

No.

In the Supreme Court of the United States

FEDERAL COMMUNICATIONS COMMISSION AND
UNITED STATES OF AMERICA, PETITIONERS

v.

AT&T INC.

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

PETITION FOR A WRIT OF CERTIORARI

D. ADAM CANDEUB
General Counsel
BRADLEY CRAIGMYLE
Deputy General Counsel
JACOB M. LEWIS
Associate General Counsel
SARAH E. CITRIN
*Deputy Associate
General Counsel*
ADAM L. SORENSEN
Counsel
*Federal Communications
Commission*
Washington, DC 20554

D. JOHN SAUER
*Solicitor General
Counsel of Record*
ABIGAIL A. SLATER
Assistant Attorney General
MALCOLM L. STEWART
Deputy Solicitor General
VIVEK SURI
*Assistant to the
Solicitor General*
ROBERT B. NICHOLSON
MATTHEW A. WARING
Attorneys
*Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217*

QUESTION PRESENTED

The Communications Act of 1934, 47 U.S.C. 151 *et seq.*, empowers the Federal Communications Commission (FCC) to assess monetary forfeiture penalties for certain violations of the Act or the FCC's regulations by issuing a notice of apparent liability, giving the regulated party an opportunity to respond in writing, and then issuing a final decision. If the regulated party declines to pay and the government sues to collect the penalties, the regulated party is entitled to a *de novo* jury trial in a federal district court. Alternatively, the subject of an FCC forfeiture order may pay the monetary penalty and file a petition for review in a court of appeals, thereby triggering a judicial-review proceeding in which no jury is available. The question presented is as follows:

Whether the Communications Act provisions that govern the FCC's assessment and enforcement of monetary forfeitures are consistent with the Seventh Amendment and Article III.

RELATED PROCEEDINGS

United States Court of Appeals (5th Cir.):

FCC v. AT&T Inc., No. 24-60223 (Aug. 22, 2025)

TABLE OF CONTENTS

	Page
Opinions below	1
Jurisdiction.....	1
Constitutional and statutory provisions involved.....	2
Introduction.....	2
Statement	3
Reasons for granting the petition	7
A. The decision below is wrong.....	7
B. The decision below warrants this Court’s review	15
Conclusion	19
Appendix A — Court of appeals rehearing order and amended opinion (Aug. 22, 2025)	1a
Appendix B — Court of appeals withdrawn opinion (Apr. 17, 2025).....	23a
Appendix C — FCC order (Apr. 29, 2024)	46a
Appendix D — Statutory provisions.....	146a

TABLE OF AUTHORITIES

Cases:

<i>Beers v. Beers</i> , 4 Conn. 535 (1823)	9
<i>Blodgett v. Holden</i> , 275 U.S. 142 (1927)	15
<i>Capital Traction Co. v. Hof</i> , 174 U.S. 1 (1899)	2, 3, 8-10, 16
<i>Emerick v. Harris</i> , 1 Binn. 416 (Penn. 1808).....	10
<i>The Flint River Steamboat Co. v. Foster</i> , 5 Ga. 194 (1848)	9
<i>Henderson’s Distilled Spirits</i> , 14 Wall. 44 (1872).....	11
<i>Iancu v. Brunetti</i> , 588 U.S. 388 (2019)	16
<i>Keddie v. Moore</i> , 6 N.C. 41 (1811)	10
<i>Kennedy v. Braidwood Management, Inc.</i> , 145 S. Ct. 2427 (2025)	16
<i>Lamb v. Lane</i> , 4 Ohio St. 167 (1854)	9

IV

Cases—Continued:	Page
<i>The Lessee of Livingston v. Moore</i> , 7 Pet. 469 (1833).....	9
<i>McLaughlin Chiropractic Associates v. McKesson Corp.</i> , 606 U.S. 146 (2025)	7, 15
<i>Meeker v. Lehigh Valley Railroad Co.</i> , 236 U.S. 412 (1915).....	2, 3, 8, 10, 16
<i>Morford v. Barnes</i> , 16 Tenn. 444 (1835).....	9
<i>NLRB v. SW General, Inc.</i> , 580 U.S. 288 (2017)	14
<i>Parsons v. Bedford</i> , 3 Pet. 433 (1830).....	13
<i>Paul v. Davis</i> , 424 U.S. 693 (1976).....	12
<i>SEC v. Jarkesy</i> , 603 U.S. 109 (2024)	5, 7, 16-18
<i>Sprint Corp. v. FCC</i> , No. 24-1224, 2025 WL 2371009 (D.C. Cir. Aug. 15, 2025)	11-13, 16
<i>Steuart v. Baltimore</i> , 7 Md. 500 (1855)	9
<i>United States v. Rahimi</i> , 602 U.S. 680 (2024)	16
<i>United States v. Stevens</i> , 691 F.3d 620 (5th Cir. 2012), cert. denied, 568 U.S. 1090 (2013)	14
<i>Vidal v. Elster</i> , 602 U.S. 286 (2024)	16
<i>Verizon Communications Inc. v. FCC</i> , No. 24-1733, 2025 WL 2609127 (2d Cir. Sept. 10, 2025)	11, 12, 14, 17
Constitution, statutes, and regulations:	
U.S. Const.:	
Art. III.....	2, 3, 5-8, 10-12, 18
Amend. V (Due Process Clause).....	12
Amend. VII	2, 3, 5-13, 16-18
Act of June 29, 1906, ch. 3591, 34 Stat. 584:	
§ 5, 34 Stat. 590	8
Administrative Procedure Act, 5 U.S.C. 701 <i>et seq.</i>	4
Communications Act of 1934, 47 U.S.C. 151 <i>et seq.</i>	3
47 U.S.C. 222.....	7
47 U.S.C. 222(h)(1)(A)	5

V

Statutes and regulations—Continued:	Page
47 U.S.C. 312(a)	17
47 U.S.C. 312(b)	17
47 U.S.C. 402(a)	4
47 U.S.C. 503	3, 146a
47 U.S.C. 503(b)(1)(B)	3, 147a
47 U.S.C. 503(b)(3)	4
47 U.S.C. 503(b)(3)(A)	4, 149a
47 U.S.C. 503(b)(4)	4, 10, 11, 150a
47 U.S.C. 504	4-6, 10, 12-14, 16, 153a
47 U.S.C. 504(a)	4, 6, 7, 10, 11, 14, 15, 153a
47 U.S.C. 504(c)	13, 154a
47 U.S.C. 510	17
Communications Act Amendments, 1960, Pub. L. No. 86-752, § 7, 74 Stat. 894-895	3
Hobbs Act, 28 U.S.C. 2342	14, 15
28 U.S.C. 2342(1)	4
47 C.F.R. 64.2010	5

Miscellaneous:

Thomas M. Cooley, <i>A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union</i> (4th ed. 1878)	10
H.R. Rep. No. 1800, 86th Cong., 2d Sess. (1960)	17
S. Rep. No. 1857, 86th Cong., 2d Sess. (1960)	4

In the Supreme Court of the United States

No.

FEDERAL COMMUNICATIONS COMMISSION AND
UNITED STATES OF AMERICA, PETITIONERS

v.

AT&T INC.

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

PETITION FOR A WRIT OF CERTIORARI

OPINIONS BELOW

The court of appeals' amended opinion (App., *infra*, 1a-22a) is reported at 149 F.4th 491. The court of appeals' original opinion (App., *infra*, 23a-45a) is reported at 135 F.4th 230. The Federal Communications Commission's order (App., *infra*, 46a-145a) is available at 39 FCC Rcd 4216.

JURISDICTION

The court of appeals issued its judgment on April 17, 2025. The court amended its opinion and denied a petition for rehearing on August 22, 2025 (App., *infra*, 1a-22a). The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

**CONSTITUTIONAL AND STATUTORY
PROVISIONS INVOLVED**

Pertinent constitutional and statutory provisions are reproduced in the appendix. App., *infra*, 146a-156a.

INTRODUCTION

Federal law empowers the Federal Communications Commission (FCC or Commission) to assess monetary penalties against those who willfully or repeatedly violate the statutes and regulations that the agency administers. To obtain such penalties under the provisions at issue here, the Commission must first issue a notice of apparent liability, give the regulated party an opportunity to respond, and issue an initial decision. The regulated party may then decide whether to pay the penalty assessed by the FCC.

If the party declines to pay, the Department of Justice may bring a suit in federal district court to collect the penalty, and the party may demand a de novo jury trial in that suit. That statutory scheme allows the FCC to issue an initial decision applying its administrative expertise and policy judgment, while still ensuring that the regulated party may obtain a jury trial in an Article III court before it must pay the penalty. Yet in the decision below, the Fifth Circuit concluded that the FCC's initial assessment of the penalty violated the Seventh Amendment and Article III.

The Fifth Circuit's decision is wrong. This Court has twice held that Congress may commit the initial adjudication of a civil case to a non-Article III tribunal acting without a jury, so long as the parties may obtain de novo review in an Article III court with a jury. See *Meeker v. Lehigh Valley Railroad Co.*, 236 U.S. 412 (1915); *Capital Traction Co. v. Hof*, 174 U.S. 1 (1899). In the earlier of those cases, the Court explained that the Constitu-

tion “does not prescribe at what stage of an action a trial by jury” must occur, and that a statute may authorize such a trial “for the first time upon appeal” from an initial decision. *Hof*, 174 U.S. at 23. In the later case, the Court upheld a scheme (much like the one at issue here) under which an executive agency could issue initial decisions finding regulated parties liable for money damages, subject to review by a jury in an Article III court. See *Meeker*, 236 U.S. at 430-431. The court of appeals identified no basis for distinguishing this case from those precedents.

The decision below warrants this Court’s review. The Court usually grants review when, as here, a court of appeals has held a federal statute unconstitutional. In addition, the Fifth Circuit’s decision conflicts with recent decisions of two other courts of appeals that have rejected similar Seventh Amendment challenges to the FCC penalty scheme. And the decision below has serious practical consequences, since it deprives the Commission of one of its most important regulatory remedies and severely impairs the agency’s ability to enforce federal communications law. This Court should grant the petition for a writ of certiorari.

STATEMENT

1. The Communications Act of 1934 (Act), 47 U.S.C. 151 *et seq.*, establishes the FCC and empowers it to regulate communications services. Under Section 503 of the Act, which Congress added to the statute in 1960, persons who have “willfully or repeatedly failed to comply” with the Act or the agency’s regulations (or who have committed certain other violations) “shall be liable to the United States for a forfeiture penalty.” 47 U.S.C. 503(b)(1)(B); see Communications Act Amendments, 1960, Pub. L. No. 86-752, § 7, 74 Stat. 894-895.

The Act establishes two alternative administrative procedures through which the FCC may seek monetary penalties. Under the procedure at issue here, the Commission issues a written notice of apparent liability, gives the regulated party an opportunity to respond in writing, and then issues a decision. See 47 U.S.C. 503(b)(4). Under the other procedure, the FCC issues a decision after a hearing before either an administrative law judge or the Commission itself. See 47 U.S.C. 503(b)(3).

When the FCC issues a notice of apparent liability and then a forfeiture order, the regulated party has two options for obtaining judicial review of the monetary forfeiture. First, the party may pay the penalty and file a petition for review in a court of appeals under the Hobbs Act, 28 U.S.C. 2342(1). See 47 U.S.C. 402(a), 503(b)(3)(A). The court must then review the agency's order under standards prescribed by the Administrative Procedure Act, 5 U.S.C. 701 *et seq.*, in a proceeding that does not involve a jury.

Alternatively, the party may simply decline to pay the penalty. To enforce the FCC's order and collect the money, the Department of Justice must then file a civil suit in federal district court under Section 504 of the Act. See 47 U.S.C. 504(a). A civil suit under Section 504 "shall be a trial de novo." *Ibid.* A Section 504 suit therefore is more than "merely a collection proceeding"; it enables the defendant "to contest * * * the merits" of the agency decision. S. Rep. No. 1857, 86th Cong., 2d Sess. 10 (1960).

2. In 2020, the FCC issued a notice of apparent liability to respondent AT&T, seeking a forfeiture penalty based on allegations that respondent had willfully and repeatedly violated its statutory and regulatory duty to

protect the confidentiality of its customers' data. See App., *infra*, 7a-8a (citing 47 U.S.C. 222(h)(1)(A) and 47 C.F.R. 64.2010). The allegations involved respondent's location-based services—*i.e.*, services that track cell-phone users' locations in order to provide information such as maps and traffic alerts. See *id.* at 5a-6a. The agency alleged that respondent had sold its customers' location data to third parties without verifying the customers' consent. See *id.* at 6a-7a.

After reviewing respondent's written response, the FCC assessed a forfeiture penalty of \$57,265,625. App., *infra*, 46a-145a. Respondent argued that imposition of the penalty would violate the Seventh Amendment and Article III. The Commission rejected that argument, explaining that Section 504 entitled respondent "to a trial *de novo* in federal district court before it can be required to pay the forfeiture." *Id.* at 116a.

3. Respondent paid the penalty and filed a petition for review in the Fifth Circuit, which granted the petition and vacated the FCC's order. App., *infra*, 23a-45a. The government then sought rehearing; the court denied that request but amended its opinion. *Id.* at 1a-22a. Except where noted otherwise, this brief discusses and cites the amended opinion.

The court of appeals determined that the FCC's imposition of the forfeiture penalty had violated the Seventh Amendment and Article III, which generally require that suits at common law brought before federal adjudicators must be tried by juries and resolved by Article III courts. See App., *infra*, 9a-22a. Citing *SEC v. Jarkesy*, 603 U.S. 109 (2024), the court observed that the determination whether a particular case is a suit at common law covered by the Seventh Amendment depends on the nature of the remedy sought and the na-

ture of the cause of action. See App., *infra*, 10a. The court concluded that both factors weigh in favor of trial by jury here because civil penalties are an “archetypal common law remedy,” and an action to recover such penalties for failing to safeguard private customer data is “closely analogous to a [common-law] negligence action.” *Id.* at 13a-14a.

The court of appeals then rejected the government’s argument that this case falls within the public-rights doctrine, which allows Congress to assign certain types of matters to executive agencies rather than to courts and juries. See App., *infra*, 14a-20a. The court concluded that, because the regulation of common carriers is “deeply rooted in the common law,” “it would be bizarre to situate a negligence action against carriers within the ‘historic categories of adjudications’ falling *outside* Article III” and the Seventh Amendment. *Id.* at 16a-17a (citation omitted).

Finally, the court of appeals rejected the government’s argument that Section 504’s authorization of a “trial de novo,” 47 U.S.C. 504(a), satisfies the Seventh Amendment and Article III. See App., *infra*, 20a-21a. The court stated that, even before the government brings a Section 504 suit, the FCC’s penalty orders “have real-world impacts”: The agency “must consider any history of prior adjudicated offenses in imposing future penalties,” and the agency’s orders “cause reputational harm to carriers.” *Ibid.*

In its original opinion, the court of appeals had found a Section 504 trial constitutionally inadequate on the additional ground that (in the court of appeals’ view) the district court in such a trial could review only the FCC’s factual findings, not its legal conclusions. See App., *infra*, 43a-44a. But the court “excise[d]” that analysis in

its amended opinion, explaining that the circuit precedent on which the analysis was based had been “called into question” by this Court’s intervening decision in *McLaughlin Chiropractic Associates v. McKesson Corp.*, 606 U.S. 146 (2025). App., *infra*, 21a n.16.

Judge Haynes concurred in the judgment but did not write a separate opinion. App., *infra*, 1a n.*.

REASONS FOR GRANTING THE PETITION

The Fifth Circuit erred in holding that the FCC forfeiture order at issue here violates the Seventh Amendment and Article III. The court’s decision warrants this Court’s review because it holds an Act of Congress unconstitutional, conflicts with this Court’s precedents and with decisions of two other courts of appeals, and has significant practical consequences.

A. The Decision Below Is Wrong

The Seventh Amendment preserves the right to trial by jury in “Suits at common law” where the amount in controversy exceeds \$20. When suits at common law are resolved by federal adjudicators, Article III ordinarily requires that the suits be tried by courts rather than executive agencies. See *SEC v. Jarkesy*, 603 U.S. 109, 136 (2024). The government does not seek review of the Fifth Circuit’s holdings that (a) a case in which the FCC seeks a forfeiture penalty to enforce Section 222 of the Act is a suit at common law and (b) such a suit falls outside the public-rights exception to the Seventh Amendment and Article III. But contrary to the decision below, the statutory review scheme here satisfies the Seventh Amendment and Article III because Section 504(a) entitled respondent to a de novo jury trial in district court before the monetary penalty could be collected.

1. The Constitution allows a non-Article III federal tribunal to adjudicate a suit at common law without a jury, so long as the parties are entitled to a subsequent de novo jury trial in an Article III court. In *Capital Traction Co. v. Hof*, 174 U.S. 1 (1899), the Court upheld a federal statute that authorized a District of Columbia justice of the peace to resolve a civil suit without a common-law jury, but that provided a right to jury trial on appeal to the Supreme Court of the District of Columbia (later renamed the U.S. District Court for the District of Columbia). See *id.* at 4-5. The Court observed that the Seventh Amendment “does not prescribe at what stage of an action a trial by jury must, if demanded, be had.” *Id.* at 23. The Court further explained that “the constitutional right of trial by jury in civil actions is not infringed by a statute which * * * allows a trial by jury for the first time upon appeal from the judgment of the justice of the peace.” *Ibid.*

In *Meeker v. Lehigh Valley Railroad Co.*, 236 U.S. 412 (1915), this Court similarly upheld a statute that empowered the Interstate Commerce Commission (ICC) to make an initial award of damages to a party injured by a carrier’s violation of the statute, but that allowed the carrier to demand a jury trial when the injured party sued in an Article III court to collect the damages. See Act of June 29, 1906, ch. 3591, § 5, 34 Stat. 590. Even though the statute directed that “the findings and order of the [ICC] shall be *prima facie* evidence of the facts therein stated,” this Court determined that the statute “does not abridge the right of trial by jury.” *Meeker*, 236 U.S. at 430. The Court emphasized that the statute “cuts off no defense, interposes no obstacle to a full contestation of all the issues, and takes no question of fact from either court or jury.” *Ibid.*

Hof and *Meeker* reflected the original understanding of the scope of the “right of trial by jury” that the Seventh Amendment had “preserved.” At the Founding, many States allowed justices of the peace or executive officers to issue initial decisions in civil cases without juries, subject to review by juries on appeal to courts of record. See *Hof*, 174 U.S. at 17 (collecting statutes). In 1801, Congress incorporated one such state law, originally enacted by Maryland, into the laws of the District of Columbia. See *id.* at 20. And in 1823, Congress enacted the statute that this Court subsequently upheld in *Hof*. See *id.* at 31-36.

In a “long line of judicial decisions,” beginning early in the 19th century, courts held that such statutes complied with state constitutional provisions securing the right to jury trial in civil cases. *Hof*, 174 U.S. at 23. In *The Lessee of Livingston v. Moore*, 7 Pet. 469 (1833), for example, this Court considered a Pennsylvania statute that allowed the State’s comptroller to adjudicate liability for debts owed to the State, subject to later review by a jury. See *id.* at 541-542; see also *Hof*, 174 U.S. at 21-22. The Court held that the statute complied with the state constitution’s civil-jury clause because “the right of an appeal to a jury [wa]s secured to the debtor.” *Livingston*, 7 Pet. at 552. State courts agreed that a law “may provide for a primary trial without the intervention of a jury,” so long as the law “secures the trial by jury upon an appeal,” thereby ensuring that either party “can have his case decided by a jury before it is finally settled.” *Steuart v. Baltimore*, 7 Md. 500, 512 (1855); see, e.g., *Lamb v. Lane*, 4 Ohio St. 167, 180 (1854); *The Flint River Steamboat Co. v. Foster*, 5 Ga. 194, 204-209 (1848); *Morford v. Barnes*, 16 Tenn. 444, 446 (1835); *Beers v. Beers*, 4 Conn. 535, 539-540 (1823);

Keddie v. Moore, 6 N.C. 41, 45 (1811); *Emerick v. Harris*, 1 Binn. 416, 424 (Penn. 1808). Summarizing those decisions, a leading 19th-century commentator explained that a legislature may “deny to parties the privilege of a [jury] trial in a court of first instance, provided the right is allowed on appeal.” Thomas M. Cooley, *A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union* 513 (4th ed. 1878).

2. The forfeiture-penalty scheme here complies with the Seventh Amendment and Article III, as interpreted in *Hof* and *Meeker* and as understood at the Founding. Under Section 503(b)(4) of the Act, the FCC may issue an initial decision that finds a regulated party liable for a forfeiture penalty. But under Section 504, the regulated party need not pay the penalty unless the United States files a suit to collect it. Because the defendant in a Section 504 proceeding may demand a jury trial, “the constitutional right of trial by jury in civil actions is not infringed.” *Hof*, 174 U.S. at 23.

In one respect, this case is easier than *Meeker*. The federal statute at issue in *Meeker* authorized an executive agency to issue an initial order awarding damages to a private party, and the statute specified that the agency’s findings would be prima facie evidence of the relevant facts in any later jury trial. See 236 U.S. at 430. The statute at issue here, by contrast, entitles the regulated party to “a trial de novo,” 47 U.S.C. 504(a), and does not require the court or the jury to treat the FCC’s findings even as prima facie evidence. If the statute this Court upheld in *Meeker* “d[id] not abridge the right of trial by jury,” 236 U.S. at 430, Section 504(a) does not do so either.

Common sense confirms that Section 503(b)(4) of the Act complies with the Constitution. Consistent with the Seventh Amendment and Article III, Congress could simply have empowered the Department of Justice—on its own, without the FCC’s involvement—to file suit in district court seeking monetary penalties from private parties. In enacting the forfeiture scheme at issue here, Congress instead required the Commission to issue an initial decision assessing a penalty before the Department of Justice may sue. That extra layer of protection cannot sensibly be viewed as rendering the statute unconstitutional.

