the Commission's rules[308] by disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it and for failing to take reasonable steps to protect its customers' location information. We decline to withdraw the Admonishment and, having already reduced the forfeiture by $1,417,500 to account for two entities that did not participate in Verizon's LBS program, decline to further reduce or to cancel the forfeiture amount of $46,901,250.

V. ORDERING CLAUSES

102. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act, 47 U.S.C. § 503(b), and section 1.80 of the Commission's rules, 47 CFR § 1.80, Verizon Communications **IS LIABLE FOR A MONETARY FORFEITURE** in the amount of forty-six million, nine-hundred and one thousand, two hundred and fifty dollars ($46,901,250) for willfully and repeatedly violating section 222 of the Act and section 64.2010 of the Commission's rules.

---

[306] *Jarkesy*, 34 F.4th at 462.

[307] 47 U.S.C. § 222.

[308] 47 CFR § 64.2010.

103. Payment of the forfeiture shall be made in the manner provided for in section 1.80 of the Commission's rules within thirty (30) calendar days after the release of this Forfeiture Order.[309] Verizon Communications shall send electronic notification of payment to Shana Yates, Michael Epshteyn, and Kimbarly Taylor, Enforcement Bureau, Federal Communications Commission, at shana.yates@fcc.gov, michael.epshteyn@fcc.gov, and kimbarly.taylor@fcc.gov on the date said payment is made. If the forfeiture is not paid within the period specified, the case may be referred to the U.S. Department of Justice for enforcement of the forfeiture pursuant to section 504(a) of the Act.[310]

104. In order for Verizon Communications to pay the proposed forfeiture, Verizon Communications shall notify Shana Yates at Shana.Yates@fcc.gov of its intent to pay, whereupon an invoice will be posted in the Commission's Registration System (CORES) at https://apps.fcc.gov/cores/userLogin.do. Payment of the forfeiture must be made by credit card using CORES at https://apps.fcc.gov/cores/userLogin.do, ACH (Automated Clearing House) debit from a bank account, or by wire transfer from a bank account. The Commission no longer accepts forfeiture payments by check or money order. Below are instructions that payors should follow based on the form of payment selected:[311]

---

[309] *Id.*

[310] 47 U.S.C. § 504(a).

[311] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #1).

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. In the OBI field, enter the FRN(s) captioned above and the letters "FORF". In addition, a completed Form 159[312] or printed CORES form[313] must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 or CORES may result in payment not being recognized as having been received. When completing FCC Form 159 or CORES, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[314] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete

---

[312] FCC Form 159 is accessible at https://www.fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159.

[313] Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form 159. CORES is accessible at https://apps.fcc.gov/cores/userLogin.do.

[314] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.

- Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). Finally, choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial

institution that the designated account has authorization to accept ACH transactions.

105. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer — Financial Operations, Federal Communications Commission, 45 L Street NE, Washington, D.C. 20554. Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by telephone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

106. **IT IS FURTHER ORDERED** that a copy of this Forfeiture Order shall be sent by first class mail and certified mail, return receipt requested, to David L. Haga, Associate General Counsel, Verizon Communications, c/o Scott H. Angstreich, Esq., and Christopher M. Young, Kellogg, Hansen, Todd, Figel & Frederick, P.L.L.C., 1615 M Street, N.W., Suite 400, Washington, D.C. 20036.

FEDERAL COMMUNICATIONS COMMISSION
Marlene H. Dortch
Secretary

STATEMENT OF CHAIRWOMAN JESSICA ROSENWORCEL

Re: *In the Matter of Verizon Communications*, Forfeiture Order, File No.: EB-TCD-18-00027698 (April 17, 2024)

Our smartphones are always with us, and as a result these devices know where we are at any given moment.

This geolocation data is especially sensitive. It is a reflection of who we are and where we go. In the wrong hands, it can provide those who wish to do us harm the ability to locate us with pinpoint accuracy. That is exactly what happened when news reports revealed that the largest wireless carriers in the country were selling our real-time location information to data aggregators, allowing this highly sensitive data to wind up in the hands of bail-bond companies, bounty hunters, and other shady actors. This ugly practice violates the law—specifically Section 222 of the Communications Act, which protects the privacy of consumer data. The Commission has long recognized the importance of ensuring that information about who we call and where we go is not for sale. In fact, these enforcement actions—leading to $200 million in fines—were first proposed by the last Administration. By following through with this order, we once again make clear that wireless carriers have a duty to keep our geolocation information private and secure.

