No. 24-1733

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

VERIZON COMMUNICATIONS INC.,

Petitioner,

v.

UNITED STATES FEDERAL COMMUNICATIONS COMMISSION and UNITED STATES OF AMERICA,

Respondents.

On Petition for Review of an Order of the Federal Communications Commission

BRIEF FOR RESPONDENTS

P. Michele Ellison
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

Scott M. Noveck
Counsel

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

Doha G. Mekki
Acting Assistant Attorney General

Robert B. Nicholson
Matthew A. Waring
Attorneys

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

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Cases: **Page(s)**

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES (continued)

Page(s)

Administrative Materials:

Constitution, Statutes, And Regulations:

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Other Authorities:

No. 24-1733

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

VERIZON COMMUNICATIONS INC.,

Petitioner,

v.

UNITED STATES FEDERAL COMMUNICATIONS COMMISSION and UNITED STATES OF AMERICA,

Respondents.

On Petition for Review of an Order of
the Federal Communications Commission

BRIEF FOR RESPONDENTS

INTRODUCTION

Section 222 of the Communications Act of 1934, as amended, requires telecommunications carriers—such as Verizon, which provides wireless telephone service to millions of customers—to safeguard their customers' confidential information. 47 U.S.C. § 222(a) & (c)(1). That duty encompasses "information that relates to the * * * location * * * of a telecommunications service." *Id.* § 222(h)(1)(A). Because wireless phones must continuously communicate with a carrier's cellular towers

to ensure that users can receive and make calls, Verizon knows every customer's approximate location at all times.

But Verizon failed to safeguard that highly sensitive customer information. Until March 2019, Verizon operated a "location-based services" (LBS) program that sold access to customer location data to commercial "aggregators" which in turn supplied this information to "LBS providers" that provided various location-related services. In all, Verizon sold customer location data to 65 entities (two aggregators and 63 LBS providers). Although the Communications Act provides that the "failure of any officer, agent, or other person acting for or employed by any common carrier * * * shall in every case be also deemed to be the act, omission, or failure of such common carrier," 47 U.S.C. § 217, Verizon did not directly oversee or ensure that its commercial partners complied with its obligation to protect this sensitive information. Instead, Verizon relied on contractual provisions directing the aggregators to provide notice to users and to obtain consent before using location information, with the aggregators in turn contractually assigning that responsibility to each LBS provider, and Verizon contracted with a third-party auditor to ostensibly monitor compliance.

This attenuated chain of contractual arrangements proved ineffective. In May 2018, the *New York Times* reported that a Missouri sheriff was able to access customer location information for hundreds of people through LBS provider Securus Technologies—which, through a chain of other entities, purchased that information from Verizon and other carriers—without legal authorization and without the customers' knowledge or consent. The *Times* reported that the sheriff used this information to unlawfully track a local judge, multiple highway patrol officers, and his predecessor as sheriff, among others.

Despite learning in May 2018 that its protections were ineffective (and despite an earlier 2017 internal report identifying weaknesses in its protections), Verizon did not promptly act to identify and fix the vulnerabilities, nor did it suspend its location data-sharing program until the vulnerabilities were identified and resolved. It announced its intention to eventually shut down the program, yet initially it terminated access only for Securus and one other related provider. It did not even suspend the aggregator that had the contractual obligation to monitor Securus. Instead, Verizon continued to sell its customers' location data for 204 days to 58 entities, and for 324 days to another 5 entities, while

continuing to rely principally on contractual arrangements that had proven ineffective at protecting this sensitive information.

In the *Order* under review, the Commission assessed a monetary forfeiture on Verizon for its failure to safeguard customer information as required by Section 222. Forfeiture Order, *In re Verizon Commc'ns*, 39 FCC Rcd. 4259 (2024) (*Order*), *reprinted at* JA45–90. Specifically, the Commission found that Verizon committed 63 continuing violations of the Act—one for each of the 63 entities to which Verizon continued providing access to customer location data after the *New York Times* article exposed that its purported safeguards were ineffective and that it was not meaningfully in control of information it provided to these entities. That conclusion was both lawful and reasonable, and Verizon's objections to the forfeiture and to the Commission's forfeiture process have no merit. The petition for review should be denied.