To be sure, respondent did not actually receive a jury trial in this case, since it elected instead to pay the forfeiture and file a petition for review in the court of appeals. But because the statutory scheme *entitled* respondent to a de novo trial by jury before the monetary forfeiture could be collected, respondent’s choice to invoke an alternative review mechanism in which a jury is unavailable is properly viewed as a waiver of its Seventh Amendment right. See *Sprint Corp. v. FCC*, No. 24-1224, 2025 WL 2371009, at *6 (D.C. Cir. Aug. 15, 2025) (holding that regulated parties that petitioned for review of an FCC forfeiture order “had the right to a jury trial” but “chose not to wait for such a trial and therefore waived that right”); *Verizon Communications Inc. v. FCC*, No. 24-1733, 2025 WL 2609127, at *14 (2d Cir. Sept. 10, 2025) (similar); see also *Henderson’s Distilled Spirits*, 14 Wall. 44, 53 (1872) (explaining that, although “the claimant was entitled to a trial by jury,” the parties had “entered into a stipulation waiving a jury and submitted the case to the court upon an agreed statement of facts, as they had a right to do”). If Section 504(a)’s provision for “trial de novo” otherwise satisfies the Sev-

enth Amendment and Article III, Congress’s decision to provide regulated parties an alternative avenue for review cannot create a constitutional violation.

3. The Fifth Circuit’s contrary analysis is unsound. The court stated that an FCC penalty order triggers the Seventh Amendment and Article III because it subjects the regulated party to adverse “real-world impacts” even before the Department of Justice sues to collect the penalty. App., *infra*, 20a. The court did not dispute, however, that the regulated party may legally decline to pay the penalty unless and until the government files suit and prevails in a Section 504 trial. Nor did the court suggest that a party’s refusal to pay the penalty before such a trial can provide a basis for criminal punishment or civil sanctions.

The court of appeals instead worried that the FCC’s penalty orders can “cause reputational harm.” App., *infra*, 21a. But the possibility of such harm does not make the Commission’s orders unconstitutional. First, harm to reputation is not a deprivation of life, liberty, or property within the meaning of the Due Process Clause. See *Paul v. Davis*, 424 U.S. 693, 701-712 (1976). A federal agency therefore need not provide any process at all, much less a jury trial in an Article III court, before taking action that could affect someone’s reputation.

Second, the prospect of reputational harm standing alone is insufficient to trigger the Seventh Amendment’s protections. See *Sprint*, 2025 WL 2371009, at *8 (explaining that, for Seventh Amendment purposes, “no legal rights are determined and no legal relief is awarded if the Commission declines to enforce an order” imposing a monetary forfeiture); *Verizon*, 2025 WL 2609127, at *15 (explaining that practical impacts other than the imposition of monetary sanctions do not

“implicate the Seventh Amendment, which requires a jury trial only upon an effort to collect payment of monetary damages”). For example, the Amendment does not require a jury trial before a court grants equitable relief, see *Parsons v. Bedford*, 3 Pet. 433, 446 (1830), even though an order granting such relief could impair a defendant’s reputation no less than an award of money damages. Third, the initial juryless decisions in *Hof* and *Meeker* likewise could have caused reputational harm to the losing party. Yet this Court held in both cases that the availability of a jury on judicial review of the initial decision satisfied the Seventh Amendment.

The court of appeals also noted that the FCC may “consider any history of prior adjudicated offenses in imposing future penalties.” App., *infra*, 21a. But the Communications Act provides that, “[i]n any case where the Commission issues a notice of apparent liability looking toward the imposition of a forfeiture,” “that fact shall not be used, in any other proceeding before the Commission, to the prejudice” of the regulated party unless the party has paid the forfeiture or a court order requiring payment has become final. 47 U.S.C. 504(c); see *Sprint*, 2025 WL 2371009, at *8 (citing Section 504(c) and stating that “it is plainly incorrect that, absent an enforcement proceeding, the Commission could have used its orders affirming the [monetary forfeitures] against the Carriers in future proceedings”). A Commission penalty order therefore cannot be used against the regulated party in subsequent proceedings unless and until the party pays the penalty or the government files and wins a Section 504 suit. And if the agency considers a party’s past violations “in imposing future penalties,” App., *infra*, 21a, those follow-on deci-

sions are themselves subject to de novo review in Section 504 suits.

4. The court of appeals’ original opinion expressed the understanding that, in a Section 504 suit, the regulated party could contest only the factual findings (and not the legal conclusions) made by the FCC in assessing the forfeiture. See App., *infra*, 43a-44a. The court cited *United States v. Stevens*, 691 F.3d 620, 622 (5th Cir. 2012), cert. denied, 568 U.S. 1090 (2013), in support of that proposition, see App., *infra*, 43a-44a; and the *Stevens* court drew that limitation from 28 U.S.C. 2342, a provision of the Hobbs Act, see *Stevens*, 691 F.3d at 622-623. The court of appeals’ original opinion here identified that supposed limitation on the scope of a Section 504 trial as an additional reason to view the statutory scheme as unconstitutional. App., *infra*, 44a. That analysis is wrong for two reasons.

First, under the “commonplace of statutory construction that the specific governs the general,” *NLRB v. SW General, Inc.*, 580 U.S. 288, 305 (2017) (citation omitted), the Communications Act provisions that specifically address FCC forfeiture-recovery suits take precedence over the Hobbs Act provisions that generally govern review of FCC orders. A proceeding in which the defendant was barred from contesting the FCC’s prior legal determinations could not reasonably be viewed as a “trial de novo.” 47 U.S.C. 504(a). See *Verizon*, 2025 WL 2609127, at *15 (“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.”). And the Fifth Circuit in *Stevens* did not explain why 28 U.S.C. 2342’s general rules for judicial review of FCC orders should

supersede Section 504(a)’s specific directive as to the scope of review in a district-court suit to enforce an FCC monetary forfeiture. The principle that ambiguous statutory language should be construed if possible to avoid a constitutional infirmity reinforces the conclusion that Section 504(a)’s directive should be given precedence.

Second, this Court’s intervening decision in *McLaughlin Chiropractic Associates v. McKesson Corp.*, 606 U.S. 146 (2025), supersedes the *Stevens* court’s analysis of Section 2342. This Court held in *McLaughlin* that the Hobbs Act “does not preclude district courts in enforcement proceedings from independently assessing whether an agency’s interpretation of the relevant statute is correct.” *Id.* at 152. In its amended opinion, the court of appeals here recognized that “*Stevens* has possibly been called into question” by the intervening decision in *McLaughlin*, and the court accordingly “excise[d]” the discussion of *Stevens* from its original opinion. App., *infra*, 21a n.16. There is consequently no reason to doubt that, in a Section 504(a) enforcement suit brought by the government, the defendant may contest the legal (as well as the factual) determinations underlying the relevant FCC forfeiture order.

B. The Decision Below Warrants This Court’s Review

The Fifth Circuit’s decision warrants this Court’s review because it holds an Act of Congress unconstitutional, conflicts with this Court’s precedents and with recent decisions of two other circuits, and, if left in place, would significantly impede the FCC’s enforcement of the Communications Act.

1. Judging the constitutionality of a federal statute is “the gravest and most delicate duty that this Court is called on to perform.” *Blodgett v. Holden*, 275 U.S. 142, 148 (1927) (opinion of Holmes, J.). Accordingly, “when

a lower court has invalidated a federal statute,” the Court’s “usual” approach is to grant certiorari. *Iancu v. Brunetti*, 588 U.S. 388, 392 (2019). The Court has recently and repeatedly reviewed decisions invalidating federal statutes even in the absence of a circuit conflict. See, e.g., *Kennedy v. Braidwood Management, Inc.*, 145 S. Ct. 2427, 2442 (2025); *SEC v. Jarkesy*, 603 U.S. 109, 120 (2024); *United States v. Rahimi*, 602 U.S. 680, 690 (2024); *Vidal v. Elster*, 602 U.S. 286, 292 (2024).

2. The decision below conflicts with this Court’s precedents. *Hof* establishes that the Seventh Amendment “does not prescribe at what stage of an action a trial by jury must, if demanded, be had,” and that “the constitutional right of trial by jury in civil actions is not infringed by a statute which * * * allows a trial by jury for the first time upon appeal from the [initial decision].” 174 U.S. at 23. *Meeker* similarly establishes that a statute empowering an executive agency to adjudicate claims for money damages, subject to review by juries in enforcement suits, “does not abridge the right of trial by jury.” 236 U.S. at 430. The court of appeals did not explain how its decision here could be reconciled with those precedents.

The Fifth Circuit’s decision in this case also conflicts with recent decisions of the D.C. Circuit and Second Circuit. In *Sprint*, the D.C. Circuit determined that, because Section 504 allows a party “to obtain a jury trial before suffering any legal consequences,” the Communications Act’s procedures for imposing forfeiture penalties comply with the Seventh Amendment. 2025 WL 2371009, at *6. The court acknowledged the Fifth Circuit’s contrary decision in this case but disagreed with the Fifth Circuit’s analysis. See *id.* at *7-*8. Similarly in *Verizon*, the Second Circuit held that Section 504

complies with the Seventh Amendment because it provides “a *de novo* jury trial if the government [sues] to collect.” 2025 WL 2609127, at *14. Like the D.C. Circuit, the Second Circuit disagreed with the Fifth Circuit’s analysis. See *id.* at *15.

3. Finally, the decision below has significant practical consequences. The FCC has described civil penalties as among the agency’s “most important regulatory remedies”; as “a top priority”; and as “an area of bipartisan agreement.” C.A. Doc. 111-1, at 18 (July 16, 2025) (citation omitted). The Commission relies on such penalties to enforce a variety of statutory and regulatory provisions, including provisions that protect consumer privacy, prohibit unlicensed broadcasting, and restrict robocalls. See *ibid.* Though the Act empowers the agency to seek other remedies—such as forfeiture of equipment, cease-and-desist orders, and orders revoking or suspending licenses or permits, see 47 U.S.C. 312(a) and (b) and 510—such remedies are less flexible and less frequently used than monetary penalties. “[T]he power to impose monetary forfeitures” gives the agency “an effective tool in dealing with violations” in circumstances where more draconian remedies, such as “revocation or suspension” of licenses or permits, do “not appear to be appropriate.” H.R. Rep. No. 1800, 86th Cong., 2d Sess. 17 (1960).

The difference between the statutory scheme here and the statutory scheme in *Jarkesy* underscores the severity of those consequences. The statute in *Jarkesy* authorized the Securities and Exchange Commission (SEC) to seek civil penalties either by commencing an administrative proceeding within the agency or by filing suit in federal court. See 603 U.S. at 117-118. This Court held that the SEC’s imposition of penalties in the

agency proceeding violated the Seventh Amendment, but its decision left the SEC free to seek such penalties in court. See *id.* at 120-121.

The Communications Act, by contrast, does not authorize either the FCC or the Department of Justice to seek monetary penalties in court without an antecedent administrative proceeding in which the Commission formally determines that a regulated party has violated the law. The court of appeals held that the mandated administrative proceeding itself violates the Seventh Amendment and Article III, since the Commission's liability determination may give rise to reputational and similar harms even before any monetary penalties are collected. The Fifth Circuit's holding that the Section 504 enforcement procedure is unconstitutional leaves the FCC with no alternative avenue for seeking monetary penalties, seriously impairing the agency's ability to enforce the statute.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

D. ADAM CANDEUB
General Counsel
 BRADLEY CRAIGMYLE
Deputy General Counsel
 JACOB M. LEWIS
Associate General Counsel
 SARAH E. CITRIN
*Deputy Associate
 General Counsel*
 ADAM L. SORENSEN
*Counsel
 Federal Communications
 Commission*

D. JOHN SAUER
Solicitor General
 ABIGAIL A. SLATER
Assistant Attorney General
 MALCOLM L. STEWART
Deputy Solicitor General
 VIVEK SURI
*Assistant to the
 Solicitor General*
 ROBERT B. NICHOLSON
 MATTHEW A. WARING
Attorneys

OCTOBER 2025

APPENDIX

TABLE OF CONTENTS

	Page
Appendix A — Court of appeals rehearing order and amended opinion (Aug. 22, 2025)	1a
Appendix B — Court of appeals withdrawn opinion (Apr. 17, 2025).....	23a
Appendix C — FCC order (Apr. 29, 2024)	46a
Appendix D — Statutory provisions:	
47 U.S.C. 503	146a
47 U.S.C. 504	153a

APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 24-60223

AT&T, INCORPORATED, PETITIONER

v.

FEDERAL COMMUNICATIONS COMMISSION;
UNITED STATES OF AMERICA, RESPONDENTS

Filed: Aug. 22, 2025

Petition for Review of the Federal Communications
Commission Agency No. 24-40

Before HAYNES, DUNCAN, and WILSON, *Circuit
Judges*.^{*}

STUART KYLE DUNCAN, *Circuit Judge*:

Because no member of the panel or judge in regular active service requested that the court be polled on rehearing en banc (FED. R. APP. P. 35 and 5th CIR. R. 35), the petition for rehearing en banc is DENIED. We withdraw our previous opinion at 135 F.4th 230, and substitute the following.

* * *

^{*} JUDGE HAYNES concurs in the judgment only.

AT&T seeks review of a Federal Communications Commission forfeiture order. In an internal proceeding, the Commission found that AT&T violated section 222 of the Telecommunications Act by mishandling customer data and fined the company \$57 million. AT&T's petition argues, among other things, that the in-house adjudication violated the Constitution by denying it an Article III decisionmaker and a jury trial. Guided by *SEC v. Jarkesy*, 603 U.S. 109 (2024), we agree with AT&T.

Accordingly, we grant the petition and vacate the forfeiture order.

I

A

We first outline section 222 of the Telecommunications Act and then explain the Commission's procedures for enforcing it.

1

Under section 222, telecommunications carriers must protect the confidentiality of “customer proprietary network information” (“CPNI”). 47 U.S.C. § 222(a). CPNI 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).

Section 222 further provides that carriers “[e]xcept as required by law or with the approval of the customer . . . shall only use, disclose, or permit access to indi-

vidually 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. . . . ” *Id.* § 222(c)(1). Commission regulations flesh out these responsibilities. Carriers “must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI,” 47 C.F.R. § 64.2010(a), and they may use or disclose CPNI only with customers’ “opt-in approval.” *Id.* § 64.2007(b).

2

The Commission assesses forfeiture penalties for violations of the Act, including violations of section 222. 47 U.S.C. § 503(b)(3)(A). The Commission adjudicates alleged violations in two ways: either by assigning a case to an administrative law judge (“ALJ”) or by investigating and adjudicating the case itself. *Ibid.* The choice is entirely up to the Commission. *Ibid.*¹ Unsurprisingly perhaps, the Commission typically opts to investigate and adjudicate violations itself, as it did here. That process works as follows.

First, upon receiving information about a potential violation, the Commission’s Enforcement Bureau opens an investigation into a carrier. The Bureau can gather information through letters of inquiry sent to the car-

¹ Section 503(b)(3)(A) provides in full:

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 judge therefore 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.

rier, which may include interrogatories and requests for production. *Enforcement Primer*, FEDERAL COMMUNICATIONS COMMISSION, <https://perma.cc/FMQ2-ZH7C>. It may also compel documents and testimony through administrative subpoenas. *Ibid.* If the Bureau suspects a violation has occurred, it issues a charging document to the carrier called a Notice of Apparent Liability for Forfeiture (“NAL”). 47 U.S.C. § 503(b)(4)(A). An NAL advises the carrier how it violated the law and proposes a penalty.

To assess the amount of a penalty, the Commission “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.” *Id.* § 503(b)(2)(E). Any penalty “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. . . .” *Id.* § 503(b)(2)(B).

Once the Commission issues an NAL, the carrier may respond in writing to explain why it should incur no penalty. *Id.* § 503(b)(4)(C). After considering this response, the Commission decides whether to affirm the NAL. If it affirms, the Commission issues a forfeiture order. The written response is the only way a carrier can oppose a NAL. That is, a carrier receives neither a hearing nor a trial before it incurs a Commission forfeiture order and accompanying penalty. *See AT&T Corp. v. FCC*, 323 F.3d 1081, 1083 (D.C. Cir. 2003) (alleged violators can challenge NAL in writing only).

Two paths exist for a carrier to seek review of forfeiture orders.

On the first path, a carrier fails to timely pay the penalty, which becomes a debt to the United States. 47 U.S.C. § 504(a). The Commission refers the debt to the United States Attorney General (DOJ) for a collection action in federal district court. *Ibid.* If DOJ pursues the action, the carrier is entitled to a trial *de novo* (we refer to this as a “section 504 trial”).

On the second path, a carrier timely pays the penalty and seeks review in the appropriate court of appeals. *See AT&T Corp.*, 323 F.3d at 1084; *see also* 47 U.S.C. § 402(a). The carrier may challenge the order’s legal validity but, by choosing this path, forgoes a jury trial. *See AT&T Corp.*, 323 F.3d at 1084.

B

Next, we sketch this case’s factual and procedural background.

1

AT&T provides its customers with voice, text, and data services. To make and receive calls and to transmit data, customers’ phones periodically “register,” or “check in,” with nearby signal towers. Because AT&T knows where these towers are, it can calculate the approximate location of its customers’ phones. AT&T uses this location information to maintain network function and to provide services to customers.

At issue here is AT&T’s former location-based services program, which it discontinued March 2019. Location-based services give users up-to-date information about their surroundings, such as maps and traffic in-

formation. They also include services from providers like Life Alert and AAA, which depend upon customers' locations.

While nothing is wrong in principle with providing location-based services, the Commission took issue with how AT&T protected its customers' location data. To implement location-based services, AT&T contracted with "location aggregators," who collected customers' location data. The aggregators, in turn, sold this data to service providers like Life Alert or AAA.

Before allowing those sales, however, AT&T would review a service provider's "use case," where the provider described why it needed the location data and how it obtained customers' opt-in consent to use the data. (That the providers—as opposed to AT&T—obtained users' consent would be important in the Commission's section 222 analysis.) AT&T's program also required providers to obtain and document customer consent for every location request.

While AT&T reviewed the providers' consent records daily, it did not verify customer consent before providing access to location data. AT&T also required aggregators to monitor providers and to comply with various security requirements, such as vulnerability scanning and encryption. At the same time, AT&T could cut off access to customer location information at any time.

Beginning in May 2018, several news articles reported problems with AT&T's (and other carriers') location-based services programs. Put simply, it became clear that some service providers were misusing or failing to

protect customer location data.² After learning about this, AT&T promptly terminated those providers' access to the data. And by March 2019, AT&T stopped providing location data to all aggregators for use by any location-based service provider.

In May 2018, prompted by such news reports, the Commission's Enforcement Bureau began investigating AT&T and eventually sent the company a letter of inquiry seeking information about its location-based services program. AT&T complied with the investigation.

In February 2020, the Commission issued AT&T an NAL for willful and repeated violations of section 222 of the Act and section 64.2010 of the Commission's rules. The NAL proposed a \$57,265,625 penalty. Responding in writing, AT&T argued that: (1) location information is not subject to the Act because it is not CPNI, and, in any event, AT&T lacked fair notice that location information is CPNI; (2) AT&T acted reasonably; (3) the forfeiture amount was arbitrary and capricious; and (4) the Commission's enforcement regime is unconstitutional under Article III, the Seventh Amendment, and the non-delegation doctrine.

In April 2024, the Commission rejected all of AT&T's arguments and affirmed the proposed \$57 million penalty. In short, the Commission decided that: (1) CPNI relates to the "location" of a telecommunications service

² One example was Securus Technologies, which provided location services to law enforcement and correctional facilities. Securus allegedly allowed officers to access customer location data without a customer's consent, so long as officers uploaded a document (like a warrant) authorizing the location request. The problem was that Securus did not verify whether uploaded documents actually authorized the request.

under § 222(h)(1)(A) because a carrier must be aware of and use the device’s location for customers to send and receive calls; (2) that section speaks for itself and thus gave AT&T notice; (3) AT&T acted unreasonably by relying on providers to enforce safeguards against unauthorized access to location information³; and (4) AT&T’s constitutional arguments failed because (a) the possibility of a section 504 trial satisfied the Seventh Amendment and Article III, and (b) the Commission’s ability to choose between enforcement procedures did not implicate the nondelegation doctrine.⁴

The Commission therefore issued a forfeiture order demanding AT&T pay the \$57 million penalty within 30 days.

AT&T elected to timely pay the penalty and seek review in our court. Before us, the company raises the same arguments it raised before the Commission.

We resolve AT&T’s appeal based on its Seventh Amendment and Article III challenges to the Commission’s enforcement regime, which we review *de novo*. *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 412-13 (2024). So, we need not reach the other issues AT&T raises.⁵

³ Specifically, the Commission found that AT&T committed 84 continuing violations of the Act and that its failures were willful or repeated.

⁴ Two Commissioners dissented from the NAL. One thought CPNI does not include customer location data; but if it did, AT&T lacked notice of that. The other thought the forfeiture amount was unreasonable.

⁵ Specifically, those issues are: whether the Commission’s discretion to choose between an NAL or ALJ violates the nondelegation doctrine; whether the Commission lacked statutory authority to is-

II

AT&T argues that the Commission’s enforcement procedures violate its Seventh Amendment right to a jury trial and its right to adjudication by an Article III court.

Our analysis is governed by *SEC v. Jarkesy*, 603 U.S. 109 (2024). In that case, the Supreme Court ruled that the Seventh Amendment prohibited the SEC from requiring respondents to defend themselves before an agency, rather than a jury, against civil penalties for alleged securities fraud. *Id.* at 140. The Court also ruled that the case did not fall within the “public rights” exception, which would let Congress assign certain matters to an agency instead of an Article III court. *Id.* at 134.

We must determine whether, following *Jarkesy*, the Commission’s enforcement regime also violates the Seventh Amendment and Article III.

A

The Seventh Amendment provides in relevant part:

In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved[.]

U.S. CONST. amend. VII. The threshold question is whether the Commission’s enforcement proceeding qualifies as a “suit at common law.” A common law suit is one that is “legal in nature,” as opposed to one sounding in the realm of equity or admiralty. *See Jarkesy*, 603 U.S. at 122 (quoting *Granfinanciera, S. A. v. Nordberg*,

sue the forfeiture order; and whether the forfeiture order is arbitrary and capricious.