DISSENTING STATEMENT OF COMMISSIONER BRENDAN CARR

Re: *In the Matter of Verizon Communications*, Forfeiture Order, File No.: EB-TCD-18-00027698 (April 17, 2024)

For more than a decade, location-based service (LBS) providers have offered valuable services to consumers, like emergency medical response and roadside assistance. Up until the initiation of the above-captioned enforcement actions, LBS providers did so by

obtaining access to certain location information from mobile wireless carriers like AT&T, Verizon, and T-Mobile. Then, in 2018, a news report revealed that a local sheriff had misused access to an LBS provider's services. That sheriff was rightly prosecuted for his unlawful actions and served jail time. Subsequently, all of the participating carriers ended their LBS programs. So our decision today does not address any ongoing practice.

This is not to say that LBS providers have ended their operations. They have simply shifted to obtaining this same type of location information from other types of entities. That is why I encouraged my FCC colleagues to examine ways that we could use these proceedings to address that ongoing practice. But my view did not prevail.

That brings us to the final Forfeiture Orders that the FCC approves today. Back in 2020, after the mobile wireless carriers exited the LBS line of business, the FCC unanimously voted to approve Notices of Apparent Liability (NALs) against the carriers. Even then, it was clear that at least one LBS provider had acted improperly. So I voted for the NALs so we could investigate the facts and determine whether or not the carriers had violated any provisions of the Communications Act.

Now that the investigations are complete, I cannot support today's Orders. This is not to say that the carriers' past conduct should escape scrutiny by a federal agency. Rather, given the nature of the services at issue, the Federal Trade Commission, not the FCC, would have been the right entity to take a final

enforcement action, to the extent the FTC determined that one was warranted.

Here's why. Unlike the FTC, Congress has provided the FCC with both limited and circumscribed authority over privacy. Congress delineated the narrow contours of our authority in section 222 of the Commu-nications Act. The services at issue in these cases plainly fall outside the scope of the FCC's section 222 authority. Indeed, today's FCC Orders rest on a newfound definition of customer proprietary network information (CPNI) that finds no support in the Communications Act or FCC precedent. And without providing advance notice of the new legal duties expected of carriers (to the extent we could adopt those new duties at all), the FCC retroactively announces eye-popping forfeitures totaling nearly $200,000,000. These actions are inconsistent with the law and basic fairness. The FCC has reached beyond its authority in these cases.

According to the Orders, our CPNI rules now apply whenever a carrier handles a customer's location information—whether or not it relates to the customer's use of a "telecommunications service" under Title II of the Communications Act. Here, the location information was unrelated to a Title II service. The customer did not need to make a call to convey his or her location. In fact, the carrier could have obtained the customer's location even if the customer had a data-only plan for tablets. Yet the Order concludes that the carriers mishandled CPNI.

That cannot be right. Start with the definition of CPNI, which section 222 of the Communications Act defines as:

> information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.[1]

That definition has two key limitations. First, the information must be of a specific type. As relevant here, CPNI must "relate to" the "location . . . of use of a telecommunications service." Second, the information must have been obtained in a specific way. The customer must have made his or her location "available to carrier" and "solely by virtue of the carrier-customer relationship."

Take the first limitation. By requiring that the location "relate" to the "use of a telecommunications service," the statute covers a particular type of data known as "call location information"—namely, the customer's location *while making or receiving a voice call*. Section 222 confirms this commonsense reading elsewhere when it expressly refers to "call location information."[2] These statutory references to "call location information" would make no sense if Congress intended for CPNI to cover all location information collected by a carrier, irrespective of particular calls.

---

[1] 47 U.S.C. § 222(h)(1)(A).

[2] 47 U.S.C. § 222(f)(1) (ordinarily requiring "express prior authorization of the customer" for carrier disclosure of "call location information"); 47 U.S.C. § 222(d)(4) (allowing, however, carrier disclosure of "call location information" in certain emergency situations).

The FCC confirmed that "straightforward" interpretation in a 2013 Declaratory Ruling.[3] The definition of CPNI, this agency held, encompassed "telephone numbers of calls dialed and received and the location of the device at the time of the calls."[4] The FCC also clarified that CPNI included "the location, date, and time a handset experiences a network event, such as a dialed or received telephone call [or] a dropped call."[5]

Although the Orders claim CPNI was at play, they do not contend that "call location information" was disclosed. Nor could they. As the Orders concede, the carriers obtained their customers' location whenever a customer's device pinged the carrier's cell site, even when the device was otherwise idle. No voice call was necessary for the carrier to obtain the customer's location. In fact, the carrier could gather the customer's location even if the customer did not have a voice plan. So, the "location" did not "relate to" the "use" of a "tele-communications service" in any meaningful sense.