JURISDICTIONAL STATEMENT

The forfeiture order challenged here was adopted pursuant to the procedures set forth in 47 U.S.C. § 503(b)(4) and was released on April 29, 2024. A forfeiture imposed under Section 503(b)(4) "shall be recoverable pursuant to section 504(a)," 47 U.S.C. § 503(b)(4), which in turn provides for the government to enforce a forfeiture penalty by

bringing "a civil suit in the name of the United States" in federal district court, *id.* § 504(a). Section 504(a) "creates an exception to th[e] general rule" that Commission orders are subject to direct review in the courts of appeals under 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1). *AT&T Corp. v. FCC*, 323 F.3d 1081, 1084 (D.C. Cir. 2003); *see Pleasant Broad. Co. v. FCC*, 564 F.2d 496 (D.C. Cir. 1977); *Dougan v. FCC*, 21 F.3d 1488 (9th Cir. 1994).

The D.C. Circuit has held, however, that if the subject of a forfeiture elects to pretermit the enforcement action contemplated under Section 504(a) by paying the forfeiture penalty (as Verizon has done here), it may then seek review directly in the court of appeals under Section 402(a). *See AT&T Corp.*, 323 F.3d at 1083–85. This Court has not specifically addressed whether it may entertain a petition for review in this circumstance, but it has undertaken review in at least one case in which such payment was made, *ABC, Inc. v. FCC*, 404 F. App'x 530 (2d Cir. 2011) (unpublished summary order).

Verizon paid the forfeiture penalty on May 22, 2024, and filed its petition for review on June 25, 2024, within 60 days of the release of the *Order*. *See* 28 U.S.C. § 2344; 47 C.F.R. § 1.4(b)(2).

STATEMENT OF THE ISSUES

1. Whether the Commission correctly interpreted the Communications Act's protections for "customer proprietary network information" to include wireless customers' location information.

2. Whether the Commission's finding that Verizon failed to adequately protect its customers' location information and the resulting forfeiture penalty were reasonable and supported by the record.

3. Whether the Commission's forfeiture procedures, which provide the opportunity to pursue a de novo jury trial in federal district court before the government can recover the forfeiture, comport with the Seventh Amendment.

STATEMENT OF THE CASE

A. Statutory And Regulatory Background

1. Section 222 of the Communications Act imposes on every telecommunications carrier "a duty to protect the * * * proprietary information of" its "customers." 47 U.S.C. § 222(a). One form of customer data protected by the Act is "customer proprietary network information," or CPNI, which includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a

telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." *Id.* § 222(h)(1)(A). Section 222(c)(1) provides that a carrier "shall only use, disclose, or permit access to individually identifiable [CPNI]" to provide "the telecommunications service from which such information is derived" or "services necessary to[] or used in" that service, "[e]xcept as required by law or with the approval of the customer." *Id.* § 222(c)(1). When a carrier relies on "any officer, agent, or other person acting for [it]" to comply with its duties under the Act, that person's "act, omission, or failure * * * shall in every case also be deemed the act, omission, or failure of such carrier." *Id.* § 217.

2. The FCC has issued regulations implementing Section 222's requirements, codified at 47 C.F.R. Part 64, Subpart U (§§ 64.2001 *et seq.*). Since 2002, the Commission's rules have required telecommunications carriers to obtain "opt-in approval" before sharing a customer's CPNI with third parties, or with any of a carrier's affiliates not involved in communications services. 47 C.F.R. § 64.2007(b); *see Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info.*, 17 FCC Rcd. 14860, 14883–84 ¶¶ 50–52 (2002) (*2002 CPNI Order*). Opt-in approval "requires that the carrier obtain from the customer

affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request." 47 C.F.R. § 64.2003(k); *see id.* § 64.2008(b)–(c) & (e).

In 2007, the Commission extended the opt-in approval requirement to the use of CPNI by a carrier's joint venture partner to market communications services. *See Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info.*, 22 FCC Rcd. 6927, 6947–54 ¶¶ 37–50 (2007) (*2007 CPNI Order*), *pet. for rev. denied*, *Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) . That order cautioned that "a carrier that practices willful blindness" regarding the protection of CPNI likely "would not be able to demonstrate that it has taken sufficient measures" to comply with Section 222 and the Commission's rules. *Id.* at 6946 ¶ 35. The Commission further clarified that a carrier does not satisfy its obligation to obtain customer approval before sharing CPNI with outside parties by simply adopting "contractual safeguards" that purport to make the outside parties responsible for protecting this information, given the heightened risks of unauthorized disclosures when information is shared with outside parties. *Id.* at 6952–53 ¶ 49.