492 U.S. 33, 53 (1989)); *see ibid.* (“[T]he Framers used the term ‘common law’ in the Amendment in contradistinction to equity, and admiralty, and maritime jurisprudence.” (quoting *Parsons v. Bedford*, 3 Pet. 433, 446 (1830))).

How do we tell whether a suit is legal in nature? By considering two things: the cause of action and the remedy provided. *Id.* at 123.

1

We start with the remedy because it is the “more important” consideration. *Ibid.* (quoting *Granfinanciera*, 492 U.S. at 421).

The Commission’s civil penalties “are the prototypical common law remedy.” *Ibid.* They are money damages designed to “punish or deter” violators of section 222. *Ibid.* This is evident from the statutory factors, which instruct the Commission to set penalties by reference to “the nature, circumstances, extent, and gravity of the violation” as well as the violator’s “degree of culpability.” 47 U.S.C. § 503(b)(2)(E). It is also evident from the considerations the Commission used to set AT&T’s penalty, such as whether AT&T acted “willfully” and “repeatedly” and whether the violations were “serious.” *Cf. Jarkesy*, 603 U.S. at 123 (noting the statutory penalty factors included whether a defendant was a repeat offender and whether its conduct was deliberate).

Moreover, the penalties are not remedial. They are not designed “solely to ‘restore the status quo.’” *Ibid.* (quoting *Tull v. United States*, 481 U.S. 412, 422 (1987)); *see also United States v. Hoffman*, 901, F.3d 523, 560-61 (5th Cir. 2018) (“As opposed to restitution which is remedial, forfeiture is punitive.”). Nor are they meant to

compensate victims whose location data was compromised. *See* 47 U.S.C. § 504(a) (“The forfeitures provided for in this chapter shall be payable into the Treasury of the United States”); *cf. Jarkesy*, 603 U.S. at 124 (noting SEC was “not obligated to return any money to victims”).

So, like the penalties in *Jarkesy*, the civil penalties here are “a type of remedy at common law that could only be enforced in courts of law.” *Id.* at 125 (quoting *Tull*, 481 U.S. at 422). That “is all but dispositive” of the Seventh Amendment issue. *Id.* at 123.

2

Saying nothing about the remedy, the Commission instead focuses on the second consideration, the nature of the cause of action. It argues that an action to enforce section 222 does not bear a “close relationship” to any common law cause of action and that, as a result, the Seventh Amendment does not apply. We disagree.

As AT&T argues, the section 222 action is analogous to common law negligence.⁶ The action punishes carriers for failing to take reasonable measures to protect customers’ personal data. *See* 47 C.F.R. § 64.2010(a) (“[Carriers] must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.”). The Commission decided whether AT&T violated section 222 by repeatedly asking whether the company had acted reasonably.

⁶ AT&T also argues the action is analogous to common law actions for intrusion upon seclusion and eavesdropping. We need not address that argument.

For example, the Commission found AT&T unreasonably failed to protect customer data by relying on aggregators to enforce procedural safeguards, instead of enforcing the safeguards itself. The Commission also found AT&T's safeguards to be unreasonable because the company continued to provide customer location data to aggregators, despite reports of unauthorized disclosures. And the Commission found AT&T acted unreasonably by failing to "rectify the systemic vulnerabilities at the heart of its [] program." In sum, the Commission assessed AT&T's protection of customer location data entirely in terms of the reasonableness of the company's actions.

Such analysis is a staple of the common law. "An act or an omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm, even though such conduct is criminal." RESTATEMENT (SECOND) OF TORTS § 302B (2024). This familiar tort mirrors the Commission's analysis of AT&T's actions: "[AT&T's] failure to adequately protect CPNI for a protracted amount of time caused substantial harm by making it possible for malicious actors to identify the exact locations of AT&T subscribers who belong to law enforcement, military, government, or other highly sensitive positions—thereby threatening national security and public safety. . . . " The Commission's action, then, is analogous to common law negligence.

The Commission responds that section 222 is not analogous to negligence but instead is a "highly reticulated and technical scheme" for safeguarding customer data. That is a false choice. The Seventh Amend-

ment applies to common law suits “whatever may be the peculiar form which they may assume.” *Jarkesy*, 603 U.S. at 122 (quoting *Parsons*, 3 Pet. at 447); *see also Tull*, 481 U.S. at 418-19 (“Actions by the Government to recover civil penalties under statutory provisions therefore historically have been viewed as one type of action in debt requiring trial by jury.”). However “technical” section 222 may be, its substance is closely analogous to a negligence action.

The Commission also points out that, unlike the securities laws in *Jarkesy*, section 222 does not borrow common law terms like “negligence” or “reasonable care.” *Cf. Jarkesy*, 603 U.S. at 125 (noting “Congress deliberately used ‘fraud’ and other common law terms of art” in the securities laws). That is partially true—the scheme does not use the term “negligence” but does speak of “reasonable measures”—but in any event it is not determinative. Yes, a statute’s borrowing common law terms may show its kinship to a common law action. *Cf. ibid.* (“Congress’s decision to draw upon common law fraud created an enduring link between federal securities fraud and its common law ‘ancestor.’”) (cleaned up). The key inquiry, though, is not what terminology the statute uses but whether the statute “target[s] the same basic conduct” as the common law claim. *Ibid.* The answer here is yes: section 222 action targets a carrier’s negligence in handling customer data.

Moreover, as *Jarkesy* explained, the statutory action need not be “identical” to a common law analogue. *See id.* at 126 (“That is not to say that federal securities fraud and common law fraud are identical.”); *id.* at 135 (“[I]f the action resembles a traditional legal claim, its statutory origins are not dispositive.” (citing *Granfi-*

nanciera, 492 U.S. at 52)). All that is needed is a “close relationship,” *Jarkesy*, 603 U.S. at 126, and section 222 satisfies that requirement.

To be sure, the relationship between the section 222 action and a common law analogue is not as obvious as it was in *Jarkesy*. But ambiguity on this second consideration points us back to the “more important” first consideration—remedy. *Jarkesy*, 603 U.S. at 123. As noted, section 222 imposes the archetypal common law remedy of money damages, which is “all but dispositive” of the Seventh Amendment issue. *Ibid.*

B

The Commission next defends its enforcement proceeding under the “public rights” exception, which, it contends, lets Congress assign the proceeding to an agency rather than a court. We disagree.

1

Suits at common law presumptively concern “private rights” and must be adjudicated by Article III courts. *Jarkesy*, 603 U.S. at 127 (citing *Stern v. Marshall*, 564 U.S. 462, 484 (2011)). “The Constitution prohibits Congress from ‘withdraw[ing] [such matters] from judicial cognizance.’” *Ibid.* (quoting *Murray’s Lessee v. Hoboken Land & Improvement Co.*, 18 How. 272, 284 (1856) (second brackets added)). “Public rights” cases, however, may be channeled to agencies instead of courts. *Ibid.*

This narrow exception to Article III applies only to matters that “historically could have been determined exclusively by [the executive and legislative] branches.” *Id.* at 128 (quoting *Stern*, 564 U.S. at 493). While the Supreme Court has not “definitively explained” what di-

vides public from private rights, it has pointed to “historic categories of adjudications” occurring outside Article III. *Id.* at 131, 130. Examples include revenue collection, foreign commerce, immigration, tariffs, tribal relations, public lands, public benefits, and patents. *Id.* at 128-30.⁷ That said, the exception must be handled “with care.” *Id.* at 131. “[E]ven with respect to matters that arguably fall within the scope of the ‘public rights’ doctrine, the presumption is in favor of Article III courts.” *Id.* at 132 (quoting *Northern Pipeline Constr. Co. v. Marathon Pipe Line Co.*, 458 U.S. 50, 69 n.23 (1982)).

2

The Commission argues its enforcement action falls within the public rights exception because it involves common carriers. *See Nat’l Cable & Telecommunications Ass’n v. Brand X Internet Servs.*, 545 U.S. 967, 975 (2005) (“The [Communications] Act regulates telecommunications carriers . . . as common carriers.”). Given that common carriers like AT&T are “affected with a public interest,” *Munn v. Illinois*, 94 U.S. 113, 130 (1876), the Commission contends Congress could as-

⁷ *See Murray’s Lessee*, 18 How. at 281, 285 (action to compel federal customs collector to pay public funds into Treasury); *Oceanic Steam Nav. Co. v. Stranahan*, 214 U.S. 320, 335 (1909) (action to enforce fine on steamship company for disobeying federal prohibition on allowing immigration by aliens with contagious diseases); *Ex parte Bakelite Corp.*, 279 U.S. 438, 458 (1929) (assessment of President’s tariffs on goods imported by “unfair methods of competition”); *United States v. Jicarilla Apache Nation*, 564 U.S. 162, 174 (2011) (relations with Indian tribes); *Crowell v. Benson*, 285 U.S. 22, 51 & n.13 (1932) (administration of public lands); *ibid.* (public benefits such as veterans benefits and pensions); *United States v. Duell*, 172 U.S. 576, 582-83 (1899) (patent rights).

sign adjudication of civil penalties against them to agencies instead of courts. For several reasons, we disagree.

First, the Commission’s proposal would blow a hole in what is meant to be a narrow exception to Article III. Myriad enterprises might be said to implicate the “public interest.”⁸ And Congress’s power to regulate common carriers is broad. *See Glob. Crossing Telecommunications, Inc. v. Metrophones Telecommunications, Inc.*, 550 U.S. 45, 48 (2007) (“When Congress enacted the Communications Act of 1934, it granted the FCC broad authority to regulate interstate telephone communications.”). If injected into the public rights exception, this combination would empower Congress to bypass Article III adjudication in countless matters. But the Supreme Court has cautioned that the doctrine is a narrow and extra-textual “*exception*” to presumptively mandatory Article III jurisdiction. *Jarkesy*, 603 U.S. at 131.

Second, the common carrier doctrine is deeply rooted in the common law. *See, e.g., NetChoice*, 49 F.4th at 469 (“The common carrier doctrine is a body of common law dating back long before our Founding.”).⁹ Negligence

⁸ *See NetChoice, L.L.C. v. Paxton*, 49 F.4th 439, 445 (5th Cir. 2022) (social media activity), *overruled on other grounds by Moody v. NetChoice, L.L.C.*, 603 U.S. 707 (2024); *Fed. Power Comm’n v. Hope Nat. Gas Co.*, 320 U.S. 591, 611 (1944) (natural gas operations); *Nat’l Union Fire Ins. Co. v. Wanberg*, 260 U.S. 71, 74 (1922) (hail insurance); *New York v. FERC*, 535 U.S. 1, 19 (2002) (electric energy).

⁹ *See* 19 CHARLES ALAN WRIGHT, ARTHUR R. MILLER & EDWARD H. COOPER, *Federal Practice and Procedure* § 4514 (3d ed. 2024) (citing cases placing common carriers’ liability within the federal common law because such liability involves significant federal interests); *see also* Robert J. Kaczorowski, *The Common-Law Back-*

claims against common carriers have been routinely adjudicated in state and federal courts. See, e.g., *Cole v. Goodwin & Storey*, 19 Wend. 251, 281 (N.Y. Sup. Ct. 1839) (a “coach proprietor’s” common carrier status made it strictly liable in tort).¹⁰ In light of that, it would be bizarre to situate a negligence action against carriers within the “historic categories of adjudications” falling *outside* Article III. *Jarkesy*, 603 U.S. at 130.¹¹

Third, the cases cited by the Commission fail to show that the public rights exception generally applies to common carriers. Some of the cases involved actions far afield from this one, such as public benefits or actions falling within federal admiralty jurisdiction.¹² Those

ground of Nineteenth-Century Tort Law, 51 Ohio State L.J. 1127, 1132 (1990) (explaining that “the common law imposed on persons engaged in a common calling a duty of reasonable care and a standard of professional competence”).

¹⁰ See also *New Jersey Steam Nav. Co. v. Merch.’s Bank of Bos.*, 47 U.S. 344 (1848) (steamboat operator liable for losses at sea); *S. Exp. Co. v. Purcell*, 37 Ga. 103 (1867) (railroad for loss of cotton bales); *Duggan v. New Jersey & W. Ferry Co.*, 76 A. 636 (Del. Super. Ct. 1909) (ferry operator for personal injuries); *Goldstein v. Northern Pac. Ry. Co.*, 164 N.D. 602 (1917) (railroad for conversion); *Korner v. Cosgrove*, 108 Ohio St. 484 (1923) (taxicab operator for employee’s assault of a passenger); *Callaway v. Hart*, 146 F.2d 103 (5th Cir. 1944) (railroad for negligently leaving doors open) *Andrews v. United Airlines, Inc.*, 24 F.3d 39 (9th Cir. 1994) (airline for luggage falling on passenger).

¹¹ Nor does it matter that this action is brought by the Government. The Supreme Court “ha[s] never held that ‘the presence of the United States as a proper party to the proceeding is . . . sufficient’ by itself to trigger the [public rights] exception.” *Jarkesy*, 603 U.S. at 135.

¹² See *Scripps-Howard Radio v. FCC*, 316 U.S. 4 (1942) (addressing FCC order granting application for a construction permit and station license); *Red Lion Broad. Co. v. FCC*, 395 U.S. 367 (1969)

actions arguably fall within the historical categories of non-Article III adjudications listed in *Jarkesy*. See 603 U.S. at 130. Whether they do or not, though, they do not involve anything like a negligence action against a common carrier for money damages.

It is true that federal agencies like the Commission have long had regulatory authority over common carriers, such as when setting rates or granting licenses. See, e.g., *Virginian Ry. Co. v. United States*, 272 U.S. 658 (1926) (discussing the Interstate Commerce Commission’s oversight of railroad carriers).¹³ But that does not imply, as the Commission seems to think, that any regulatory action concerning common carriers implicates the public rights exception and can therefore be “siphon[ed] . . . away from an Article III court.” *Jarkesy*, 603 U.S. at 135.

Not even the first modern administrative agency thought that was so.¹⁴ The Interstate Commerce Commission, while empowered to regulate common carriers and recommend monetary penalties, believed its enforcement actions were subject to the Seventh Amendment and so, necessarily, to Article III adjudication.

(addressing “fairness doctrine” governing content carriers could broadcast over radio frequency); *Crowell*, 285 U.S. 22 (addressing challenge to the Longshoremen’s and Harbor Workers’ Compensation Act of 1927).

¹³ See also *Burlington N., Inc. v. United States*, 459 U.S. 131, 141 (1982) (discussing Commission’s authority to set rates); *Regents of Univ. Sys. of Ga. v. Carroll*, 338 U.S. 586, 598 (1950) (discussing Commission’s authority to grant licenses); *Belluso v. Turner Commc’ns Corp.*, 633 F.2d 393, 397 (5th Cir. 1980) (discussing the Commission’s authority to sanction licensees).

¹⁴ See LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 439 (2d ed. 1985). The ICC was the FCC’s predecessor.

The agency’s 1887 report, issued the year it was created, stated that its power “must be so construed as to harmonize with the seventh amendment to the Federal Constitution, which preserves the right of trial by jury in common-law suits.” 1887 Interstate Com. Comm’n Ann. Rep. 27; *see also* Richard L. Jolly, *The Administrative State’s Jury Problem*, 98 Wash. L. Rev. 1187, 1242 (2023) (quoting Report’s conclusion that it was “unquestionable that parties can not [*sic*] be deprived of [the jury] right through conferring authority to award reparation upon a tribunal that sits without a jury as assistant”). The Commission takes no account of this history, which is flatly inconsistent with exempting its enforcement action from Article III adjudication.¹⁵

* * *

Ultimately, “what matters” for Article III purposes “is the substance of the suit, not where it is brought, who brings it, or how it is labeled.” *Jarkesy*, 603 U.S. at 135. As explained, this matter involves an action closely analogous to a common law negligence action—and, importantly, one where the Commission seeks “civil

¹⁵ Consistent with this history is *Meeker v. Lehigh Valley R.R. Co.*, 236 U.S. 412, 430 (1915), which involved an ICC action targeting a railroad’s unreasonable rates. The Supreme Court addressed whether a provision treating the ICC’s initial factfinding as a “rebuttable presumption” that could be reconsidered in a later jury trial comported with the Seventh Amendment. *Ibid.* Unlike the Commission’s action against AT&T here, the ICC action there (rate setting) had no common law analogue. Even so, the Court assumed the railroad had a jury right in the action and held the provision does not violate the Seventh Amendment because “[i]t cuts off no defense, interposes no obstacle to a full contestation of all the issues, and takes no question of fact from either court or jury.” *Ibid.*

penalties, a punitive remedy that [the Supreme Court] ha[s] recognized ‘could only be enforced in courts of law.’” *Id.* at 134 (quoting *Tull*, 481 U.S. at 422). Accordingly, the public rights exception does not apply and Article III adjudication is mandatory. *Id.* at 128.

C

Finally, the Commission argues that, even if the Seventh Amendment and Article III apply, the proceeding here meets their demands.

The Commission points to the possibility of a back-end section 504 trial. Recall that a carrier who fails to timely pay a forfeiture penalty may be sued by DOJ in federal district court. *See* 47 U.S.C. § 504(a). The Commission suggests this would give a carrier everything promised by the Seventh Amendment and Article III. We disagree.

To begin with, by the time DOJ sues (if it does), the Commission would have already adjudged a carrier guilty of violating section 222 and levied fines. This case shows how the process works. The Commission investigated AT&T, issued a charging document (the NAL), and received AT&T’s written objections. The Commission then affirmed the NAL by making fact findings, interpreting section 222, and applying that understanding to the facts it had found. This resulted in a forfeiture order concluding AT&T had violated the law and imposing \$57 million in penalties. So, in this process, which was completely in-house, the Commission acted as prosecutor, jury, and judge.

Such forfeiture orders, furthermore, are not mere suggestions—to the contrary, they have real-world impacts on carriers. For example, the Commission must

consider any history of prior adjudicated offenses in imposing future penalties. *See* 47 U.S.C. § 503(b)(2)(E) (“In determining the amount of such a forfeiture penalty, the Commission or its designee shall take into account . . . any history of prior offenses. . . .”). Unsurprisingly, they also cause reputational harm to carriers because they can be widely publicized and reported. *See FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 256 (2012) (explaining forfeiture orders’ impact on carriers’ reputations). And consider the risks to a carrier of even getting to the section 504 trial: the carrier must refuse to pay a penalty and wait for DOJ to drag it into court.

In light of this, we reject the Commission’s argument that a section 504 enforcement proceeding satisfies Article III and the Seventh Amendment. The Commission cites no authority supporting the proposition that the constitutional guarantee of a jury trial is honored by a trial occurring after an agency has already found the facts, interpreted the law, adjudged guilt, and levied punishment.¹⁶

¹⁶ Our original opinion noted another problem with a section 504 trial: under our precedent, the district court could consider a petitioner’s challenge to the factual basis for the agency action but was foreclosed from challenging its legal basis. *See AT&T, Inc. v. F.C.C.*, 135 F.4th 230, 242 (5th Cir. 2025) (citing *United States v. Stevens*, 691 F.3d 620, 622 (5th Cir. 2012)). Because *Stevens* has possibly been called into question by a Supreme Court decision issued after our panel opinion, we excise that part of the opinion as unnecessary to our holding. *See McLaughlin Chiropractic Assocs., Inc. v. McKesson Corp.*, 145 S. Ct. 2006, 2013 (2025) (holding district courts may assess the Commission’s interpretation of a statute in Hobbs Act enforcement proceedings).

IV

No one denies the Commission's authority to enforce laws requiring telecommunications companies like AT&T to protect sensitive customer data. But the Commission must do so consistent with our Constitution's guarantees of an Article III decisionmaker and a jury trial.

Accordingly, we GRANT AT&T's petition and VACATE the Commission's forfeiture order.

APPENDIX B

UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 24-60223

AT&T, INCORPORATED, PETITIONER

v.

FEDERAL COMMUNICATIONS COMMISSION;
UNITED STATES OF AMERICA, RESPONDENTS

Filed: Apr. 17, 2025

Petition for Review of the Federal Communications
Commission Agency No. 24-40

Before HAYNES, DUNCAN, and WILSON, *Circuit
Judges*.^{*}

STUART KYLE DUNCAN, *Circuit Judge*:

AT&T seeks review of a Federal Communications Commission forfeiture order. In an internal proceeding, the Commission found that AT&T violated section 222 of the Telecommunications Act by mishandling customer data and fined the company \$57 million. AT&T's petition argues, among other things, that the in-house adjudication violated the Constitution by denying it an Article III decisionmaker and a jury trial. Guided by

^{*} JUDGE HAYNES concurs in the judgment only.

SEC v. Jarkesy, 603 U.S. 109 (2024), we agree with AT&T.

Accordingly, we grant the petition and vacate the forfeiture order.

I

A

We first outline section 222 of the Telecommunications Act and then explain the Commission’s procedures for enforcing it.

1

Under section 222, telecommunications carriers must protect the confidentiality of “customer proprietary network information” (“CPNI”). 47 U.S.C. § 222(a). CPNI 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).

Section 222 further provides that carriers “[e]xcept as required by law or with the approval of the customer . . . 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. . . .” *Id.* § 222(c)(1). Commission regulations flesh out these responsibilities. Carriers “must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI,”

47 C.F.R. § 64.2010(a), and they may use or disclose CPNI only with customers’ “opt-in approval.” *Id.* § 64.2007(b).

2

The Commission assesses forfeiture penalties for violations of the Act, including violations of section 222. 47 U.S.C. § 503(b)(3)(A). The Commission adjudicates alleged violations in two ways: either by assigning a case to an administrative law judge (“ALJ”) or by investigating and adjudicating the case itself. *Ibid.* The choice is entirely up to the Commission. *Ibid.*¹ Unsurprisingly perhaps, the Commission typically opts to investigate and adjudicate violations itself, as it did here. That process works as follows.