Turning to the second limitation, it seems implausible to conclude that the carrier obtained the customer's location "*solely* by virtue of the carrier-customer relationship," as section 222 requires. True, many of these customers might have had voice plans, thereby creating a "carrier-customer relationship." But any Title II

---

[3] *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, para. 22 (2013).

[4] *Id.* at para. 22.

[5] *Id.* at para. 25.

relationship was, at most, coincidental. The carrier could have obtained the customer's location even in the absence of a call, and even in the absence of a voice plan.

The massive forfeitures imposed in these Orders offend basic principles of fair notice. The FCC has never held that location information other than "call location information" constitutes CPNI. Nor has the FCC stated that a carrier might be liable under our CPNI rules for location information unrelated to a Title II service and collected outside the Title II relationship. So, even if we could proscribe the conduct at issue here through a rulemaking (and I am dubious that we could), it would be inappropriate and unlawful to impose the retroactive liability that these Orders do.

In the end, these matters should have been handled by the FTC. Our CPNI rules are narrow and do not cover every piece of data collected by an FCC-regulated entity. Besides, as the Communications Act makes clear, carriers are regulated under Title II only when they are engaged in offering Title II services.[6] In situations where an FCC-regulated entity offers a Title I service, such as mobile broadband, the FTC is the proper agency to enforce privacy and data security

---

[6] 47 U.S.C. § 153(51) ("A telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services . . ."); *see also FTC v. AT&T Mobility LLC*, 883 F.3d 848, 863-64 (9th Cir. 2018) (holding that the FTC's "common carrier" exemption to Section 5 of the FTC Act "bars the FTC from regulating 'common carriers' only to the extent that they engage in common-carriage activity").

practices under generally applicable rules of the road. I respectfully dissent.

DISSENTING STATEMENT OF COMMISSIONER NATHAN SIMINGTON

Re: *In the Matter of Verizon Communications*, Forfeiture Order, File No.: EB-TCD-18-00027698 (April 17, 2024)

Today, each of the major national mobile network operators faces a forfeiture for its purported failure to secure the confidentiality of its customer proprietary network information ('CPNI') as it relates to location information of network user devices. While the facts of each alleged violation are somewhat different, the enforcement calculation methodology used to arrive at the forfeitures is shared. Because I am concerned principally with that issue, together with what I view as a significant and undesirable policy upshot common across the actions that the Commission takes today, I will draft one dissent.

There is no valid basis for the arbitrary and capricious finding—enunciated in the Commission's erroneous rationale in *TerraCom Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) ('*TerraCom*') and relied upon today—that a single, systemic failure to follow the Commission's rules (in that case, violations of sections 201(b) and 222(a) of the Act; here, a violation of section 64.2010 of the Rules) may constitute however many separate and continuing violations the Commission chooses to find on the basis of the whole-cloth creation

of a novel legal ontology. In *TerraCom*—which was resolved by consent decree and never proceeded to a forfeiture order—the Commission found that each customer record exposed by a single insecure data protection method (some 305,065 records) could be treated as having formed a separate and continuing violation. Here, the Commission purports to count individual location-based services providers ('LBS') and aggregators relied upon by each mobile network operator to arrive at its separate and distinct continuing violations.

Whether counting individual exposed customer records or LBS providers and aggregators, the clear effect of the Commission's arbitrary selection of a violation class used to increase the number violations emerging from a single act or failure to act of a regulatee alleged to be in violation of our rules is to exceed our section 503 statutory authority. Here it cannot credibly be argued that any of the mobile network operators, in operating an LBS/aggregator program, committed more than one act relevant for the purposes of forfeiture calculation. It is simply not plausible that Congress intended that the Commission may arrive at forfeitures of any size simply by disaggregating an "act" into its individual constituent parts, counting the members of whatever class of objects may be related to the alleged violation to arrive at whatever forfeiture amount suits a preordained outcome. In this case we exceed our statutory maximum forfeiture by a factor of, in some cases, dozens; in *TerraCom*, we asserted the right to exceed it by thousands.

What's more, the Commission ought to act prudentially here: even assuming, purely *arguendo*, that

location-based CPNI were illicitly exposed, let us not forget that, at every moment, any of thousands of unregulated apps may pull GPS location information, Wi-Fi and Bluetooth signal strength, and other fragments of data indicating location from customer handsets at every moment the device is on. Indeed, this can be, and routinely is, accomplished even without consumer permission. By sending a strong market signal that any alleged violation of Commission rules regarding CPNI safekeeping (whether or not the rules actually were violated) can and will result in an outsize fine, we have effectively choked off one of the only ways that valid and legal users of consent-based location data services had to access location data for which legal safeguards and oversight actually exist.