The Commission's rules further require that telecommunications carriers "must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a). The Commission codified this requirement in response to a growing "black market for CPNI" and "the actions of data brokers * * * to obtain private and personal information" from telecommunications carriers, including from Verizon. *2007 CPNI Order*, 22 FCC Rcd. at 6928–29 ¶¶ 1–2, 6034 ¶ 12 & n.35, 6946 ¶ 39.

3. Any person who "willfully or repeatedly fail[s] to comply with any of the provisions of [the Communications Act] or of any rule, regulation, or order issued by the Commission * * * shall be liable to the United States for a forfeiture penalty." 47 U.S.C. § 503(b)(1)(B).[1] The Act and the Commission's rules specify the maximum amount of the forfeiture penalty and set out factors that the Commission will consider in assessing a penalty. *See id.* § 503(b)(2)(B) & (E); 47 C.F.R. § 1.80(b). The Commission "shall take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the

[1] For obligations under the Communications Act, "willful" means "the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision." 47 U.S.C. § 312(f)(1); *see Order* ¶¶ 70–72 (JA72).

degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require." 47 U.S.C. § 503(b)(2)(E); 47 C.F.R. § 1.80(b)(11).

B. Factual Background

1. Verizon provides mobile voice and data services to millions of customers nationwide through its wireless network. *Order* ¶ 8 (JA48). Because wireless devices must continuously communicate with a carrier's cellular towers to enable users to receive and make calls, and customers typically carry their phones on their person or keep them nearby, carriers like Verizon know each customer's approximate location at all times. *Id.* ¶ 23 (JA54).

Until March 2019, Verizon ran a "Location-Based Services (LBS) program" that "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" (sometimes through additional intermediary companies). *Order* ¶ 8 (JA48). "In total, Verizon sold access to its customers' location information (directly or indirectly) to [65] third-party entities." *Ibid.* These entities purportedly used customer location data for services such as "roadside assistance, proximity marketing, transportation and

logistics, fraud mitigation/identity management, and mobile gaming/lottery." *Id.* ¶ 10 (JA49).

Verizon's LBS program "was largely governed via contractual provisions." *Order* ¶ 9 (JA48). "Verizon entered into contracts with Aggregators," who "then entered into their own contracts with various LBS providers." *Ibid.* "This arrangement meant that it was typically the LBS providers who were obligated 'to provide notice and obtain consent' from consumers—not the Aggregators or Verizon." *Id.* (JA49).

Verizon similarly contracted with "a third-party Auditor, Aegis Mobile," to ostensibly "validate and reconcile the records of consent events and the records of each access" supplied by each LBS provider. *Order* ¶ 11 (JA49). Because Aegis relied on self-reported records from LBS providers, however, a Verizon internal report in 2017 warned that "'it is possible for [LBS] program companies * * * to falsify consent records and obtain [Verizon] subscriber data without [customers'] consent.'" *Id.* ¶ 12 (JA50). "According to Verizon, Aegis 'applied fraud analytics techniques to refine its ability to broadly identify potential issues going forward'—but Verizon offered no examples of issues identified and addressed via such data analysis." *Ibid.*

2. On May 10, 2018, the *New York Times* reported that a Missouri sheriff named Cory Hutcheson used a location-finding service from LBS provider Securus Technologies to obtain unauthorized access to the location data of hundreds of people without legal authorization and without their consent. *Order* ¶¶ 13–14 (JA50–51); *see* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018). Hutcheson reportedly used this service to track a local judge, multiple highway patrol officers, and his predecessor as sheriff, among others. *See*, *e.g.*, *Order* ¶¶ 14, 89 (JA51, 77).

Securus was supposedly authorized to use Verizon customer location data to operate "an inmate collect-calling service," *Order* ¶ 43 (JA62)—that is, "to confirm that recipients of collect calls from inmates were not within a certain distance of a prison," Resp. to NAL at 3 (JA159).[2] This was touted "as a security measure to help prevent call recipients from doing such things as aiding breakout attempts or making illicit drops to inmates," and was supposed to be allowed only "after obtaining affirmative customer consent." *Ibid.* But the *New York Times* article

[2] Verizon "claims that it only approved applications for one of six specific types of Use Cases." *Order* ¶ 10 (JA49). It is not apparent which of the six listed use cases the inmate collect-calling service would fall under. *See ibid.*