First, upon receiving information about a potential violation, the Commission’s Enforcement Bureau opens an investigation into a carrier. The Bureau can gather information through letters of inquiry sent to the carrier, which may include interrogatories and requests for production. *Enforcement Primer*, Federal Communications Commission, <https://perma.cc/FMQ2-ZH7C>. It may also compel documents and testimony through administrative subpoenas. *Ibid.* If the Bureau suspects a violation has occurred, it issues a charging document to the carrier called a Notice of Apparent Liability for

¹ Section 503(b)(3)(A) provides in full:

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 judge therefore 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.

Forfeiture (“NAL”). 47 U.S.C. § 503(b)(4)(A). An NAL advises the carrier how it violated the law and proposes a penalty.

To assess the amount of a penalty, the Commission “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.” *Id.* § 503(b)(2)(E). Any penalty “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. . . . ” *Id.* § 503(b)(2)(B).

Once the Commission issues an NAL, the carrier may respond in writing to explain why it should incur no penalty. *Id.* § 503(b)(4)(C). After considering this response, the Commission decides whether to affirm the NAL. If it affirms, the Commission issues a forfeiture order. The written response is the only way a carrier can oppose a NAL. That is, a carrier receives neither a hearing nor a trial before it incurs a Commission forfeiture order and accompanying penalty. *See AT&T Corp. v. FCC*, 323 F.3d 1081, 1083 (D.C. Cir. 2003) (alleged violators can challenge NAL in writing only).

Two paths exist for a carrier to seek review of forfeiture orders.

On the first path, a carrier fails to timely pay the penalty, which becomes a debt to the United States. 47 U.S.C. § 504(a). The Commission refers the debt to the United States Attorney General (DOJ) for a collection action in federal district court. *Ibid.* If DOJ pursues the action, the carrier is entitled to a trial *de novo* (we

refer to this as a “section 504 trial”). At trial, however, the carrier may challenge only the order’s factual basis, not its legal validity. See *United States v. Stevens*, 691 F.3d 620, 622 (5th Cir. 2012) (in section 504(a) action, district court was “limited to considering the factual basis for the agency action” but not petitioner’s “legal arguments”).

On the second path, a carrier timely pays the penalty and seeks review in the appropriate court of appeals. See *AT&T Corp.*, 323 F.3d at 1084; see also *Stevens*, 691 F.3d at 623 (noting “the courts of appeals['] . . . exclusive jurisdiction . . . to determine the validity of final FCC forfeiture orders”) (quoting 28 U.S.C. § 2342(1)) (cleaned up); see also 47 U.S.C. § 402(a). The carrier may challenge the order’s legal validity but, by choosing this path, forgoes a jury trial. See *AT&T Corp.*, 323 F.3d at 1084.

B

Next, we sketch this case’s factual and procedural background.

1

AT&T provides its customers with voice, text, and data services. To make and receive calls and to transmit data, customers’ phones periodically “register,” or “check in,” with nearby signal towers. Because AT&T knows where these towers are, it can calculate the approximate location of its customers’ phones. AT&T uses this location information to maintain network function and to provide services to customers.

At issue here is AT&T’s former location-based services program, which it discontinued March 2019. Location-based services give users up-to-date infor-

mation about their surroundings, such as maps and traffic information. They also include services from providers like Life Alert and AAA, which depend upon customers' locations.

While nothing is wrong in principle with providing location-based services, the Commission took issue with how AT&T protected its customers' location data. To implement location-based services, AT&T contracted with "location aggregators," who collected customers' location data. The aggregators, in turn, sold this data to service providers like Life Alert or AAA.

Before allowing those sales, however, AT&T would review a service provider's "use case," where the provider described why it needed the location data and how it obtained customers' opt-in consent to use the data. (That the providers—as opposed to AT&T—obtained users' consent would be important in the Commission's section 222 analysis.) AT&T's program also required providers to obtain and document customer consent for every location request.

While AT&T reviewed the providers' consent records daily, it did not verify customer consent before providing access to location data. AT&T also required aggregators to monitor providers and to comply with various security requirements, such as vulnerability scanning and encryption. At the same time, AT&T could cut off access to customer location information at any time.

Beginning in May 2018, several news articles reported problems with AT&T's (and other carriers') location-based services programs. Put simply, it became clear that some service providers were misusing or fail-

ing to protect customer location data.² After learning about this, AT&T promptly terminated those providers' access to the data. And by March 2019, AT&T stopped providing location data to all aggregators for use by any location-based service provider.

2

In May 2018, prompted by such news reports, the Commission's Enforcement Bureau began investigating AT&T and eventually sent the company a letter of inquiry seeking information about its location-based services program. AT&T complied with the investigation.

In February 2020, the Commission issued AT&T an NAL for willful and repeated violations of section 222 of the Act and section 64.2010 of the Commission's rules. The NAL proposed a \$57,265,625 penalty. Responding in writing, AT&T argued that: (1) location information is not subject to the Act because it is not CPNI, and, in any event, AT&T lacked fair notice that location information is CPNI; (2) AT&T acted reasonably; (3) the forfeiture amount was arbitrary and capricious; and (4) the Commission's enforcement regime is unconstitutional under Article III, the Seventh Amendment, and the non-delegation doctrine.

In April 2024, the Commission rejected all of AT&T's arguments and affirmed the proposed \$57 million pen-

² One example was Securus Technologies, which provided location services to law enforcement and correctional facilities. Securus allegedly allowed officers to access customer location data without a customer's consent, so long as officers uploaded a document (like a warrant) authorizing the location request. The problem was that Securus did not verify whether uploaded documents actually authorized the request.

alty. In short, the Commission decided that: (1) CPNI relates to the “location” of a telecommunications service under § 222(h)(1)(A) because a carrier must be aware of and use the device’s location for customers to send and receive calls; (2) that section speaks for itself and thus gave AT&T notice; (3) AT&T acted unreasonably by relying on providers to enforce safeguards against unauthorized access to location information³; and (4) AT&T’s constitutional arguments failed because (a) the possibility of a section 504 trial satisfied the Seventh Amendment and Article III, and (b) the Commission’s ability to choose between enforcement procedures did not implicate the nondelegation doctrine.⁴

The Commission therefore issued a forfeiture order demanding AT&T pay the \$57 million penalty within 30 days.

AT&T elected to timely pay the penalty and seek review in our court. Before us, the company raises the same arguments it raised before the Commission.

We resolve AT&T’s appeal based on its Seventh Amendment and Article III challenges to the Commission’s enforcement regime, which we review *de novo*. *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 412-13

³ Specifically, the Commission found that AT&T committed 84 continuing violations of the Act and that its failures were willful or repeated.

⁴ Two Commissioners dissented from the NAL. One thought CPNI does not include customer location data; but if it did, AT&T lacked notice of that. The other thought the forfeiture amount was unreasonable.

(2024). So, we need not reach the other issues AT&T raises.⁵

II

AT&T argues that the Commission’s enforcement procedures violate its Seventh Amendment right to a jury trial and its right to adjudication by an Article III court.

Our analysis is governed by *SEC v. Jarkesy*, 603 U.S. 109 (2024). In that case, the Supreme Court ruled that the Seventh Amendment prohibited the SEC from requiring respondents to defend themselves before an agency, rather than a jury, against civil penalties for alleged securities fraud. *Id.* at 140. The Court also ruled that the case did not fall within the “public rights” exception, which would let Congress assign certain matters to an agency instead of an Article III court. *Id.* at 134.

We must determine whether, following *Jarkesy*, the Commission’s enforcement regime also violates the Seventh Amendment and Article III.

A

The Seventh Amendment provides in relevant part:

In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved[.]

⁵ Specifically, those issues are: whether the Commission’s discretion to choose between an NAL or ALJ violates the nondelegation doctrine; whether the Commission lacked statutory authority to issue the forfeiture order; and whether the forfeiture order is arbitrary and capricious.

U.S. Const. amend. VII. The threshold question is whether the Commission’s enforcement proceeding qualifies as a “suit at common law.” A common law suit is one that is “legal in nature,” as opposed to one sounding in the realm of equity or admiralty. *See Jarkesy*, 603 U.S. at 122 (quoting *Granfinanciera, S. A. v. Nordberg*, 492 U.S. 33, 53 (1989)); *see ibid.* (“[T]he Framers used the term ‘common law’ in the Amendment in contradistinction to equity, and admiralty, and maritime jurisprudence.” (quoting *Parsons v. Bedford*, 3 Pet. 433, 446 (1830))).

How do we tell whether a suit is legal in nature? By considering two things: the cause of action and the remedy provided. *Id.* at 123.

1

We start with the remedy because it is the “more important” consideration. *Ibid.* (quoting *Granfinanciera*, 492 U.S. at 421).

The Commission’s civil penalties “are the prototypical common law remedy.” *Ibid.* They are money damages designed to “punish or deter” violators of section 222. *Ibid.* This is evident from the statutory factors, which instruct the Commission to set penalties by reference to “the nature, circumstances, extent, and gravity of the violation” as well as the violator’s “degree of culpability.” 47 U.S.C. § 503(b)(2)(E). It is also evident from the considerations the Commission used to set AT&T’s penalty, such as whether AT&T acted “willfully” and “repeatedly” and whether the violations were “serious.” *Cf. Jarkesy*, 603 U.S. at 123 (noting the statutory penalty factors included whether a defendant was a repeat offender and whether its conduct was deliberate).

Moreover, the penalties are not remedial. They are not designed “solely to ‘restore the status quo.’” *Ibid.* (quoting *Tull v. United States*, 481 U.S. 412, 422 (1987)); see also *United States v. Hoffman*, 901, F.3d 523, 560-61 (5th Cir. 2018) (“As opposed to restitution which is remedial, forfeiture is punitive.”). Nor are they meant to compensate victims whose location data was compromised. See 47 U.S.C. § 504(a) (“The forfeitures provided for in this chapter shall be payable into the Treasury of the United States”); cf. *Jarkesy*, 603 U.S. at 124 (noting SEC was “not obligated to return any money to victims”).

So, like the penalties in *Jarkesy*, the civil penalties here are “a type of remedy at common law that could only be enforced in courts of law.” *Id.* at 125 (quoting *Tull*, 481 U.S. at 422). That “is all but dispositive” of the Seventh Amendment issue. *Id.* at 123.

2

Saying nothing about the remedy, the Commission instead focuses on the second consideration, the nature of the cause of action. It argues that an action to enforce section 222 does not bear a “close relationship” to any common law cause of action and that, as a result, the Seventh Amendment does not apply. We disagree.

As AT&T argues, the section 222 action is analogous to common law negligence.⁶ The action punishes carriers for failing to take reasonable measures to protect customers’ personal data. See 47 C.F.R. § 64.2010(a) (“[Carriers] must take reasonable measures to discover

⁶ AT&T also argues the action is analogous to common law actions for intrusion upon seclusion and eavesdropping. We need not address that argument.

and protect against attempts to gain unauthorized access to CPNI.”). The Commission decided whether AT&T violated section 222 by repeatedly asking whether the company had acted reasonably.

For example, the Commission found AT&T unreasonably failed to protect customer data by relying on aggregators to enforce procedural safeguards, instead of enforcing the safeguards itself. The Commission also found AT&T’s safeguards to be unreasonable because the company continued to provide customer location data to aggregators, despite reports of unauthorized disclosures. And the Commission found AT&T acted unreasonably by failing to “rectify the systemic vulnerabilities at the heart of its [] program.” In sum, the Commission assessed AT&T’s protection of customer location data entirely in terms of the reasonableness of the company’s actions.

Such analysis is a staple of the common law. “An act or an omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm, even though such conduct is criminal.” RESTATEMENT (SECOND) OF TORTS § 302B (2024). This familiar tort mirrors the Commission’s analysis of AT&T’s actions: “[AT&T’s] failure to adequately protect CPNI for a protracted amount of time caused substantial harm by making it possible for malicious actors to identify the exact locations of AT&T subscribers who belong to law enforcement, military, government, or other highly sensitive positions—thereby threatening national security and public safety. . . . ” The Commission’s action, then, is analogous to common law negligence.

The Commission responds that section 222 is not analogous to negligence but instead is a “highly reticulated and technical scheme” for safeguarding customer data. That is a false choice. The Seventh Amendment applies to common law suits “whatever may be the peculiar form which they may assume.” *Jarkesy*, 603 U.S. at 122 (quoting *Parsons*, 3 Pet. at 447); *see also Tull*, 481 U.S. at 418-19 (“Actions by the Government to recover civil penalties under statutory provisions therefore historically have been viewed as one type of action in debt requiring trial by jury.”). However “technical” section 222 may be, its substance is closely analogous to a negligence action.

The Commission also points out that, unlike the securities laws in *Jarkesy*, section 222 does not borrow common law terms like “negligence” or “reasonable care.” *Cf. Jarkesy*, 603 U.S. at 125 (noting “Congress deliberately used ‘fraud’ and other common law terms of art” in the securities laws). That is partially true—the scheme does not use the term “negligence” but does speak of “reasonable measures”—but in any event it is not determinative. Yes, a statute’s borrowing common law terms may show its kinship to a common law action. *Cf. ibid.* (“Congress’s decision to draw upon common law fraud created an enduring link between federal securities fraud and its common law ‘ancestor.’”) (cleaned up). The key inquiry, though, is not what terminology the statute uses but whether the statute “target[s] the same basic conduct” as the common law claim. *Ibid.* The answer here is yes: section 222 action targets a carrier’s negligence in handling customer data.

Moreover, as *Jarkesy* explained, the statutory action need not be “identical” to a common law analogue. *See*

id. at 126 (“That is not to say that federal securities fraud and common law fraud are identical.”); *id.* at 135 (“[I]f the action resembles a traditional legal claim, its statutory origins are not dispositive.” (citing *Granfinanciera*, 492 U.S. at 52)). All that is needed is a “close relationship,” *Jarkesy*, 603 U.S. at 126, and section 222 satisfies that requirement.

To be sure, the relationship between the section 222 action and a common law analogue is not as obvious as it was in *Jarkesy*. But ambiguity on this second consideration points us back to the “more important” first consideration—remedy. *Jarkesy*, 603 U.S. at 123. As noted, section 222 imposes the archetypal common law remedy of money damages, which is “all but dispositive” of the Seventh Amendment issue. *Ibid.*

B

The Commission next defends its enforcement proceeding under the “public rights” exception, which, it contends, lets Congress assign the proceeding to an agency rather than a court. We disagree.

1

Suits at common law presumptively concern “private rights” and must be adjudicated by Article III courts. *Jarkesy*, 603 U.S. at 127 (citing *Stern v. Marshall*, 564 U.S. 462, 484 (2011)). “The Constitution prohibits Congress from ‘withdraw[ing] [such matters] from judicial cognizance.’” *Ibid.* (quoting *Murray’s Lessee v. Hoboken Land & Improvement Co.*, 18 How. 272, 284 (1856) (second brackets added)). “Public rights” cases, however, may be channeled to agencies instead of courts. *Ibid.*

This narrow exception to Article III applies only to matters that “historically could have been determined exclusively by [the executive and legislative] branches.” *Id.* at 128 (quoting *Stern*, 564 U.S. at 493). While the Supreme Court has not “definitively explained” what divides public from private rights, it has pointed to “historic categories of adjudications” occurring outside Article III. *Id.* at 131, 130. Examples include revenue collection, foreign commerce, immigration, tariffs, tribal relations, public lands, public benefits, and patents. *Id.* at 128-30.⁷ That said, the exception must be handled “with care.” *Id.* at 131. “[E]ven with respect to matters that arguably fall within the scope of the ‘public rights’ doctrine, the presumption is in favor of Article III courts.” *Id.* at 132 (quoting *Northern Pipeline Constr. Co. v. Marathon Pipe Line Co.*, 458 U.S. 50, 69 n.23 (1982)).

2

The Commission argues its enforcement action falls within the public rights exception because it involves common carriers. See *Nat’l Cable & Telecommunications Ass’n v. Brand X Internet Servs.*, 545 U.S. 967, 975

⁷ See *Murray’s Lessee*, 18 How. at 281, 285 (action to compel federal customs collector to pay public funds into Treasury); *Oceanic Steam Nav. Co. v. Stranahan*, 214 U.S. 320, 335 (1909) (action to enforce fine on steamship company for disobeying federal prohibition on allowing immigration by aliens with contagious diseases); *Ex parte Bakelite Corp.*, 279 U.S. 438, 458 (1929) (assessment of President’s tariffs on goods imported by “unfair methods of competition”); *United States v. Jicarilla Apache Nation*, 564 U.S. 162, 174 (2011) (relations with Indian tribes); *Crowell v. Benson*, 285 U.S. 22, 51 & n.13 (1932) (administration of public lands); *ibid.* (public benefits such as veterans benefits and pensions); *United States v. Duell*, 172 U.S. 576, 582-83 (1899) (patent rights).

(2005) (“The [Communications] Act regulates telecommunications carriers . . . as common carriers.”). Given that common carriers like AT&T are “affected with a public interest,” *Munn v. Illinois*, 94 U.S. 113, 130 (1876), the Commission contends Congress could assign adjudication of civil penalties against them to agencies instead of courts. For several reasons, we disagree.

First, the Commission’s proposal would blow a hole in what is meant to be a narrow exception to Article III. Myriad enterprises might be said to implicate the “public interest.”⁸ And Congress’s power to regulate common carriers is broad. See *Glob. Crossing Telecommunications, Inc. v. Metrophones Telecommunications, Inc.*, 550 U.S. 45, 48 (2007) (“When Congress enacted the Communications Act of 1934, it granted the FCC broad authority to regulate interstate telephone communications.”). If injected into the public rights exception, this combination would empower Congress to bypass Article III adjudication in countless matters. But the Supreme Court has cautioned that the doctrine is a narrow and extra-textual “*exception*” to presumptively mandatory Article III jurisdiction. *Jarkesy*, 603 U.S. at 131.

Second, the common carrier doctrine is deeply rooted in the common law. See, e.g., *NetChoice*, 49 F.4th at

⁸ See *NetChoice, L.L.C. v. Paxton*, 49 F.4th 439, 445 (5th Cir. 2022) (social media activity), *overruled on other grounds by Moody v. NetChoice, L.L.C.*, 603 U.S. 707 (2024); *Fed. Power Comm’n v. Hope Nat. Gas Co.*, 320 U.S. 591, 611 (1944) (natural gas operations); *Nat’l Union Fire Ins. Co. v. Wanberg*, 260 U.S. 71, 74 (1922) (hail insurance); *New York v. FERC*, 535 U.S. 1, 19 (2002) (electric energy).

469 (“The common carrier doctrine is a body of common law dating back long before our Founding.”).⁹ Negligence claims against common carriers have been routinely adjudicated in state and federal courts. *See, e.g., Cole v. Goodwin & Storey*, 19 Wend. 251, 281 (N.Y. Sup. Ct. 1839) (a “coach proprietor’s” common carrier status made it strictly liable in tort).¹⁰ In light of that, it would be bizarre to situate a negligence action against carriers within the “historic categories of adjudications” falling *outside* Article III. *Jarkesy*, 603 U.S. at 130.¹¹

⁹ *See* 19 CHARLES ALAN WRIGHT, ARTHUR R. MILLER & EDWARD H. COOPER, *Federal Practice and Procedure* § 4514 (3d ed. 2024) (citing cases placing common carriers’ liability within the federal common law because such liability involves significant federal interests); *see also* Robert J. Kaczorowski, *The Common-Law Background of Nineteenth-Century Tort Law*, 51 Ohio State L.J. 1127, 1132 (1990) (explaining that “the common law imposed on persons engaged in a common calling a duty of reasonable care and a standard of professional competence”).

¹⁰ *See also New Jersey Steam Nav. Co. v. Merch.’s Bank of Bos.*, 47 U.S. 344 (1848) (steamboat operator liable for losses at sea); *S. Exp. Co. v. Purcell*, 37 Ga. 103 (1867) (railroad for loss of cotton bales); *Duggan v. New Jersey & W. Ferry Co.*, 76 A. 636 (Del. Super. Ct. 1909) (ferry operator for personal injuries); *Goldstein v. Northern Pac. Ry. Co.*, 164 N.D. 602 (1917) (railroad for conversion); *Korner v. Cosgrove*, 108 Ohio St. 484 (1923) (taxicab operator for employee’s assault of a passenger); *Callaway v. Hart*, 146 F.2d 103 (5th Cir. 1944) (railroad for negligently leaving doors open) *Andrews v. United Airlines, Inc.*, 24 F.3d 39 (9th Cir. 1994) (airline for luggage falling on passenger).

¹¹ Nor does it matter that this action is brought by the Government. The Supreme Court “ha[s] never held that ‘the presence of the United States as a proper party to the proceeding is . . . sufficient’ by itself to trigger the [public rights] exception.” *Jarkesy*, 603 U.S. at 135.

Third, the cases cited by the Commission fail to show that the public rights exception generally applies to common carriers. Some of the cases involved actions far afield from this one, such as public benefits or actions falling within federal admiralty jurisdiction.¹² Those actions arguably fall within the historical categories of non-Article III adjudications listed in *Jarkesy*. See 603 U.S. at 130. Whether they do or not, though, they do not involve anything like a negligence action against a common carrier for money damages.

It is true that federal agencies like the Commission have long had regulatory authority over common carriers, such as when setting rates or granting licenses. See, e.g., *Virginian Ry. Co. v. United States*, 272 U.S. 658 (1926) (discussing the Interstate Commerce Commission’s oversight of railroad carriers).¹³ But that does not imply, as the Commission seems to think, that any regulatory action concerning common carriers implicates the public rights exception and can therefore be “siphon[ed] . . . away from an Article III court.” *Jarkesy*, 603 U.S. at 135.

¹² See *Scripps-Howard Radio v. FCC*, 316 U.S. 4 (1942) (addressing FCC order granting application for a construction permit and station license); *Red Lion Broad. Co. v. FCC*, 395 U.S. 367 (1969) (addressing “fairness doctrine” governing content carriers could broadcast over radio frequency); *Crowell*, 285 U.S. 22 (addressing challenge to the Longshoremen’s and Harbor Workers’ Compensation Act of 1927).