It was available for the Commission to work with the carriers to issue consent decrees to promote best practices to develop further safeguards around location-based and aggregation services, and to actively monitor ongoing compliance in an effort to vouchsafe a regulated means of consensually sharing handset location data with legitimate users of the same. We opt, instead, to appear "tough on crime" in a way that actually reduces consumer data privacy by pushing legitimate users of location data toward unregulated data brokerage. Accordingly, I dissent.

APPENDIX C

1. U.S. Const., amend. VII provides:

In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.

2. 47 U.S.C. § 222 provides:

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 telecommuni-cations services provided by a telecommunications carrier.

(b) Confidentiality of carrier information

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

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

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

(2) Disclosure on request by customers

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

(3) Aggregate customer information

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

reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

(d) Exceptions

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

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

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

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

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

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

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

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

(e) Subscriber list information

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

(f) Authority to use location information

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

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

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

(g) Subscriber listed and unlisted information for emergency services

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

(h) Definitions

As used in this section:

(1) Customer proprietary network informa-tion

The term "customer proprietary network information" means—

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

carrier by the customer solely by virtue of the carrier-customer relationship; and

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

except that such term does not include subscriber list information.

(2) Aggregate information

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

(3) Subscriber list information

The term "subscriber list information" means any information—

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

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

(4) Public safety answering point

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

(5) Emergency services

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

(6) Emergency notification services

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

(7) Emergency support services

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

3. 47 U.S.C. § 503 provides:

Forfeitures

(a) Rebates and offsets

Any person who shall deliver messages for interstate or foreign transmission to any carrier, or for whom as sender or receiver, any such carrier shall transmit any interstate or foreign wire or radio communication, who shall knowingly by employee, agent, officer, or otherwise, directly or indirectly, by or through any means or device whatsoever, receive or accept from such common carrier any sum of money or any other valuable consideration as a rebate or offset against the regular charges for transmission of such messages as fixed by

the schedules of charges provided for in this chapter, shall in addition to any other penalty provided by this chapter forfeit to the United States a sum of money three times the amount of money so received or accepted and three times the value of any other consideration so received or accepted, to be ascertained by the trial court; and in the trial of said action all such rebates or other considerations so received or accepted for a period of six years prior to the commencement of the action, may be included therein, and the amount recovered shall be three times the total amount of money, or three times the total value of such consideration, so received or accepted, or both, as the case may be.

(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;

(C) violated any provision of section 317(c) or 509(a) of this title; or

(D) violated any provision of section 1304, 1343, 1464, or 2252 of title 18;

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.

(C) Notwithstanding subparagraph (A), if the violator is—

(i)

(I) a broadcast station licensee or permittee; or

(II) an applicant for any broadcast license, permit, certificate, or other instrument or authorization issued by the Commission; and

(ii) determined by the Commission under paragraph (1) to have broadcast obscene, indecent, or profane language, the amount of any forfeiture penalty determined under this subsection shall not exceed $325,000 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 $3,000,000 for any single act or failure to act.

(D) In any case not covered in subparagraph (A), (B), or (C), the amount of any forfeiture penalty determined under this subsection shall not exceed $10,000 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 $75,000 for any single act or failure to act described in paragraph (1) of this subsection.

(E) The amount of such forfeiture penalty shall be assessed by the Commission, or its designee, by written notice. In determining the amount of such a forfeiture penalty, the Commission or its designee shall take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require.

(F) Subject to paragraph (5) of this section, if the violator is a manufacturer or service provider subject to the requirements of section 255, 617, or 619 of this title, and is determined by the Commission to have violated any such requirement, the manufacturer or provider shall be liable to the United States for a forfeiture penalty of not more than $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.

(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.

(5) No forfeiture liability shall be determined under this subsection against any person, 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 notice required by paragraph (3) of this subsection or the notice of apparent liability required by paragraph (4) of this subsection, such person (A) is sent a citation of the violation charged; (B) is given a reasonable opportunity for a personal interview with an official of the Commission, at the field office of the Commission which is nearest to such person's place of residence; and (C) subsequently engages in conduct of the type described in such citation. The provisions of this paragraph shall not apply, however, if the person involved is engaging in activities for which a license, permit, certificate, or other authorization is required, or is a cable television system operator, if the person involved is transmitting on frequencies assigned for use in a service in which individual station operation is authorized by rule pursuant to section 307(e) of this title, or in the case of violations of section 303(q) of this title, if the person involved is a non-licensee tower owner who has previously received notice of the obligations imposed by section 303(q) of this title from the Commission or the permittee or licensee who uses

that tower. Whenever the requirements of this paragraph are satisfied with respect to a particular person, such person shall not be entitled to receive any additional citation of the violation charged, with respect to any conduct of the type described in the citation sent under this paragraph.