¹³ See also *Burlington N., Inc. v. United States*, 459 U.S. 131, 141 (1982) (discussing Commission’s authority to set rates); *Regents of Univ. Sys. of Ga. v. Carroll*, 338 U.S. 586, 598 (1950) (discussing Commission’s authority to grant licenses); *Belluso v. Turner Commc’ns Corp.*, 633 F.2d 393, 397 (5th Cir. 1980) (discussing the Commission’s authority to sanction licensees).

Not even the first modern administrative agency thought that was so.¹⁴ The Interstate Commerce Commission, while empowered to regulate common carriers and recommend monetary penalties, believed its enforcement actions were subject to the Seventh Amendment and so, necessarily, to Article III adjudication. The agency’s 1887 report, issued the year it was created, stated that its power “must be so construed as to harmonize with the seventh amendment to the Federal Constitution, which preserves the right of trial by jury in common-law suits.” 1887 Interstate Com. Comm’n Ann. Rep. 27; *see also* Richard L. Jolly, *The Administrative State’s Jury Problem*, 98 Wash. L. Rev. 1187, 1242 (2023) (quoting Report’s conclusion that it was “unquestionable that parties can not [*sic*] be deprived of [the jury] right through conferring authority to award reparation upon a tribunal that sits without a jury as assistant”). The Commission takes no account of this history, which is flatly inconsistent with exempting its enforcement action from Article III adjudication.¹⁵

¹⁴ *See* LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 439 (2d ed. 1985). The ICC was the FCC’s predecessor.

¹⁵ Consistent with this history is *Meeker v. Lehigh Valley R.R. Co.*, 236 U.S. 412, 430 (1915), which involved an ICC action targeting a railroad’s unreasonable rates. The Supreme Court addressed whether a provision treating the ICC’s initial factfinding as a “rebuttable presumption” that could be reconsidered in a later jury trial comported with the Seventh Amendment. *Ibid.* Unlike the Commission’s action against AT&T here, the ICC action there (rate setting) had no common law analogue. Even so, the Court assumed the railroad had a jury right in the action and held the provision does not violate the Seventh Amendment because “[i]t cuts off no defense, interposes no obstacle to a full contestation of all the issues, and takes no question of fact from either court or jury.” *Ibid.*

Ultimately, “what matters” for Article III purposes “is the substance of the suit, not where it is brought, who brings it, or how it is labeled.” *Jarkesy*, 603 U.S. at 135. As explained, this matter involves an action closely analogous to a common law negligence action—and, importantly, one where the Commission seeks “civil penalties, a punitive remedy that [the Supreme Court] ha[s] recognized ‘could only be enforced in courts of law.’” *Id.* at 134 (quoting *Tull*, 481 U.S. at 422). Accordingly, the public rights exception does not apply and Article III adjudication is mandatory. *Id.* at 128.

C

Finally, the Commission argues that, even if the Seventh Amendment and Article III apply, the proceeding here meets their demands.

The Commission points to the possibility of a back-end section 504 trial. Recall that a carrier who fails to timely pay a forfeiture penalty may be sued by DOJ in federal district court. *See* 47 U.S.C. § 504(a). The Commission suggests this would give a carrier everything promised by the Seventh Amendment and Article III. We disagree.

To begin with, by the time DOJ sues (if it does), the Commission would have already adjudged a carrier guilty of violating section 222 and levied fines. This case shows how the process works. The Commission investigated AT&T, issued a charging document (the NAL), and received AT&T’s written objections. The Commission then affirmed the NAL by making fact findings, interpreting section 222, and applying that understanding to the facts it had found. This resulted in a forfeiture order con-

cluding AT&T had violated the law and imposing \$57 million in penalties. So, in this process, which was completely in-house, the Commission acted as prosecutor, jury, and judge.

Such forfeiture orders, furthermore, are not mere suggestions—to the contrary, they have real-world impacts on carriers. For example, the Commission must consider any history of prior adjudicated offenses in imposing future penalties. *See* 47 U.S.C. § 503(b)(2)(E) (“In determining the amount of such a forfeiture penalty, the Commission or its designee shall take into account . . . any history of prior offenses. . . .”). Unsurprisingly, they also cause reputational harm to carriers because they can be widely publicized and reported. *See FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 256 (2012) (explaining forfeiture orders’ impact on carriers’ reputations). And consider the risks to a carrier of even getting to the section 504 trial: the carrier must refuse to pay a penalty and wait for DOJ to drag it into court.

In light of this, we reject the Commission’s argument that a section 504 enforcement proceeding satisfies Article III and the Seventh Amendment. The Commission cites no authority supporting the proposition that the constitutional guarantee of a jury trial is honored by a trial occurring after an agency has already found the facts, interpreted the law, adjudged guilt, and levied punishment.

But put all that aside for a moment and consider another glaring problem. In a section 504 trial, a defendant cannot challenge a forfeiture order’s legal conclusions. As our court has explained, in a section 504(a) action, the district court is “limited to considering the

factual basis for the agency action” but not petitioner’s “legal arguments.” *Stevens*, 691 F.3d at 622.¹⁶ So, even assuming an after-the-fact jury trial could potentially satisfy the demands of the Constitution, the one provided here amputates the carrier’s ability to challenge the legality of the forfeiture order.

True, AT&T could challenge the Commission’s legal conclusions by doing what it did in this case—paying the forfeiture and seeking direct appellate review. *See* 47 U.S.C. § 402(a); *see also AT&T Corp.*, 323 F.3d at 1084. But that only underscores the dilemma in which AT&T finds itself. If AT&T wants an Article III court to review the forfeiture order’s legality, it has to give up a jury trial. If it wants a jury trial, it has to defy a multi-million dollar penalty, wait for DOJ to sue, and, even then, relinquish its ability to challenge the order’s legality.

Either way, AT&T’s Seventh Amendment rights have been denied.

¹⁶ The Commission tries to distinguish *Stevens* on the ground that it involved legal challenges to a rule outside of a statutorily imposed deadline, but *Stevens*’ reasoning was not limited to such challenges. *See id.* at 623 (“Persons aggrieved by a final FCC forfeiture order must raise legal challenges to the validity of the order in a timely petition for review in the appropriate court of appeals.”). And, contrary to the Commission’s argument, *PDR Network, LLC v. Carlton & Harris Chiropractic, Inc.*, 588 U.S. 1 (2019), does not support a narrow reading of *Stevens*. There, the Supreme Court expressly refused to decide whether the Hobbs Act’s exclusive-review provision affords a prior and adequate opportunity for judicial review of Commission orders interpreting statutory provisions. *Id.* at 8.

IV

No one denies the Commission's authority to enforce laws requiring telecommunications companies like AT&T to protect sensitive customer data. But the Commission must do so consistent with our Constitution's guarantees of an Article III decisionmaker and a jury trial.

Accordingly, we GRANT AT&T's petition and VACATE the Commission's forfeiture order.

APPENDIX C

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

File No.: EB-TCD-18-00027704
NAL/Acct. No.: 202032170004
FRN: 00057193701

IN THE MATTER OF AT&T, INC.

Adopted: Apr. 17, 2024
Released: Apr. 29, 2024

FORFEITURE ORDER

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

TABLE OF CONTENTS

Heading	Paragraph #
I. INTRODUCTION	[1]
II. BACKGROUND.....	[2]
A. Legal Background	[2]
B. Factual Background	[8]
III. DISCUSSION	[17]
A. Location Information is CPNI.....	[18]

B.	AT&T Had Fair Notice That Its LBS Practices Were Subject to Enforcement Under the Communications Act	[31]
C.	AT&T Failed to Take Reasonable Steps to Protect CPNI	[38]
1.	AT&T's Customer Location to Securus Were Unauthorized and Violated Section 222.....	[39]
2.	AT&T's Protection of Customer Location Information Was Unreasonable Both Before and After the Securus/Hutcheson Disclosures	[41]
3.	AT&T Bore the Burden of Production.....	[47]
D.	The Forfeiture Amount is Lawful and Consistent with FCC Precedent	[54]
1.	The Commission Reasonably Found that AT&T Engaged in 84 Continuing Violations That Warranted an Upward Adjustment.....	[56]
2.	AT&T Willfully and Repeatedly Violated the Act and the Commission's Rules	[63]
3.	The Commission Rightfully Treated LBS Providers Equally for Purposes of Calculating Violations	[66]
E.	Section 503(b) Is Employed Here Consistent With the Constitution.....	[68]
I.	CONCLUSION	[82]
II.	ORDERING CLAUSES.....	[83]

I. INTRODUCTION

1. On February 28, 2020, the Commission issued a Notice of Apparent Liability for Forfeiture and Admonishment (*NAL*) against AT&T, Inc. (AT&T or Com-

pany).¹ In the *NAL*, the Commission admonished AT&T 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 AT&T \$57,265,625 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, withdraw, or reduce the proposed penalty, and impose a penalty of \$57,265,625 against AT&T.

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 (Act).⁴ The Commission has advised carriers that this duty requires them to take "every reasonable precaution" to safeguard their customers' information.⁵ Section

¹ *AT&T, Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743 (2020) (*NAL*).

² *AT&T, Inc.*, Response to Notice of Apparent Liability for Forfeiture and Admonishment (filed May 7, 2020) (on file in EB-TCD-18-00027704) (*NAL Response* or *Response*).

³ *See generally NAL*.

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*).

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 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,

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 AT&T are “telecommunications services.” See 47 U.S.C. § 332(c)(1); H.R. Conf. Rep. No. 104-458 at 125 (1996) (“This definition [of ‘telecommunications service’] is intended to include commercial mobile service.”).

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 telecommu-

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 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

nications 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 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.

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 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

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).

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

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

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 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

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).

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

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 AT&T Location-Based Services Business Model.* AT&T pro-

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/plainlanguage/pdf0205-start-withsecurity.pdf>; Communications Security, Reliability and Interoperability Council, CSRIC Best Practices, <https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data>; CISA, Cross-Sector Cybersecurity Performance Goals and Objectives (last visited Aug. 17, 2022), <https://www.cisa.gov/cpgs>.

²⁵ 47 U.S.C. § 217.

vides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on AT&T's wireless network.²⁶ As part of its business, AT&T ran a Location-Based Services (LBS) program until March 2019. Through the LBS program, AT&T 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 service providers.²⁷ AT&T had arrangements with two location information aggregators: LocationSmart and Zumigo (the Aggregators).²⁸ Each Aggregator, in turn, had arrangements with location-based service providers. In total, AT&T sold access to its customers' location information (directly or indirectly) to 88 third-party entities (including the two Aggregators).²⁹

9. The AT&T LBS program was largely governed via contractual provisions that vested AT&T with oversight authority over the Aggregators. The Aggregators then entered into their own contracts with various LBS providers. This arrangement meant that it was

²⁶ See AT&T, Inc., 2021 Annual Report, <https://investors.att.com/~media/Files/A/ATT-IR-V2/financial-reports/annual-reports/2021/complete-2021-annual-report.pdf>.

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 1748-56, paras. 11-30.

²⁸ AT&T does not contend that its customers consented to these arrangements with the Aggregators.

²⁹ See *NAL*, 35 FCC Rcd at 1748-50, paras. 12-13 (citations omitted).

the LBS providers who were obligated “to provide notice and obtain consent” from consumers—not the Aggregators or AT&T. AT&T asserts that its LBS program was subject to a number of safeguards and that the LBS providers and Aggregators had to satisfy various requirements, which were memorialized in and governed by contract provisions with the Aggregators and any parties that AT&T directly sold location information to.³⁰ The contracts obligated the Aggregators to monitor the practices of the location-based service providers—including by making sure the LBS providers notified customers and collected affirmative customer consent for any use of location information.³¹ However, AT&T did not verify the customers’ consent before providing access to the location information; instead it claimed to verify on a daily basis that each request for information was tied to a consent record.³² In addition, each LBS provider was contractually required to access and use AT&T customer location information only for a specific purpose (known as a “Use Case”) that was reviewed and approved by AT&T in advance.³³ AT&T had broad authority under its contracts with the Aggregators to

³⁰ See *NAL*, 35 FCC Rcd at 1750-51, paras. 15-17 (citations omitted).

³¹ See *NAL*, 35 FCC Rcd at 1750, para. 16 (citing Response to Initial Letter of Inquiry from AT&T, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 6, Response to Question 1 (Nov. 14, 2018) (on file in EB-TCD-18-00027704) (LOI Response)).

³² See *NAL*, 35 FCC Rcd at 1750-51, para. 16 (citing Response to Supplemental Letter of Inquiry from AT&T, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 11, Response to Question 9 (May 24, 2019) (on file in EB-TCD-18-00027704) (Supplemental LOI Response)).

³³ See *NAL*, 35 FCC Rcd at 1750, para. 15.

quickly terminate access to customer location information if an Aggregator engaged in conduct that exposed AT&T to “sanctions, liability, prosecution or other adverse consequences under applicable law.”³⁴

10. AT&T also had the authority to conduct audits and other internal reviews of the LBS program. According to AT&T, between January 2016 and May 2019, it conducted five reviews or audits of its disclosure of customer location information to third parties.³⁵ The Company claims that three of the five analyses are subject to attorney-client privilege, however, and submitted the results only of the two reviews that AT&T treated as non-privileged.³⁶ The results of those two audits identified various issues of concern. One audit, which

³⁴ See *NAL*, 35 FCC Rcd at 1751, para. 17 (citing LOI Response at ATT-LOI-00013380, Response to Request for Documents No. 3, 2016 Master Agreement between AT&T Corp. and TechnoCom Corporation d/b/a LocationSmart, at Section 8.2 - Termination or Suspension (executed on Feb. 17, 2016 by Mario Proietti, CEO for LocationSmart and Glenn C. Girard, Assoc Dir. Customer Contracts-AT&T Services, Inc.); LOI Response at ATTLOI-00025859, Response to Request for Documents No. 3, 2014 Master Agreement between AT&T Corp. and Zumigo, Inc., Section 8.2 – Termination or Suspension (executed on Apr. 25, 2014 by Chira Bakshi, CEO for Zumigo and Ana Castaneda, Contract Specialist for AT&T)). The contracts required the Aggregators to indemnify AT&T for various types of claims, including those arising from privacy violations, but did not provide for any other remedy—such as direct restitution to affected customers—in the event of breach.

³⁵ See *NAL*, 35 FCC Rcd at 1751, para. 18 (citing LOI Response at 19-21, Response to Question 11; Supplemental LOI Response at 16, Response to Question 15).

³⁶ See *NAL*, 35 FCC Rcd at 1751, para. 18 (citing LOI Response at 20-21, Response to Question 11; Supplemental LOI Response at 16, Response to Question 15).

reviewed the Aggregators' compliance with AT&T information security requirements for third-party vendors, identified numerous instances of non-compliance with security requirements by both Aggregators.³⁷ The other audit, focused on a review of AT&T's controls over certain disclosures of customer location information for the provision of location-based services, identified issues related to the "completeness of subscriber consents" and "record retention practices regarding subscriber consents."³⁸ AT&T averred that the issues identified in both audits were remediated.³⁹ AT&T provided the general topics of the remaining three audits, but declined to produce any other information concerning those privileged reviews.

11. *Unauthorized Access and Use of Customer Location Information.* On May 10, 2018, the *New York Times* published an article that detailed security breaches involving AT&T's (and other carriers') practice of selling access to customer location information.⁴⁰ The 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

³⁷ See NAL, 35 FCC Rcd at 1751-52, para. 18 (citing LOI Response at 19-20, Response to Question 11).

³⁸ See NAL, 35 FCC Rcd at 1751, para. 18 (citing LOI Response at 20, Response to Question 11).

³⁹ See NAL, 35 FCC Rcd at 1751-52, para. 18 (citing LOI Response at 19-20, Response to Question 11; Supplemental LOI Response at 9, Response to Question 7).

⁴⁰ See Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018), <https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html>.

enforcement and corrections officials that allowed such officials to access customer mobile device location *without* that device owner’s knowledge or consent.⁴¹ 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 by AT&T), 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.⁴² AT&T conceded that it was unable to distinguish location requests unrelated to the authorized Use Case (which involved an inmate collect-calling service) because each request included a customer consent record that was identical to the records received for the approved service.⁴³

12. 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 identifi-

⁴¹ See *NAL*, 35 FCC Rcd at 1752-53, paras. 20-21 (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>).

⁴² See *NAL*, 35 FCC Rcd at 1752-53, paras. 20-21 (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>).

⁴³ See *NAL*, 35 FCC Rcd at 1753, para. 23.

cation of others, and Hutcheson pleaded guilty on November 20, 2018.⁴⁴ 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.⁴⁵ In order 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.’”⁴⁶ 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).⁴⁷ Rather than “uploading the required legal process,” Hutcheson instead “routinely uploaded false

⁴⁴ 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>.

⁴⁵ 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 1752-53, paras. 20-21.

⁴⁶ Hutcheson Sentencing Memo at 3; see also *NAL*, 35 FCC Rcd at 1752, para. 20.

⁴⁷ See Hutcheson Sentencing Memo at 3-4; see also *NAL*, 35 FCC Rcd at 1752, para. 20.

and fraudulent documents . . . , each time representing that the uploaded documents were valid legal process authorizing the location requests the defendant made.”⁴⁸ Those “false and fraudulent documents” included “his health insurance policy, his auto insurance policy, and pages selected from Sheriff training materials.”⁴⁹ Hutcheson “submitted thousands of Securus LBS requests and obtained the location data of hundreds of individual phone subscribers without valid legal authorization.”⁵⁰

13. *AT&T’s Response to the Securus Disclosures.* AT&T terminated Securus’s access to AT&T customer location information in May 2018, following the *New York Times* article.⁵¹ In June 2018, AT&T announced that it would phase out access to location information for the Aggregators and certain location-based service providers, except for those that the Company identified as offering public benefits, such as emergency services or fraud prevention.⁵² Although AT&T did not specify how long the process would take, according to AT&T it terminated the access of 36 location-based service providers to its customer location information by the end of 2018.⁵³ In November 2018, AT&T told Enforcement

⁴⁸ Hutcheson Sentencing Memo at 4; *see also* NAL, 35 FCC Rcd at 1753, para. 21.

⁴⁹ Hutcheson Sentencing Memo at 4; *see also* NAL, 35 FCC Rcd at 1753, para. 21.

⁵⁰ Hutcheson Sentencing Memo at 4; *see also* NAL, 35 FCC Rcd at 1753, para. 21.

⁵¹ *See* NAL, 35 FCC Rcd at 1753, para. 23.

⁵² *See* NAL, 35 FCC Rcd at 1754, para. 25 (citing Supplemental LOI Response at 1, Introduction); *see also* NAL Response at 29.

⁵³ *See* NAL, 35 FCC Rcd at 1754, para. 25; *see also* NAL Response at 29.

Bureau staff that it planned to implement “enhanced” notice and consent measures for location information-sharing in 2019 for the remaining location-based service providers, though in its NAL Response the Company states that those efforts were rendered moot by its January 10, 2019, decision to completely shut down the LBS program.⁵⁴ According to AT&T, it terminated the access to its customer location information of an additional 28 location-based service providers by the end of January 2019 and an additional 10 such providers by the end of February 2019.⁵⁵

14. AT&T’s decision to end its LBS program followed a January 8, 2019, Motherboard article alleging that access to customer location information was sold and resold, with little or no oversight, within the bail bonds industry, and that this led to consumers being tracked without their knowledge or consent.⁵⁶ That article focused in part on the activities of a company called MicroBilt, whose access to customer location information was suspended by AT&T on January 4, 2019.⁵⁷ On January 10, 2019, AT&T announced that “[i]n light of recent reports about misuse of location services, we decided to eliminate all location aggregator services—even those with clear consumer benefits” and stated that its loca-

⁵⁴ See NAL, 35 FCC Rcd at 1754, para. 25; NAL Response at 31-32.

⁵⁵ See NAL, 35 FCC Rcd at 1755-56, para. 29; NAL Response at 34.

⁵⁶ See NAL, 35 FCC Rcd at 1755, para. 27 (citing Joseph Cox, *I Gave a Bounty Hunter \$300. Then He Located Our Phone*, Motherboard (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-MicroBilt-zumigo-tmobile).

⁵⁷ See NAL, 35 FCC Rcd at 1755, para. 26.

tion-based service program would end in March 2019.⁵⁸ While AT&T states that it sent notices of termination to the two Aggregators in January 2019,⁵⁹ it was not until March 29, 2019, that its LBS program (and the sharing of AT&T's customers' location information) finally ceased.⁶⁰ In other words, the Company did not finally terminate its location-based service program until March 29, 2019,⁶¹ or 323 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.

15. *Notice of Apparent Liability.* On February 28, 2020, the Commission issued the *AT&T NAL* proposing a \$57,265,625 fine against AT&T 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 *AT&T NAL*, the Commission also admonished AT&T for apparently disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it.

⁵⁸ See Alfred Ng, *AT&T is Cutting Off All Location-Data Sharing Ties in March*, CNET (Jan. 11, 2019), <https://www.cnet.com/news/at-t-is-cutting-off-all-location-data-sharing-ties-by-march/>.

⁵⁹ See *NAL*, 35 FCC Rcd at 1755-56, para. 29 & n.111 (citing Supplemental LOI Response at 2, Response to Question 1).

⁶⁰ See *NAL*, 35 FCC Rcd at 1755-56, para. 29 (citing Supplemental LOI Response at 2, Response to Question 1; Further Response, LBS Chart Attachment); *NAL* Response at 34.

⁶¹ See *NAL*, 35 FCC Rcd at 1756, para. 29 (citing Supplemental LOI Response at 1-2, Introduction); *NAL* Response at 34.

16. On May 7, 2020, AT&T filed a response to the *NAL*.⁶² AT&T makes a number of arguments as to why the *NAL* should be withdrawn and cancelled. AT&T 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 not have fair notice that it would be classified as CPNI.⁶³ AT&T also argues that it acted reasonably 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.⁶⁴ Finally, AT&T argues that the forfeiture amount is arbitrary and capricious.⁶⁵

III. DISCUSSION

17. The Commission proposed a forfeiture in this case in accordance with section 503(b) of the Communications Act of 1934, as amended (Act),⁶⁶ section 1.80 of the Commission's rules,⁶⁷ and the Commission's *Forfeiture Policy Statement*.⁶⁸ When we assess forfeitures, section 503(b)(2)(E) requires that the Commission take

⁶² See *NAL Response*.

⁶³ *NAL Response* at 4-17.

⁶⁴ *NAL Response* at 17-35.

⁶⁵ *NAL Response* at 35-40.

⁶⁶ 47 U.S.C. § 503(b).

⁶⁷ 47 CFR § 1.80.

⁶⁸ *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).

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.”⁶⁹ We have fully considered AT&T’s NAL Response, which includes a variety of legal and factual arguments, but we find none of them persuasive. We therefore affirm the \$57,265,625 forfeiture proposed in the *NAL*.

A. Location Information is CPNI

18. As the *NAL* explained in more detail, the customer location information disclosed in AT&T’s LBS program is CPNI under the Act and our rules.⁷⁰ 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.”⁷¹ The customer location information used in AT&T’s LBS program falls squarely within this definition. AT&T’s arguments to the contrary⁷² 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.

⁶⁹ 47 U.S.C. § 503(b)(2)(E).

⁷⁰ See *NAL*, 35 FCC Rcd at 1757-59, paras. 33-41.

⁷¹ 47 U.S.C. § 222(h)(1)(A) (emphasis added).

⁷² See *NAL* Response at 5-11.

19. *First*, the customer location information at issue here relates to the location of a telecommunications service—i.e., AT&T’s commercial mobile service.⁷³ 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. AT&T is therefore providing telecommunications service to these customers whenever it is enabling the customer’s device to send and receive calls—regardless of whether the device is actively in use for a call.⁷⁴

20. 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. . . .”⁷⁵ 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

⁷³ 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”).

⁷⁴ See *NAL*, 35 FCC Rcd at 1757, para. 35.

⁷⁵ 47 U.S.C. § 222(h)(1)(A).

opposed to the preceding terms such as “location.”⁷⁶ 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” service⁷⁷—an event that, aspects of which, ordinarily occur before the service is in “use.”

21. The location information at issue here readily fits within that interpretation of the first prong of the CPNI definition. AT&T’s customers can access the 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 AT&T’s ability to use its network to determinate that location—is reasonably understood as associated with or a reference to the location of the AT&T telecommunications service.⁷⁸ Consequently, consistent with our assessment in the *NAL*,⁷⁹ we find this to be information that “relates to” the loca-

⁷⁶ 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’”).

⁷⁷ 47 U.S.C. § 222(d)(1).

⁷⁸ See, e.g., *NAL*, 35 FCC Rcd at 1748, para. 11 (“AT&T provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on AT&T’s wireless network.”).

⁷⁹ See, e.g., *NAL*, 35 FCC Rcd at 1757, 1758, paras. 35, 38.

tion of AT&T's telecommunications service within the meaning of the first prong of the CPNI definition.⁸⁰

22. 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. AT&T does not dispute the *NAL*'s explanation that customers' devices and AT&T's network regularly exchange information as necessary for customers to send and receive calls.⁸¹ To the extent that AT&T contends that this does not represent use of the telecommunications service because it merely enables the provision of that service, AT&T 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*,⁸² we believe that AT&T's customers subscribe to its commercial mobile service to enable them to receive and transmit calls. When customers' devices are exchanging communications with AT&T's network, and thereby ensuring that they can receive in-

⁸⁰ 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”).

⁸¹ *NAL*, 35 FCC Rcd at 1757, para. 35.

⁸² See, e.g., *NAL*, 35 FCC Rcd at 1757, 1758, paras. 35, 38.

coming 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.⁸³

23. Nor do AT&T's arguments about the source and intended purpose of the location data at issue here persuade us to reach a contrary result. AT&T contends that the location data at issue here were generated via a different mechanism than is used to ensure connectivity to the network for purposes of commercial mobile service and certain other services, and that AT&T obtained them with the intent of using them for purposes of its LBS initiative, rather than its provision of commercial mobile service.⁸⁴ But nothing in the text of the first prong of the CPNI definition turns on the classification of the service or technology used to obtain the infor-

⁸³ 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 serve for purpose; bring into service” and “exploit for one's own ends”).

⁸⁴ NAL Response at 7. To the extent that AT&T assumes that the functionality used to obtain the location information for its LBS initiative was not itself a telecommunications service, we need not, and thus do not, address that here because our conclusions do not turn on that point.

mation, nor 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 AT&T 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 AT&T obtained the information and how it planned to use the information.

24. We also are unpersuaded by AT&T'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 AT&T gleans from other language in section 222.⁸⁵ In addition to the NAL's responses in this regard,⁸⁶ 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:⁸⁷ 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

⁸⁵ See, e.g., NAL Response at 5-6.

⁸⁶ NAL, 35 FCC Rcd at 1758, para. 39.

⁸⁷ 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'").

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 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 222.⁸⁸

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

AT&T provides wireless telephony services to the affected customers because they have chosen AT&T to be their provider of telecommunications service—in other words, they have a carrier-customer relationship. . . . AT&T's customers provided their wire-

⁸⁸ 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*).

less location data to AT&T because of their customer-carrier relationship with AT&T,⁸⁹

In sum, the *NAL* reasoned that “[a]lthough AT&T might also provide non-common-carrier services to the same customer,” the customer provided the relevant data “by virtue of the carrier-customer relationship.”⁹⁰

26. The *NAL* did not specify with precision the standard for applying the second prong of the CPNI 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.”⁹¹ 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.”⁹² Thus, although AT&T suggests that its ac-

⁸⁹ See *NAL*, 35 FCC Rcd at 1757-58, para. 36.

⁹⁰ *NAL*, 35 FCC Rcd at 1758, para. 37.

⁹¹ 47 U.S.C. § 222(h)(1)(A).

⁹² 47 U.S.C. § 222(h)(1)(A). Insofar as AT&T refers at times to a question of whether it “received the relevant location information ‘solely by virtue of’ its voice telecommunications service,” see, e.g., *NAL* Response at 9, the focus on AT&T’s “voice telecommunications service” neither reflects the statutory text regarding prong two of the CPNI definition nor does it appropriately account for

quisition of the location information at issue here is in some technical sense distinct from, or does not depend exclusively on, the carrier-customer relationship,⁹³ we find that belied by the technical and marketplace realities here, as experienced by AT&T customers.

27. As the *NAL* explains, when a customer subscribes to AT&T's commercial mobile service, AT&T "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."⁹⁴ AT&T does not dispute that the carrier-customer relationship fully enables AT&T to obtain the location data at issue here. Although AT&T does contend that it "used distinct technological platforms to obtain location data for purposes of LBS lookups and voice services,"⁹⁵ it does not claim that a customer, having subscribed to its commercial mobile service, entered a separate agreement with AT&T for the provision of that location information—or that AT&T's voice customers

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, AT&T disputes whether the location information at issue meets the statutory definition of CPNI in section 222(h)(1)(A), *see* *NAL* Response at 5-11, but does not contend that, if it does meet that definition, section 222(c)(1) nonetheless should not be interpreted to apply here.

⁹³ *See, e.g.*, *NAL* Response at 8-11.

⁹⁴ *NAL*, 35 FCC Rcd at 1758, para. 40.

⁹⁵ *NAL* Response at 9.

had any way to avoid providing that information if they wanted to subscribe to AT&T's commercial mobile service. Under circumstances such as these, we conclude that the location information at issue from AT&T's commercial mobile service customers was "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."⁹⁶

28. 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. As discussed in the *NAL*, for example, AT&T has sought to rely on the theory that its offering of bundled telecommunications service and information services take location data outside the purview of "CPNI."⁹⁷ But we are not persuaded that AT&T's inclusion of multiple services in a bundle—which includes one or more telecommunications services—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 AT&T's customers to make their location information

⁹⁶ 47 U.S.C. § 222(h)(1)(A).

⁹⁷ See, e.g., *NAL*, 35 FCC Rcd at 1758, para. 37; see also, e.g., *NAL* Response at 9-11 (raising similar arguments). AT&T does not catalog all the various services included in its bundles, and given that at least some of the services identified by AT&T have been classified as information services under existing Commission precedent, we need not otherwise evaluate the possible classifications of all of AT&T possible service offerings for purposes of our analysis here.

available to AT&T,⁹⁸ and 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.”⁹⁹ AT&T points out 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.”¹⁰⁰ But we are far from that scenario here, given the many necessary links to AT&T’s telecommunications services for the CPNI definition to apply.¹⁰¹ 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

⁹⁸ 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 AT&T to obtain the location information at issue here. *Bostock v. Clayton Cty.*, 140 S. Ct. 1731, 1739 (2019) (In contrast to the statute 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.

⁹⁹ *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para 23.

¹⁰⁰ 47 U.S.C. § 153(51).

¹⁰¹ For similar reasons, we reject the suggestion that our approach regulates AT&T 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 8, 10.

any customer of” AT&T.¹⁰² And the information must have been provided by consumers in a manner that reflects the statutorily required nexus to AT&T’s telecommunications service.¹⁰³ 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 AT&T would prefer.¹⁰⁴

29. Finally, we reject AT&T’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.¹⁰⁵ 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 AT&T’s corporate practices as a whole with respect to the entities that received

¹⁰² 47 U.S.C. § 222(h)(1)(A).

¹⁰³ 47 U.S.C. § 222(h)(1)(A).

¹⁰⁴ AT&T also argues that jurisdiction over this matter lies with the Federal Trade Commission. *See* *NAL* Response at 12-13. But as we have found here, the data in question is CPNI and therefore properly within the Commission’s jurisdiction under section 222 of the Act. As explained in the *NAL*, the Commission has authority to bring action for violations of section 222 of the Communications Act and the CPNI Rules against providers of telecommunications services and providers of interconnected Voice over Internet Protocol services. *See NAL*, 35 FCC Red at 1747, para. 10 (citing 47 U.S.C. § 222; *2007 CPNI Order*, 22 FCC Red at 6954-57, paras 54-59).

¹⁰⁵ *See* *NAL* Response at 9-10.

LBS data.¹⁰⁶ AT&T does not contend that 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 AT&T 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.

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

B. AT&T Had Fair Notice That Its LBS Practices Were Subject to Enforcement Under the Communications Act

31. We reject AT&T’s claim that it lacked fair notice that its practices involving customer location information were subject to the Communications Act and poten-

¹⁰⁶ 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 AT&T 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 AT&T allegedly did not have a reasonable policy in place for particular entities that received LBS data. *See, e.g., NAL*, 35 FCC Rcd at 1768-69, para. 76. 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 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*.

tial penalties thereunder.¹⁰⁷ The language of section 222 demonstrates that customer location information is CPNI; AT&T’s practices involving CPNI, including customer location information, therefore unquestionably are regulated under the Act and the Commission’s CPNI Rules; and AT&T’s failure to comply with the requirements of the Act and our rules, including the “reasonable measures” mandate of section 64.2010, foreseeably makes the Company liable for a forfeiture penalty under section 503 of the Act.

32. AT&T argues that the “proper vehicle” for the Commission to address carriers’ LBS practices “would have been a rulemaking or other order with prospective-only application.”¹⁰⁸ But the Commission is not limited to this option. 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.¹⁰⁹

¹⁰⁷ See NAL Response at 14-17.

¹⁰⁸ NAL Response at 14.

¹⁰⁹ 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

33. Contrary to AT&T’s assertion, the Commission is not required by principles of fair notice to “announce” that LBS data, in particular, meets the definition of CPNI under section 222 of the Act or the CPNI Rules before enforcing that statute and those rules with respect to those data.¹¹⁰ 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.’”¹¹¹ 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.¹¹²

is one that lies primarily in the informed discretion of the administrative agency”).

¹¹⁰ See NAL Response at 14 (referring to “the proper vehicle for announcing that [section 222 encompasses LBS location data]” and the punishment of AT&T “for conduct that preceded the announcement”). In any event, however, absolute specificity is not a prerequisite for enforcing a statute or regulation. See, e.g., *Lachman*, 387 F.3d at 56-57 (stating the “mere fact that a statute or regulation requires interpretation does not render it unconstitutionally vague,” and that case law “do[es] not stand for the proposition that any ambiguity in a regulation bars punishment”).

¹¹¹ *Mississippi Comm’n on Env’tl. 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”).

¹¹² *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

34. 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.”¹¹³ Thus, AT&T cannot reasonably have assumed that the fact 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.”¹¹⁴ Moreover, even while declining to comprehensively identify CPNI, in-

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).

¹¹³ *2013 CPNI Declaratory Ruling*, 28 FCC Red at 9617, para. 24 n.54.

¹¹⁴ *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”).

cluding in the case of location information, the Commission emphasized that “location information in particular can be very sensitive customer information.”¹¹⁵ In addition, notwithstanding the fair notice claims it makes now, AT&T previously asserted to the Commission that it treated customer location information in an essentially equivalent manner to CPNI.¹¹⁶

35. 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 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.”¹¹⁷ 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.”¹¹⁸ 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.

36. Finally, AT&T had fair notice of its obligations with respect to CPNI under section 64.2010 of the Com-

¹¹⁵ *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

¹¹⁶ *See NAL*, 35 FCC Rcd at 1758, para. 37 n.122.

¹¹⁷ 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’”).

¹¹⁸ 47 U.S.C. § 222(h)(1)(A).

mission'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."¹¹⁹ 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."¹²⁰ The Commission granted carriers flexibility to incorporate the specific measures and practices that are consistent with their otherwise-existing "technological choices."¹²¹ 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.¹²² 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.¹²³ 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

¹¹⁹ 47 CFR § 64.2010(a).

¹²⁰ *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

¹²¹ *2007 CPNI Order*, 22 FCC Rcd 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").

¹²² *2007 CPNI Order*, 22 FCC Rcd at 6946, para. 35.

¹²³ *2007 CPNI Order*, 22 FCC Rcd at 6952-53, para. 49.

‘roadmap’ of how to obtain CPNI without authorization.”¹²⁴ This provides sufficient direction for AT&T to understand its obligations under the rule as relevant here.¹²⁵

37. Thus, AT&T 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) AT&T would be subject to forfeiture penalties for failing to protect that customer location information as required under section 222 and the Commission’s rules.¹²⁶

¹²⁴ 2007 CPNI Order, 22 FCC Rcd at 6959-60, para. 65.

¹²⁵ AT&T cites *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1235-36 (11th Cir. 2018), but we are not persuaded that case calls for more here. For one, that case deals specifically with requirements for cease-and-desist orders and injunctions. See, e.g., *LabMD*, 894 F.3d at 1234-35. Further, the requirements at issue in that case lacked the supplementing guidance providing greater clarity that we find present in the case of section 64.2010 of the Commission’s rules. See, e.g., *LabMD*, 894 F.3d at 1236 (explaining that the proposed court order “is devoid of any meaningful standard informing the court of what constitutes a ‘reasonably designed’ data-security program”). Separately, AT&T’s reliance on contractual safeguards and its failure to investigate key details that would ensure LBS providers only were engaging in authorized uses and disclosures of CPNI appears directly at odds with guidance the Commission has provided. Even where a regulation is amenable to different interpretations, courts have rejected ‘fair notice’ claims where the regulated entity did not comply with at least some viable interpretation of the requirement. See, e.g., *21st Century Telesis Joint Venture v. FCC*, 318 F.3d 192, 202 (D.C. Cir. 2003).

¹²⁶ We reject as inapposite AT&T’s argument that the Commission cannot rely on principles of deference to satisfy fair notice requirements. NAL Response at 16-17 (citing *Kisor v. Wilkie*, 139

C. AT&T Failed to Take Reasonable Steps to Protect CPNI

38. AT&T 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.¹²⁷ 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. 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). AT&T contends that the Securus disclosures to Hutcheson did not constitute legal violations of section 222.¹²⁸ AT&T then claims

S. Ct. 2400 (2019); *Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 158 (2012); *General Electric Co. v. EPA*, 53 F.3d 1324, 1334 (D.C. Cir. 1995); *Gates & Fox Co. v. Occupational Safety & Health Review Commission*, 790 F.2d 154, 156 (D.C. Cir. 1986)). As the analysis above indicates, we are not relying on deference as grounds for finding fair notice of an interpretation of the definition of CPNI for which fair notice would not otherwise exist.

¹²⁷ 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.”).

¹²⁸ *See* NAL Response at 18-21.

that it acted reasonably to protect its customers' location information both before and after the Securus disclosure came to light.¹²⁹ AT&T also argues that the Commission improperly shifted the burden of proving that such protections were reasonable to AT&T.¹³⁰ We find AT&T's arguments unpersuasive.

1. AT&T's Customer Location Disclosures to Securus Were Unauthorized and Violated Section 222

39. As an initial matter, we conclude that it was not just disclosures to Hutcheson that were unauthorized. Rather, Securus's entire location-finding service¹³¹ (as detailed in paragraphs 11-12, above) was predicated on unauthorized disclosures. Consistent with AT&T'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 AT&T).¹³² AT&T conceded that it was unable to distinguish location requests unrelated to the authorized Use Case (which involved an in-

¹²⁹ See NAL Response at 25-35.

¹³⁰ See NAL Response at 18-25.

¹³¹ See NAL, 35 FCC Red at 1752-53, paras. 20-21 (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>).

¹³² See LOI Response at 17, Response to Inquiry No. 8 ("AT&T never approved this [Securus] program and did not receive the government requests."); see also, e.g., NAL Response at 21 (contending that certain information relied upon in the NAL "at most," supported "the proposition that Securus sent Hutcheson location data for certain AT&T customers outside the scope of AT&T's approved use case").

mate collect-calling service) because each Securus request included a customer consent record that was identical to the records received for the approved service.¹³³ And, to be clear, none of the “consent 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 AT&T provided the requested location information, a separate, unauthorized disclosure occurred.

40. AT&T attempts to avoid this conclusion by: (1) concentrating only on the disclosures made to Hutcheson, not on the overall Securus location-finding program;¹³⁴ and (2) trying to use section 222(c)(1)’s exception for disclosures that are required by law to shield itself.¹³⁵ This misses the larger point. Whether or not there was a legitimate law enforcement request for the information is irrelevant if AT&T did not satisfy its own obligations under section 222. AT&T provided the location information to Securus under Securus’s false pretenses, and AT&T only did so because it took Securus at its word that Securus had obtained opt-in consumer consent.¹³⁶ This means that AT&T did not review any law

¹³³ See *NAL*, 35 FCC Rcd at 1753, para. 23.

¹³⁴ See *NAL* Response at 24 (saying there is “no pattern of data breaches” and that it is “only isolated and dated incidents involving a single errant LBS provider (Securus) with a single bad customer (Hutcheson)”).

¹³⁵ See *NAL* Response at 20 (relying on 47 CFR § 222(c)(1), which allows disclosure of CPNI “as required by law”).

¹³⁶ AT&T’s attempt to distinguish whether “location lookups violated Securus’s contractual obligations to AT&T” from the question of whether there was a violation of section 222 thus is futile

enforcement requests and likewise did not provide the information pursuant to a law enforcement request because AT&T did not know there *were* any law enforcement requests in the first place—legitimate or otherwise.¹³⁷ 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.¹³⁸ Thus, the disclo-

under the circumstances here. *See, e.g.*, NAL Response at 20. 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 1760, para. 37 n.141. Although the NAL noted that “AT&T 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 AT&T’s arguments here.

¹³⁷ *See* LOI Response at 17, Response to Inquiry No. 8 (“AT&T never approved this [Securus] program and did not receive the government requests.”); NAL Response at 20 (stating that “Securus enabled law enforcement officials—without AT&T’s knowledge—to access customer location data” in a manner that “violated Securus’s contractual obligations to AT&T”). *See also* NAL, 35 FCC Rcd at 1752-53, paras. 20-21 (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 AT&T as having been relying on a third party to disclose information as required by law where AT&T neither knew or approved of the third party doing so.

¹³⁸ *See* Hutcheson Sentencing Memo at 3-4 (explaining that after uploading documents that were blatantly not legal authorizations,

asures made 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 AT&T’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.¹³⁹ Despite AT&T’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 disclo-

location information was immediately transmitted with no intervening time for any documents to be reviewed for validity); *NAL*, 35 FCC Rcd at 1753, para. 21 (describing Hutcheson’s uploading of documents that were blatantly not legal authorizations in order to obtain location information). As the *NAL* explained, “AT&T does not deny the existence of the Securus location-finding service nor the abuse of that system by Hutcheson.” *NAL*, 35 FCC Rcd at 1753, para. 22. AT&T 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 AT&T customers, *see* *NAL* Response at 20-21, but does provide any reason to believe that Securus (let alone AT&T) could have or would have made that assessment before providing the location data.

¹³⁹ *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 1753, para. 21.

asures, including those made to Hutcheson, were unauthorized and AT&T was appropriately admonished in relation to such disclosures.

2. AT&T's Protection of Customer Location Information Was Unreasonable Both Before and After the Securus/Hutcheson Disclosures

41. The Commission affirms the *NAL* and finds that AT&T 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 AT&T did not have reasonable protections in place prior to 2018 *New York Times* article detailing the Securus/Hutcheson breaches,¹⁴⁰ but also that AT&T failed to promptly address its demonstrably inadequate CPNI safeguards after Securus/Hutcheson disclosure.¹⁴¹

42. AT&T attempts to excuse its unreasonable practices by cataloging the steps it did take before and after the *New York Times* article. AT&T argues that, prior to the Securus disclosure, its efforts exceeded the CTIA Guidelines for ensuring customer consent to the use of location data.¹⁴² Specifically, AT&T states that its safeguards included: (1) vetting each LBS provider and aggregator; (2) predicated access to location data on individualized preapproval of each LBS provider and each LBS Use Case; (3) limiting a number of LBS providers' access to specific location data even for consenting customers; (4) imposing exceptionally detailed information-security requirements on all LBS providers and aggre-

¹⁴⁰ See *NAL*, 35 FCC Rcd at 1761-63, paras. 51-59.

¹⁴¹ See *NAL*, 35 FCC Rcd at 1763-77, paras. 60-70.