(6) No forfeiture penalty shall be determined or imposed against any person under this subsection if—

(A) such person holds a broadcast station license issued under subchapter III of this chapter and if the violation charged occurred—

(i) more than 1 year prior to the date of issuance of the required notice or notice of apparent liability; or

(ii) prior to the date of commencement of the current term of such license,

whichever is earlier; or

(B) such person does not hold a broadcast station license issued under subchapter III of this chapter and if the violation charged occurred more than 1 year prior to the date of issuance of the required notice or notice of apparent liability.

For purposes of this paragraph, "date of commencement of the current term of such license" 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) of this title

pending decision on an application for renewal of the license.

4. 47 U.S.C. § 504 provides:

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.

(b) Remission and mitigation

The forfeitures imposed by subchapter II, parts II and III of subchapter III, and sections 503(b) and 507 of this title shall be subject to remission or mitigation by the Commission under such regulations and methods of ascertaining the facts as may seem to it advisable, and, if suit has been instituted, the Attorney General, upon request of the Commission, shall direct the discontinuance of any prosecution to recover such forfeitures: Provided, however, That no forfeiture shall be remitted or mitigated after determination by a court of competent jurisdiction.

(c) Use of notice of apparent liability

In any case where the Commission issues a notice of apparent liability looking toward the imposition of a forfeiture under this chapter, that fact shall not be used, in any other proceeding before the Commission, to the prejudice of the person to whom such notice was issued, unless (i) the forfeiture has been paid, or (ii) a court of competent jurisdiction has ordered payment of such forfeiture, and such order has become final.

5. 47 C.F.R. § 1.80 provides in relevant part:

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.

(8) Violated section 60506 of the Infrastructure and Jobs Act of 2021 or 47 CFR part 16.

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—***

* * *

(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 $251,322 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 $2,513,215 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.

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 particular cases. The Commission and its staff retain the discretion to issue a higher or lower forfeiture than provided in the guidelines, to issue no forfeiture at all, or to apply alternative or additional sanctions as permitted by the statute. The forfeiture ceilings 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).

* * *

(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 violation 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 section 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.

* * *

(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) [*sic*] of this section, or (2) a notice of opportunity for hearing, in accordance with paragraph (g) [*sic*].

(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.

* * *

6. 47 C.F.R. § 64.2010 provides in relevant part:

Safeguards on the disclosure of customer proprietary network information.

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

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

(c) *Online access to CPNI.* A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online

access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

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

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

(f) *Notification of account changes.*

(1) Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten password, online account, or address of

record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

(2) Beginning on July 15, 2024, paragraph (f)(1) of this section does not apply to a change made in connection with a line separation request under 47 U.S.C. 345 and subpart II of this part.

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

(h) *Subscriber Identity Module (SIM) changes.* A provider of commercial mobile radio service (CMRS), as defined in 47 CFR 20.3, including resellers of wireless service, shall only effectuate SIM change requests in accordance with this section. For purposes of this section, SIM means a physical or virtual card associated with a device that stores unique information that can be identified to a specific mobile network.

(1) *Customer authentication.* A CMRS provider shall use secure methods to authenticate a customer that are reasonably designed to confirm the customer's identity before executing a SIM change request, except to the extent otherwise required by 47

U.S.C. 345 (Safe Connections Act of 2022) or subpart II of this part. Authentication methods shall not rely on readily available biographical information, account information, recent payment information, or call detail information unless otherwise permitted under 47 U.S.C. 345 or subpart II of this part. A CMRS provider shall regularly, but not less than annually, review and, as necessary, update its customer authentication methods to ensure that its authentication methods continue to be secure. A CMRS provider shall establish safeguards and processes so that employees who receive inbound customer communications are unable to access CPNI in the course of that customer interaction until after the customer has been properly authenticated.

(2)-(6) [Reserved]

(7) *Employee training.* A CMRS provider shall develop and implement training for employees to specifically address fraudulent SIM change attempts, complaints, and remediation. Training shall include, at a minimum, how to identify potentially fraudulent SIM change requests, how to identify when a customer may be the victim of SIM swap fraud, and how to direct potential victims and individuals making potentially fraudulent requests to employees specifically trained to handle such incidents.

(8) [Reserved]

(9) *Compliance.* This paragraph (h) contains information-collection and/or recordkeeping requirements. Compliance with this paragraph (h) will not be required until this paragraph is removed or contains a compliance date.