¹⁴² See *NAL* Response at 26.

gators; (5) reviewing customer-consent records daily; and (6) conducting audits and assessments to monitor and strengthen its controls.¹⁴³

43. The safeguards that AT&T had in place before the Securus disclosure were not reasonable. As fully explained in the *NAL*:

[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. 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.¹⁴⁴

As for the other safeguards that AT&T implemented to protect its customers' location information against unauthorized access, these safeguards relied almost entirely upon contractual agreement, passed on to location-based service providers through an attenuated chain of downstream contracts.¹⁴⁵ To enforce these safeguards, AT&T would have needed to take steps to determine whether they were actually being followed. Further, AT&T would have had to have a way of distinguishing between a legitimate request for customer location information (i.e., made pursuant to valid consumer consent) and an illegitimate one (i.e., the Securus/ Hutcheson requests absent valid customer consent). Although

¹⁴³ See *NAL* Response at 26.

¹⁴⁴ *NAL*, 35 FCC Rcd at 1762, para. 55.

¹⁴⁵ See *NAL*, 35 FCC Rcd at 1762-1763, paras. 53-59.

the Commission requested that AT&T describe its efforts to verify that LBS providers obtained valid customer consent for related location requests,¹⁴⁶ nothing that AT&T has provided shows that it made any meaningful efforts or that it could effectively distinguish between valid and unauthorized requests for location information. And any further claim by AT&T that its contractual safeguards were effective are undermined by the inexorable fact that after the Securus disclosure, AT&T was unable to “compel Securus to cooperate with [its] investigation.”¹⁴⁷ As the Commission said in the *NAL*, if AT&T could not compel Securus to cooperate, “it cannot say that the same contract-based system actually protects customer location information from unauthorized access by other entities. [Securus’s] . . . refusal [to cooperate] is further evidence of the fact that AT&T disclosed CPNI to a third party over which it had little or no control or authority.”¹⁴⁸

44. Likewise, AT&T’s safeguards after the Securus disclosure were also unreasonable. AT&T became keenly aware of the inadequacy of its safeguards after the May 2018 *New York Times* article, and again after Securus’s resistance to AT&T’s subsequent investigation. Nonetheless, AT&T did not and cannot demonstrate that its safeguards were made reasonable in the months that followed the 2018 *New York Times* article.

¹⁴⁶ See Letter from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau to Jeanine Poltronieri, Assistant Vice President, External Affairs, AT&T Services, Inc., Letter of Inquiry at 3, Question 5(e), (Sep. 13, 2018) (on file in EB-TCD-18-00027704).

¹⁴⁷ *NAL*, 35 FCC Rcd at 1764, para. 63.

¹⁴⁸ *NAL*, 35 FCC Rcd at 1764, para. 63.

In fact, rather than promptly implementing reasonable safeguards, AT&T 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.¹⁴⁹ Although AT&T worked towards implementing an enhanced notice and consent mechanism, this mechanism was never deployed.¹⁵⁰ According to AT&T, the mechanism was never deployed because AT&T decided to shut down its LBS program altogether—in the wake of a report of yet another LBS provider's systems being misused.¹⁵¹ But the mere fact that AT&T was working on new processes is not sufficient to satisfy its obligation to “take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.”¹⁵² Until the new measures actually are in place, 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 in-

¹⁴⁹ See *NAL*, 35 FCC Rcd at 1764, para. 60.

¹⁵⁰ See NAL Response at 30-32. In connection to implementing its enhanced notice and consent mechanism and ending its LBS program, AT&T argues that the *NAL* “pluck[ed] [a 30-day] deadline from thin air [and] it is arbitrary and capricious.” *Id.* at 32. 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, AT&T's existing data security practices were unreasonable both before and after the May 2018 article—the article merely exposed those unreasonable 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 AT&T with a grace period to either end the program or reform its practices.

¹⁵¹ See NAL Response at 33-34.

¹⁵² 47 CFR § 64.2010(a).

volved in AT&T's work on new processes render the procedures that remained in place in the meantime "reasonable" under that rule, given their glaring weaknesses. The Commission has considered all of the data security measures that AT&T implemented in response to the Securus disclosure¹⁵³ and concludes that these measures were inadequate.

45. AT&T argues that the Commission "faults AT&T's response [to the Securus disclosure] only because [the Commission] arbitrarily (1) ignores the consumer benefits of LBS services and the social costs of shutting them down and (2) all but ignores the substantial data security measures AT&T took in response to the Securus disclosure."¹⁵⁴ We disagree. The issue here is not whether there are any beneficial services offered by LBS providers, but whether AT&T reasonably protected its customers' location information. And even under AT&T's reasoning, the Company would have no excuse for its failure to promptly terminate every other non-critical LBS provider. 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 AT&T did not have a reliable way of confirming customer consent. The Commission considered AT&T's arguments, but finds they are outweighed by these risks.

46. 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 con-

¹⁵³ See *NAL* Response at 25-35.

¹⁵⁴ See *NAL* Response at 26.

sumer consent) and shutting down the LBS program.¹⁵⁵ Rather than taking definitive steps to remedy the obvious LBS program issues, AT&T instead took piecemeal steps. The Commission has fully considered all of the safeguards AT&T implemented after the Securus disclosure and has determined these safeguards to be inadequate because they 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.¹⁵⁶

3. AT&T Bore the Burden of Production

47. 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 AT&T did not use reasonable safeguards throughout the period of the violation.¹⁵⁷ As such, while the *NAL* discussed AT&T's burden of production to demonstrate that its protection of customer CPNI was reasonable,¹⁵⁸ that burden-shifting is not necessary given the preponderance of the evidence. Nonetheless, even if unnecessary to prove AT&T's violations in this matter, the *NAL* properly shifted the burden of production to AT&T.

¹⁵⁵ See *NAL*, 35 FCC Rcd at 1765-66, paras. 67-69.

¹⁵⁶ Although AT&T asserts that it worked towards implementing enhanced notice and consent mechanisms, those enhanced mechanisms were never deployed given AT&T's decision to shut down its LBS program altogether. See *NAL* Response at 30-32.

¹⁵⁷ See *NAL*, 35 FCC Rcd at 1761-66, paras. 51-69.

¹⁵⁸ See *NAL*, 35 FCC Rcd at 1746-47, 1761-62, and 1764, paras. 8, 52-53, and 62.

48. *First*, as the *NAL* explained¹⁵⁹ 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.¹⁶⁰ In the *NAL*, the Commission found that AT&T failed to demonstrate that its safeguards were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018.¹⁶¹

49. AT&T acknowledges that the *2007 CPNI Order*¹⁶² states 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."¹⁶³ However, AT&T is incorrect when it asserts that the *2007 CPNI Order* cannot support the burden-shifting approach in cases outside of the pretexting context. The *2007 CPNI Order*

¹⁵⁹ See *NAL*, 35 FCC Rcd at 1746-47, para. 8.

¹⁶⁰ 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").

¹⁶¹ See *NAL*, 35 FCC Rcd at 1761-66, paras. 51-69.

¹⁶² See *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*).

¹⁶³ See *NAL Response* at 22 (citing *NAL*, 35 FCC Rcd 1746-47, 61-62, at paras. 8, 52).

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 AT&T 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 in order to obtain access to CPNI.¹⁶⁴ Broadly, in relation to Securus’s entire unauthorized location-finding service, Securus used the pretext that it was requesting location information from AT&T 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.¹⁶⁵ 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.

50. *Second*, AT&T admits that an evidentiary presumption is valid if the circumstances (here, a breach of CPNI) giving rise to that presumption make it “more

¹⁶⁴ The breach at issue here arguably falls within the letter of criminal pretexting. See 18 U.S.C. § 1039.

¹⁶⁵ 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 1753, para. 21; see also *supra* para. 12.

likely than not” that the presumed fact (here, that CPNI safeguards were unreasonable) exists.¹⁶⁶ The Commission finds that the unauthorized disclosure in this case gave rise to a rebuttable presumption that AT&T did not reasonably protect customer location information from unlawful access.¹⁶⁷ 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 AT&T’s resultant disclosures of consumer location information were unauthorized. AT&T’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, AT&T argues that the Commission cannot use the Securus and Hutcheson breaches (particularly as they occurred in 2014-2017) to support shifting the burden of production to the AT&T to provide evidence of the reasonableness of their post-May 2018 security practices.¹⁶⁸ Specifically, AT&T asserts that (1) there is no basis for concluding that LocationSmart or

¹⁶⁶ See NAL Response at 23.

¹⁶⁷ 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).

¹⁶⁸ See NAL Response at 18-22.

Securus actually committed a legal violation for which AT&T could be vicariously liable and (2) even if such violation was found, it could form no basis for presuming that AT&T responded unreasonably after the violation was found long after it occurred. We disagree.

51. In the *NAL*, we found that AT&T apparently violated section 222(c) of the Act and section 64.2007(b) of our rules in connection with its unauthorized disclosures of CPNI to Hutcheson.¹⁶⁹ This is further bolstered by the Department of Justice’s case against Hutcheson.¹⁷⁰ And though the Commission opted to admonish AT&T only for the unauthorized disclosures made to Hutcheson, it would have been appropriate to admonish AT&T 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,¹⁷¹ carriers cannot disclaim their obligations to protect customer CPNI by delegating those obligations to third parties.¹⁷² In its *NAL* Response, AT&T does not

¹⁶⁹ See *NAL*, 35 FCC Rcd at 1759-61, paras. 42-50. “The evidence reflects that Hutcheson used the Securus service to obtain the location information of AT&T customers. AT&T shared the information with LocationSmart, which then shared it with 3Cinteractive, which then shared it with Securus. *Id.* at 1759 at para. 43. “The evidence shows that between 2014 and 2017, at least 147 AT&T customers’ location information was disclosed to Hutcheson, via Securus, without the customers’ consent.” *Id.* at 1759 at para. 43.

¹⁷⁰ See, e.g., Hutcheson Sentencing Memo.

¹⁷¹ 47 U.S.C. § 217.

¹⁷² See *NAL*, 35 FCC Rcd at 1747, 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.

dispute that Hutcheson’s “location lookups violated Securus contractual obligations to AT&T.”¹⁷³ We reiterate here that “AT&T is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred.”¹⁷⁴ Further, section 222(c)(1) of the Act¹⁷⁵ makes the responsibility for avoiding unauthorized disclosures a carrier obligation and prohibits use and disclosure except in certain narrow circumstances, without any reasonableness criterion. AT&T 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 the disclosures involving Hut-

¹⁷³ See NAL Response at 20. AT&T argues that Hutcheson’s unauthorized location lookups, which they concede violated Securus’s legal obligations to AT&T including safeguarding its customers’ CPNI, did not violate the Act or the Commission’s rules because “section 222(c)(1) expressly authorizes information-sharing “required by law.”” *Id.* We find AT&T’s argument unavailing. Although AT&T 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 AT&T 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 1752, para. 20.

¹⁷⁴ See NAL, 35 FCC Rcd at 1759, para. 45; see also *id.* at 1760, para. 47 n.141 (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)).

¹⁷⁵ 47 U.S.C. § 222(c)(1).

cheson and the imposition of a burden to produce evidence of reasonable protections during the later violations period was reasonable—particularly because, as discussed, those safeguards did not materially change in the interim timeframe.¹⁷⁶

52. *Third*, AT&T misinterprets the *NAL* when it argues that the Commission improperly shifted the burden of persuasion to the Company.¹⁷⁷ To the contrary, the Commission properly (and consistent with APA precedent) shifted only the burden of *production*, and not the burden of *persuasion*, to AT&T. The unauthorized disclosure at issue gave rise to a rebuttable presumption that AT&T did not adequately protect customer information from unlawful access. The burden

¹⁷⁶ We thus reject AT&T's claim that burden-shifting based on the Securus disclosures makes no sense when the issue is the reasonableness of AT&T's procedures years after those disclosures. *See* NAL Response at 24-25. As we explain above, the procedures AT&T actually employed—rather than the unimplemented processes it worked on developing—are what matters for assessing compliance with section 64.2010 of the rules. Since the procedures AT&T actually employed did not materially change from the time of the Securus disclosure through the time periods at issue here, the reasonableness of the procedures employed at the time of the Hutcheson disclosure remain fully relevant—and thus shifting the burden of production based on unauthorized disclosures under those procedures is logically consistent. In addition, the disclosures made to Hutcheson are not the only unauthorized disclosures. Disclosures made pursuant to Securus's unauthorized program are all unauthorized, and both pre- and post-dated any disclosures made to Hutcheson.

¹⁷⁷ *See* NAL Response at 22-25.

of production then shifted to AT&T to offer evidence that it had reasonable safeguards in place.¹⁷⁸

53. Rather than taking reasonable steps to safeguard its customers' location information after the Securus/Hutcheson disclosures were reported,¹⁷⁹ AT&T placed its customers' location information at continuing risk of unauthorized access through its failure to terminate its program or impose reasonable safeguards to protect its customers' location information. For these reasons, we conclude that AT&T failed in its obligation under section 222 and our rules to have reasonable measures in place to discover and protect against attempts to gain unauthorized access to its customers' CPNI.

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

54. After considering the evidence in the record, the relevant statutory factors, the Commission's *Forfeiture Policy Statement*, and the arguments advanced by AT&T in the NAL Response, we find that AT&T is liable for a total forfeiture of \$57,265,625 for its violations of section 222 of the Act and section 64.2010 of the Commission's rules.¹⁸⁰ As explained in the *NAL*, this total

¹⁷⁸ We note that in some instances—most notably with regard to various audits that implicated the LBS program and over which AT&T asserted privilege—AT&T claimed to have taken certain reasonable steps, but did not produce documentary evidence of those steps. *See NAL*, 35 FCC Rcd at 1751-52, paras. 18-19.

¹⁷⁹ Many of the possible reasonable steps were enumerated in the *NAL*. *See NAL*, 35 FCC Rcd at 1764-66, paras. 61-69.

¹⁸⁰ 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

results 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).¹⁸¹ The Commission found in the *NAL* that AT&T apparently engaged in 84 continuing violations—one for each ongoing relationship with a third-party LBS provider or aggregator that had access to AT&T customer location information more than 30 days after publication of the *New York Times* report—and that each violation continued until AT&T terminated the corresponding entity’s access to customer location information.¹⁸² Using this methodology, the Commission found AT&T apparently liable for a total base forfeiture of \$45,812,500. Upon considering the nature of the violations and the risk of harm they posed to consumers, the Commission then applied a 25% upward adjustment to the base forfeiture amount, resulting in a total proposed forfeiture of \$57,265,625.¹⁸³

55. AT&T challenges these forfeiture calculations with three principal arguments. *First*, AT&T asserts that the *NAL* describes at most a single continuing violation, not 84 separate violations, and that the upward adjustment was based on the same factors used to determine the base forfeiture for these violations. As such, according to AT&T, the forfeiture exceeds the applicable statutory maximum and violates due process, and both the forfeiture and the upward adjustment are arbi-

U.S.C. § 657, “Oversight of Regulatory Enforcement,” in addition to other rights set forth herein.

¹⁸¹ *NAL*, 35 FCC Rcd at 1778, para. 75.

¹⁸² *NAL*, 35 FCC Rcd at 1778-79, para. 76.

¹⁸³ *NAL*, 35 FCC Rcd at 1780, para. 79.

trary and capricious.¹⁸⁴ *Second*, AT&T argues that because it did not engage in “willful or repeated” violations, it cannot be subject to a forfeiture penalty under section 503(b).¹⁸⁵ *Third*, AT&T claims that the Commission bore (and failed to meet) the burden of showing that each of the 84 third-party relationships upon which the forfeiture was based posed a significant threat of unauthorized access to AT&T customer location information.¹⁸⁶ For the reasons discussed below, we are not persuaded by any of these arguments and decline to cancel or reduce the forfeiture proposed in the *NAL*.

**1. The Commission Reasonably Found that
AT&T Engaged in 84 Continuing Violations
That Warranted an Upward Adjustment**

56. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against AT&T of up to \$204,892 for each day of a continuing violation, up to a statutory maximum of \$2,048,915 “for any single act or failure to act.”¹⁸⁷ According to AT&T, the *NAL* describes at most one continuing violation for which a penalty may be assessed—namely, the “fail[ure] . . . to

¹⁸⁴ *NAL* Response at 35-38, 37 n.29.

¹⁸⁵ *NAL* Response at 38.

¹⁸⁶ *NAL* Response at 39-40.

¹⁸⁷ *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).

have reasonable [data security] measures in place.”¹⁸⁸ AT&T asserts that because the *NAL* describes that failure in unitary terms, and because the *NAL* does not suggest that AT&T “should have tailored distinct safeguards to specific LBS providers,” the Commission can only find there to have been one continuing violation (subject to the \$2,048,915 penalty cap).¹⁸⁹ AT&T also claims that the *NAL* justifies the base forfeiture and the upward adjustment on the same factors and that doing so is arbitrary and capricious.¹⁹⁰ Thus, AT&T contends, the *NAL*’s finding of 84 separate continuing violations (one for each LBS provider or aggregator) constitutes an impermissible attempt to circumvent the statutory maximum set by Congress.

57. We reject these arguments. Neither section 503(b) nor the forfeiture guidelines in section 1.80 of the Commission’s rules speak to the application of the phrase “single act or failure to act,” or otherwise to the calculation of the number of violations, in the CPNI or data security context.¹⁹¹ 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 vio-

¹⁸⁸ *NAL Response* at 36 (citing *Notice*, 35 FCC Red at 1766-67, para. 70).

¹⁸⁹ *NAL Response* at 36-37.

¹⁹⁰ *NAL Response* at 37 n.29.

¹⁹¹ 47 U.S.C. § 503(b); 47 CFR § 1.80(b).

lation for which a forfeiture may be assessed.”¹⁹² The Commission further observed that “[e]ach unprotected document constitutes a continuing violation that occurred on each of the 81 days [until] the date that the Companies remedied the failure. . . .”¹⁹³

58. 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),¹⁹⁴ 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 AT&T and an LBS 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.¹⁹⁵ Each such relationship relied upon a distinct and unique contractual chain (from AT&T 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

¹⁹² *TerraCom*, 29 FCC Rcd at 13343, para. 50.

¹⁹³ *TerraCom*, 29 FCC Rcd at 13343, para. 50.

¹⁹⁴ *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 (EB 2015), para. 20.

¹⁹⁵ Because our approach adheres to the requirements of section 503 of the Act, we reject AT&T’s nondelegation and excessive fines clause arguments that were premised on the theory that the Commission was seeking to evade those requirements. See NAL Response at 37.

reviewed and authorized by AT&T. 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.

59. The approach taken in the *NAL* was not only reasonable, it was—contrary to AT&T’s claim that it led to a “stratospheric” penalty that was “astronomically higher” than the statutory maximum—eminently *conservative*, both in terms of the base forfeiture and the upward adjustment. 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.”¹⁹⁶ 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.¹⁹⁷ These factors include, importantly, “egregious misconduct,” “substantial harm,” “repeated or continuous violation,” and “ability to pay/relative disincentive,” among others.¹⁹⁸ The Commission weighed these factors when making the determination that the base forfeiture in this case merited a substantial upward

¹⁹⁶ 47 U.S.C. § 503(b).

¹⁹⁷ 47 CFR § 1.80(b)(10), Table 3.

¹⁹⁸ *Id.*

adjustment. AT&T's conduct was egregious; 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.¹⁹⁹ Its failure to adequately protect CPNI for a protracted amount of time caused substantial harm by making it possible for "malicious actors to identify the exact locations of AT&T subscribers who belong to law enforcement, military, government, or other highly sensitive positions—thereby threatening

¹⁹⁹ 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 EBTCD-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 EBTCD-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-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/pressreleases/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 AT&T, Verizon, T-Mobile, and Sprint).

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.²⁰⁰ 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 AT&T’s status as a major telecommunications provider to determine what penalty, when applied, would adequately provide AT&T 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. AT&T’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.”²⁰¹ Nor do AT&T’s arguments persuade us that the 25% upward adjustment, which is relatively modest compared to upward adjustments in other cases involving consumer harms,²⁰² was unwarranted.

²⁰⁰ *NAL*, 35 FCC Rcd at 1780, para. 79.

²⁰¹ 47 U.S.C. § 503(b).

²⁰² *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/spoofers 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%

60. Turning to the per-LBS provider violations, as described in the *NAL*, AT&T'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 AT&T 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).²⁰³ Using that methodology—and taking into account the tens of millions of consumers whose highly sensitive location information was made vulnerable by AT&T—would have resulted in a significantly higher forfeiture than what was proposed in the *NAL*.

61. 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 AT&T 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

of base forfeiture amount imposed on robocaller who engaged in illegal spoofing for robocall telemarketing activities).

²⁰³ Although it involved a data breach—and not, as in this case, an ongoing failure to maintain reasonable safeguards such that customer data were placed at unreasonable risk of unauthorized disclosure—*TerraCom* supports applying a customer-centric forfeiture calculation that takes into account the number of customers whose data were inadequately protected. See *TerraCom*, 29 FCC Red at 13343, para. 50.

took a conservative approach, giving AT&T 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 AT&T 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.

62. We also reject AT&T's assertion that its due process rights were violated because it lacked fair notice 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 AT&T's fair notice claims,²⁰⁴ 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. AT&T 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.²⁰⁵ Independently, we observe that the penalties at issue here are governed by section 503

²⁰⁴ See *supra* B.

²⁰⁵ See, e.g., *TerraCom*, 29 FCC Rcd at 13343, paras. 51-52.

of the Act, with which we fully comply in our decision.²⁰⁶ 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.²⁰⁷

2. AT&T Willfully and Repeatedly Violated the Act and the Commission's Rules

63. AT&T asserts that it cannot be subject to a forfeiture penalty under section 503(b)(1)(B) of the Act because that provision applies only to “willful[] or repeated[]” violations.²⁰⁸ According to AT&T, because the *NAL* “describes at most a unitary continuing violation,” it does not allege any “repeated” failure to comply with statutory or regulatory requirements. And, AT&T claims, the violation cannot be “willful” because the *NAL* does not allege that AT&T acted in knowing violation of any requirement.

64. These arguments lack merit. The terms “willful” and “repeated,” as used in section 503(b) of the Act, do not have the restrictive meaning that AT&T would assign to them. As the Commission previously stated in *Midwest Radio-Television*:

. . . 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

²⁰⁶ 47 U.S.C. § 503.

²⁰⁷ *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).

²⁰⁸ 47 U.S.C. § 503(b)(1)(B).

he was doing the acts in question—in short, that the acts were not accidental (such as brushing against a power knob or switch).²⁰⁹

AT&T contends that “willful” should not be interpreted by reference to the definition in section 312(f) as the Commission has done previously, but instead should be interpreted to require “at least a knowing violation or reckless disregard of law, citing the Supreme Court’s decision in *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47 (2007).²¹⁰ We find instead that the Commission’s historical approach to interpreting “willfully” in section 503(b) is on firmer footing than AT&T suggests. The Commission’s interpretation reflected in *Midwest Radio-Television*, which predated the enactment of section 312(f), was premised on interpretations from Commission precedent interpreting “willful” elsewhere in the Act and Commission rules, and a consideration of court cases from other fields, along with the legislative history of the then-recently enacted “willful[] or repeated[]” language of section 503(b).²¹¹ Although *Safeco* states that “where willfulness is a statutory condition of civil liability, we have generally taken it to cover not only knowing violations of a standard, but reckless ones as well,” it also recognizes that “‘willfully’ is a ‘word of many meanings whose construction is often

²⁰⁹ *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)

²¹⁰ See NAL Response at 38 n.32.

²¹¹ *Midwest Radio-Television*, 40 F.C.C. at 1665-67, paras. 8-11.

dependent on the context in which it appears.’”²¹² Particularly given that *Midwest Radio-Television* was decided close in time to the enactment of the relevant language in section 503(b), and included an analysis of precedent interpreting willfulness as it had been used elsewhere in the Act previously,²¹³ that more highly relevant context persuades us to continue to follow the *Midwest Radio-Television Inc.* approach to interpreting “willfully” in section 503(b).²¹⁴ Separately and independently, however one might use the legislative history of section 312(f) to interpret section 312(f) itself, the relevant Conference Report indicates that the definitions enacted in section 312(f) were “consistent with the Commission’s application of those terms [“willfully” and “repeatedly”] in *Midwest Radio-Television Inc.*, 45 F.C.C. 1137 (1963).”²¹⁵ That can be seen as Congressional endorsement of the interpretations in *Midwest Radio-Television*, or at least more instructive than such legislative history otherwise commonly might be viewed.

²¹² *Safeco*, 551 U.S. at 57.

²¹³ *Midwest Radio-Television*, 40 F.C.C. at 166, para. 9.

²¹⁴ As the Commission has noted, a federal district court decision declined to enforce the *Midwest Radio-Television* decision. See *Application For Review Of Southern California Broadcasting Company Licensee, Radio Station Kiev(Am) Glendale, California*, Memorandum Opinion and Order, 6 FCC Red 4387, 4387-88, para. 5 (1991) (referencing *U.S. v. Midwest Radio-Television, Inc.*, 249 F. Supp. 936, 937 (D. Minn. 1966)). However, that district court decision does not reflect any statutory analysis, nor does it otherwise grapple with the Commission and court precedent interpreting willfulness under other provisions of the Act and Commission rules, let alone any of the other considerations relied on in *Midwest Radio-Television*.

²¹⁵ H.R. Conf. Rep. 97-765, at 51, 1982 U.S.C.C.A.N. 2261, 2295 (Aug. 19, 1982).

65. Likewise, 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.²¹⁶ In the present case, both are true—AT&T not only failed to meet its obligations to have reasonable protections of customer CPNI repeatedly with each LBS provider and Aggregator, but also failed to meet such obligations for more than one day. Thus, by continuing to operate its LBS program in the absence of reasonable safeguards, AT&T willfully and repeatedly violated section 222 of the Act and section 64.2010 of the Commission’s rules.

3. The Commission Rightfully Treated LBS Providers Equally for Purposes of Calculating Violations

66. AT&T also challenges the Commission’s finding that each and every LBS provider and aggregator relationship that AT&T left in place more than 30 days after the *New York Times* report involved a failure to reasonably protect CPNI. AT&T contends that, because some of these 84 entities were “well known and highly reputable” companies, they did not “pose a realistic data-security threat” and the Commission should not have treated them uniformly for purposes of determin-

²¹⁶ See, e.g., *Playa Del Sol Broadcasters*, Order on Review, 28 FCC Rcd 2666, 2668, para. 4 (2013); *Hale Broadcasting Corporation*, 79 FCC2d 169, 171, para. 5 (1980); *Midwest Radio-Television*, 40 F.C.C. at 168, paras. 15-16. Although AT&T contends that the Commission cannot find a repeated violation here, it does not offer any particular interpretation of the term “repeated.” See NAL Response at 38.

ing the number of violations and calculating the proposed penalty.²¹⁷

67. We disagree. The exact level of threat posed by each LBS entity is both unquantifiable and beside the point. The Commission determined that the system of safeguards, under which these entities each operated pursuant to individual contracts and differing approved Use Cases, did not meet the reasonableness requirement of section 64.2010. Of particular significance is the fact that, at all times relevant to the violations period, AT&T still had not implemented a consent mechanism that would enable it to verify that a customer's purported consent to the disclosure of location information was legitimate. As noted in the *NAL*, "[a]fter the Securus and Hutcheson breaches came to light, AT&T had good reason to doubt the accuracy of the consent records it received from *any* location-based service provider."²¹⁸ The reputation of any particular third party is no substitute for implementing reasonable safeguards to protect customer location information that AT&T made available to that entity (and potentially its individual employees and contractors). Indeed, even "well known and highly reputable" companies such as AT&T are not immune to security threats posed by insiders.²¹⁹ Accordingly, we reject AT&T's argument that the Commission erred in finding 84 separate continuing viola-

²¹⁷ *NAL* Response at 39-40.

²¹⁸ *NAL*, 35 FCC Rcd 1758, para. 39 (emphasis added).

²¹⁹ See *AT&T Services, Inc.*, Order and Consent Decree, 30 FCC Rcd 2808 (EB 2015) (resolving an investigation into unauthorized access to CPNI perpetrated by employees at three different AT&T call centers).

tions for the 84 entities that AT&T continued to provide with access to customer location information.

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

68. We reject AT&T’s supplemental constitutional objections that: (1) the FCC combines prosecutorial and adjudicative roles in violation of constitutional due process requirements;²²⁰ (2) the issuance of a forfeiture order by the Commission would violate Article III and the Seventh Amendment;²²¹ 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.²²² AT&T’s arguments are premised on misunderstandings regarding the relevant statutory framework, the nature of the Commission’s actions, and relevant precedent.

²²⁰ Letter from C. Frederick Beckner III, counsel to AT&T, to Michael Epshteyn and Rosemary Cabral,, Enforcement Bureau, FCC, EB-TCD-18-00027704, at 2 (filed June 22, 2023) (AT&T June 22, 2023 Supplemental NAL Response).

²²¹ AT&T June 22, 2023 Supplemental NAL Response at 2-3.

²²² AT&T June 22, 2023 Supplemental NAL Response at 3. AT&T also claims in passing that “[t]he Bureau’s compulsory investigative process, in which targets are compelled to respond to often excessively broad requests for information—upon threat of additional enforcement action and without an appropriate opportunity to object or appeal—also raises serious due process concerns.” *Id.* at 2 n.6. AT&T does not explain how, exactly, the investigatory process used by the Enforcement Bureau either here or more generally violates due process, however, nor how such concerns bear on the ultimate validity of the Commission’s action in this forfeiture order. We thus reject that undeveloped claim as a reason not to proceed with a forfeiture order here.

69. As a threshold matter, AT&T 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, AT&T is entitled to a trial *de novo* in federal district court before it can be required to pay the forfeiture.²²³ AT&T's objection to the combination of 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 forfeiture.²²⁴ Likewise, AT&T'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 AT&T's statutory right to a trial *de novo* before it can be required to pay the forfeiture.²²⁵ The

²²³ 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 AT&T theoretically might elect to pay the forfeiture voluntarily does not diminish its statutory right to a trial *de novo* in federal district court.

²²⁴ *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.’”).

²²⁵ *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 find-

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.

70. Independently, there are sufficient grounds to reject AT&T's arguments for other reasons, as well. We discuss each of these in turn below.

71. *Combination of Functions.* With respect to AT&T's claimed due process violation,²²⁶ AT&T fails to demonstrate sufficient grounds for concluding that a combination of functions in the Commission's enforcement process here renders it constitutionally suspect, even apart from AT&T'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."²²⁷ To overcome that presumption re-

ings 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).

²²⁶ AT&T June 22, 2023 Supplemental NAL Response at 2.

²²⁷ *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

quires “a showing of conflict of interest or some other specific reason for disqualification.”²²⁸

72. AT&T fails to demonstrate a concern specific to the Commission’s forfeiture order here sufficient to overcome the presumption of honesty and integrity. Insofar as AT&T 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.²²⁹

73. AT&T also expresses concerns that the Commission “(1) affords the respondents no hearing before an ostensibly neutral ALJ in any NAL-based proceeding; (2) does not wall itself off from enforcement staff when adjudicating such a proceeding; and (3) can impose massive financial penalties at the conclusion of its adminis-

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).

²²⁸ *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’”).

²²⁹ *See* AT&T 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), as well as other pending challenges in the Fifth Circuit and the U.S. District Court for the District of Columbia).

trative case.”²³⁰ 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, the first of AT&T’s concerns 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 by individuals despite earlier involvement in a matter.²³¹

²³⁰ AT&T June 22, 2023 Supplemental NAL Response at 2.

²³¹ 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.

We are unpersuaded to rely on precedent cited by AT&T that does not grapple with the presumption of honesty and integrity on the part of agency adjudicators. In particular, in *Proper v. Dist. of Columbia*, a vehicle owner challenged a D.C. enforcement regime for “junk” cars, and given the subjectivity of the standard being applied, the court observed that because “[t]he officer to whom appeal may be made is the same officer who decides that the vehicle is

74. As to AT&T's second concern, both the Communications Act²³² and the Administrative Procedure Act²³³ require formal separation of personnel in specific circumstances not present here, and the Supreme Court has cautioned against requiring agencies to follow procedures beyond those specified by statute.²³⁴ Particularly against the backdrop presumption of honesty and integrity on the part of agency adjudicators, AT&T identifies nothing specific to this case that would persuade us to depart from Congress' assessment of when formal separation of personnel is required.

75. Nor does the third concern cited by AT&T persuade us 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.²³⁵

'junk' in the first place; . . . serious questions as to impartiality arise"—but without considering any presumption of honesty and integrity. 948 F.2d 1327, 1333-34 (D.C. Cir. 1991).

²³² 47 U.S.C. § 409.

²³³ 5 U.S.C. § 554.

²³⁴ See, e.g., *Vermont Yankee Nuclear Power Corp. v. Nat. Res. Def. Council*, 435 U.S. 519, 524 (1978).

²³⁵ 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

We also are not 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.²³⁶ 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 AT&T provide evidence that is the case here.²³⁷ 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

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

²³⁶ *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).

²³⁷ *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).

a criminal prosecutor then serving as a judge.²³⁸ 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,”²³⁹ and AT&T 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.

76. To the extent that AT&T purports to identify concerns about the neutrality of two specific commissioners, we reject those arguments, as well. In particular, AT&T contends that statements accompanying the NAL by then-Commissioner Rosenworcel and Commissioner Starks “criticized the NAL for not being punitive enough.”²⁴⁰ However, what is relevant for purposes of evaluating bias in an adjudicatory proceeding is whether “a disinterested observer may conclude that [the agency] has in some measure adjudged the facts as well as

²³⁸ 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”).

²³⁹ 47 U.S.C. § 503(b)(4).

²⁴⁰ AT&T June 22, 2023 Supplemental NAL Response at 2 (citing NAL, 35 FCC Rcd at 1778 (Statement of Commissioner Jessica Rosenworcel Dissenting) (*Rosenworcel Statement*) and NAL, 35 FCC Rcd at 1779 (Statement of Commissioner Geoffrey Starks Approving In Part and Dissenting In Part) (*Starks Statement*)).

the law of a particular case in advance of hearing it.”²⁴¹ Properly understood, the portions of the separate statements quoted by AT&T address a legal or policy issue—the methodology used to calculate the proposed forfeiture—along with the related issue of the Commission’s failure to gather facts that would have enabled it to calculate a forfeiture using a different methodology.²⁴² That does not reflect any prejudgment of the facts to be resolved in the adjudication resulting from the *NAL*—to the contrary, the commissioners’ statements demonstrate that they viewed the ultimate issues as unresolved at that time.²⁴³ We thus reject AT&T’s claims of a due process violation through our implementation of the section 503(b) *NAL*-based process here.

77. *Trial By Jury*. We also reject AT&T’s contention that adjudication of the violations at issue here may not

²⁴¹ *Cinderella Career & Finishing Schs., Inc. v. FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970).

²⁴² See, e.g., *Rosenworcel Statement*, 35 FCC Rcd at 1778 (criticizing the proposed forfeiture as relying on “bureaucratic math to discount the violations of our privacy laws” leading to proposed forfeitures “that are too small relative to the law and the population put at risk”); *Starks Statement*, 35 FCC Rcd at 1779 (stating that “I strongly believe we should have determined the number of customers impacted by the abuses and based our forfeiture calculations on that data”).

²⁴³ See, e.g., *Rosenworcel Statement*, 35 FCC Rcd at 1778 (“[W]hen the FCC releases a Notice of Apparent Liability, it is just early days. The fines are not final until after the carriers that are the subject of this action get a chance to respond. That means there is still work to do. . . . ”); *id.* (observing that the *NAL* merely “proposes” certain fines); *Starks Statement*, 35 FCC Rcd at 1781-83 (repeatedly describing the forfeiture amounts as merely “proposed” in the *NAL*).

constitutionally be assigned to a federal agency.²⁴⁴ The Seventh Amendment preserves “the right of trial by jury” in “Suits at common law, where the value in controversy shall exceed twenty dollars,”²⁴⁵ but the Seventh Amendment applies only to suits litigated in Article III courts, not to administrative adjudications conducted by federal agencies.²⁴⁶ In determining whether an adjudication involves an exercise of judicial power vested in the federal courts under Article III of the constitution, the Supreme Court has distinguished between “public rights” and “private rights.”²⁴⁷ Congress has broad authority to “assign adjudication of public rights to entities other than Article III courts.”²⁴⁸ 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,²⁴⁹ “adjudicating violations of the customs and immigration laws and assessing penalties based thereon,”²⁵⁰ adjudicating “whether an unfair labor practice had been committed and of ordering back-pay where appropriate,”²⁵¹ and the grant or reconsider-

²⁴⁴ AT&T June 22, 2023 Supplemental NAL Response at 2-3.

²⁴⁵ U.S. Const. amend. VII.

²⁴⁶ 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).

²⁴⁷ *Oil States*, 138 S. Ct. at 1373 (citation omitted).

²⁴⁸ *Id.*

²⁴⁹ *Atlas Roofing*, 430 U.S. at 450, 461

²⁵⁰ *Id.* at 451.

²⁵¹ *Id.* at 453.

ation of a grant of a patent.²⁵² That precedent confirms the constitutional validity of FCC adjudication of violations of the Communications Act, even setting aside the reality that AT&T 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”²⁵³ designed to protect consumer privacy even as the communications marketplace became more open to competition,²⁵⁴ 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.²⁵⁵

78. Relying on the Fifth Circuit’s decision in *Jarkesy*, AT&T 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

²⁵² *Oil States*, 138 S. Ct. at 1373.

²⁵³ *Atlas Roofing*, 430 U.S. at 450.

²⁵⁴ 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.”).

²⁵⁵ *Atlas Roofing*, 430 U.S. at 450.

trial by jury—because the violations allegedly are analogous to common law negligence.²⁵⁶ Even on its own terms, however, *Jarkesy* did not deal with a claim that was analogized to common-law negligence.²⁵⁷ By contrast, the Supreme Court itself has held that an agency could conduct adjudications to enforce federal workplace-safety rules, even though workplace-safety disputes historically had been resolved through “common-law actions for negligence and wrongful death.”²⁵⁸ Given that Supreme Court precedent, we are not persuaded by AT&T’s attempt to implicate Article III and the Seventh Amendment based on asserted analogies to common-law negligence, even taking the Fifth Circuit’s decision in *Jarkesy* on its own terms.

79. Separately, AT&T also quotes the statement in *Jarkesy* that “actions seeking civil penalties are akin to special types of actions in debt from early in our nation’s history which were distinctly legal claims.”²⁵⁹ In support of that statement, the Fifth Circuit cited the Su-

²⁵⁶ AT&T June 22, 2023 Supplemental NAL Response at 2-3 (citing *Jarkesy v. SEC*, 34 F.4th 446 (5th Cir. 2022)). AT&T also cites Justice Thomas’ concurrence in *Axon. Id.* (citing *Axon*, 143 S. Ct. at 907 (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 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.

²⁵⁷ *Jarkesy*, 34 F.4th at 455.

²⁵⁸ *Atlas Roofing*, 430 U.S. at 445.

²⁵⁹ AT&T June 22, 2023 Supplemental NAL Response at 3 (quoting *Jarkesy*, 34 F.4th at 454-55).

preme Court's decision in *Tull v. United States*.²⁶⁰ In *Tull*, the 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.²⁶¹ 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."²⁶² 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

²⁶⁰ *Jarkesy*, 34 F.4th at 454-55 (citing *Tull v. United States*, 481 U.S. 412, 418-19 (1987)).

²⁶¹ *Tull*, 481 U.S. at 414-15.

²⁶² *Atlas Roofing*, 430 U.S. at 455.

jury trials are unavailable.²⁶³ We thus are unpersuaded by AT&T's reliance on *Jarkesy*.²⁶⁴

80. *Nondelegation*. Finally, contrary to AT&T's contention,²⁶⁵ 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 forfei-

²⁶³ *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.

²⁶⁴ As AT&T notes, the government has petitioned for certiorari in the *Jarkesy* case. AT&T June 22, 2023 Supplemental NAL Response at 3 n.8; *see also* Petition for a Writ of Certiorari, SEC v. Jarkesy, No. 22-859 (filed Mar. 8, 2023).

²⁶⁵ AT&T June 22, 2023 Supplemental NAL Response at 3.

tures: either the NAL-based path most commonly 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.²⁶⁶ Contrary to AT&T’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.²⁶⁷

81. We also are unpersuaded by AT&T’s reliance on the Fifth Circuit decision in *Jarkesy* to support its non-delegation concerns. In addition to questions about the

²⁶⁶ 47 U.S.C. § 503(b)(3), (4).

²⁶⁷ 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”).

merits of the Fifth Circuit’s approach in that regard,²⁶⁸ 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.²⁶⁹ 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.”²⁷⁰ 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.²⁷¹ The circumstances here therefore are distinct from those in *Jarkesy* where “Congress offered *no guidance whatsoever*.”²⁷²

²⁶⁸ 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 264.

²⁶⁹ *Jarkesy*, 34 F.4th at 462.

²⁷⁰ 47 U.S.C. § 154(j).

²⁷¹ *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).

²⁷² *Jarkesy*, 34 F.4th at 462.

IV. CONCLUSION

82. Based on the record before us and in light of the applicable statutory factors, we conclude that AT&T willfully and repeatedly violated section 222 of the Act²⁷³ as well as section 64.2010 of the Commission's rules²⁷⁴ 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 or to cancel or reduce the \$57,265,625 forfeiture proposed in the *NAL*.

V. ORDERING CLAUSES

83. 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, AT&T, Inc., **IS LIABLE FOR A MONETARY FORFEITURE** in the amount of fifty-seven million, two-hundred and sixty-five thousand, six hundred and twenty-five dollars (\$57,265,625) for willfully and repeatedly violating section 222 of the Act and section 64.2010 of the Commission's rules.

84. 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.²⁷⁵ AT&T, Inc., 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

²⁷³ 47 U.S.C. § 222.

²⁷⁴ 47 CFR § 64.2010.

²⁷⁵ *Id.*

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.²⁷⁶

85. In order for AT&T, Inc. to pay the proposed forfeiture, AT&T, Inc. 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/core/userLogin.do>. Payment of the forfeiture must be made by credit card using CORES at <https://apps.fcc.gov/core/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:²⁷⁷

- 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 159²⁷⁸ or printed CORES form²⁷⁹ must be faxed to the

²⁷⁶ 47 U.S.C. § 504(a).

²⁷⁷ For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #1).

²⁷⁸ FCC Form 159 is accessible at <https://www.fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159>.

²⁷⁹ Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form

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).²⁸⁰ 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 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

159. CORES is accessible at <https://apps.fcc.gov/cores/userLogin.do>.

²⁸⁰ Instructions for completing the form may be obtained at <http://www.fcc.gov/Forms/Form159/159.pdf>

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.

86. 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.

87. **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 R. McAtee II, Senior Executive Vice President and General Counsel, AT&T, Inc., c/o Jonathan E. Nuechterlein, Esq., and C. Frederick Beckner III, Esq., Sidley Austin LLP, 1501 K Street, N.W., Washington, DC, 20005.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

**STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL**

Re: *In the Matter of AT&T Inc.*, Forfeiture Order,
File No.: EB-TCD-18-00027704 (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 AT&T Inc.*, Forfeiture Order,
File No.: EB-TCD-18-00027704 (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 Communications 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 new-found 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

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).

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.

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 “telecommunications 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 cus-

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.

tomers might have had voice plans, thereby creating a “carrier-customer relationship.” But any Title II 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 practices under

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”).

142a

generally applicable rules of the road. I respectfully dissent.

**DISSENTING STATEMENT OF
COMMISSIONER NATHAN SIMINGTON**

Re: *In the Matter of AT&T Inc.*, Forfeiture Order,
File No.: EB-TCD-18-00027704 (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 D

1. 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 oper-

ator 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,¹ the amount of any forfeiture penalty determined under this subsection shall not exceed

¹ So in original. Following provision probably should be set flush with subpar. (C).

\$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 in-

volved is a nonlicensee 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.

2. 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.