(and a parallel federal criminal proceeding) revealed that Securus "offered a location-finding service to law enforcement and corrections officials that allowed such officials to access customer mobile device location *without* that device owner's knowledge or consent." *Order* ¶ 13 (JA50). That service simply required users to "input the telephone number of the device they wanted to locate" and "upload a document [and] check[] a box * * * certify[ing] the attached document is an official document giving permission to look up the location o[f] this phone number." *Id.* ¶ 14 (JA51) (internal quotation marks omitted). Upon doing so, "the Securus LBS platform would *immediately* provide the requested location information (regardless of the adequacy of the uploaded document)." *Ibid.*; *see*, *e.g.*, *id.* ¶ 61 n.204 (JA69) (Hutcheson "'upload[ed] entirely irrelevant documents * * * in lieu of genuine legal process'").

3. The day after the *New York Times* article, Verizon terminated access to customer location data for Securus and one other related provider. *Order* ¶ 15 (JA51). A month later, Verizon announced that it "intended" to terminate the aggregators' contracts, but it did not actually do so for many months after. *Id.* ¶ 16 (JA52). It did not stop providing customer location data to most LBS providers until November 30, 2018,

more than 200 days after the *Times* report. *Ibid.* And it allowed four LBS providers and one of the aggregators to continue accessing customer location data until March 30, 2019, which was 324 days after the *Times* article. *Id.* ¶ 18 (JA52).

While it continued operating the flawed LBS program, Verizon began testing "a 'Direct Location Services' program as an alternative, under which Verizon itself would obtain consent from its customers * * * by sending its customer a text message and only sharing location information with an LBS provider if the Verizon customer responded affirmatively." *Order* ¶ 17 (JA52). Ultimately, however, Verizon decided to instead "completely exit[] the location-based services business" rather than continue with a Direct Location Services program. *Id.* ¶ 18 (JA52).

C. The Commission's Forfeiture Order

1. Section 503(b) of the Communications Act provides two routes by which the Commission may pursue a forfeiture. *See AT&T Corp. v. FCC*, 323 F.3d 1081, 1083–84 (D.C. Cir. 2003).

Under Section 503(b)(3), the Commission may initiate a formal adjudication before an administrative law judge or the Commission itself, and any resulting forfeiture is reviewable directly in a court of appeals. 47 U.S.C. § 503(b)(3) (citing 47 U.S.C. § 402(a)).

Alternatively (and more typically), under Section 503(b)(4), the Commission may "issue[] a notice of apparent liability" that "set[s] forth the nature of the act or omission charged * * * and the facts upon which such charge is based"; provide the alleged violator an opportunity to respond in writing; and then, after considering all relevant information, assess an appropriate forfeiture penalty. 47 U.S.C. § 503(b)(4); *see* 47 C.F.R. § 1.80(g). Any forfeiture penalty assessed under this procedure "shall be recoverable pursuant to section 504(a)," 47 U.S.C. § 503(b)(4); *see* 47 C.F.R. § 1.80(g)(5), which requires the government to bring "a civil suit in the name of the United States" in federal district court and provides that "any [such] suit * * * shall be a trial de novo," 47 U.S.C. § 504(a). The D.C. Circuit has held, however, that a carrier may elect to waive its opportunity for trial by paying the forfeiture immediately and may then petition for review in a court of appeals under 47 U.S.C. § 402(a). *See AT&T Corp.*, 323 F.3d at 1083–85.

2. The Commission here followed the second pathway. On February 28, 2020, the Commission issued a Notice of Apparent Liability proposing a $48,318,750 penalty against Verizon for its apparent willful and repeated violations of Section 222 and the Commission's implementing rules by failing to protect its customers' CPNI. *See* Notice

of Apparent Liability, *In re Verizon Commc'ns*, 35 FCC Rcd. 1698 (2020) (*NAL*), *reprinted at* JA112–56. "In particular," the Commission alleged that "for almost a year after Verizon became aware of Securus's unapproved location-finding service—and thereby had notice that the 'consent records' it received through indirect arrangements with location-based service providers were not reliable indicia of customer consent—the Company's continued reliance on such attenuated consent mechanisms and ineffective monitoring tools apparently did not meet" its obligation to protect customer location data. *Id.* ¶ 40 (JA126).

The Notice of Apparent Liability tentatively found that Verizon committed 65 continuing violations of the Act—one for each aggregator or LBS provider that it provided access to its customers' location data without effective safeguards. *NAL* ¶¶ 86–87 (JA140). For each violation, the Commission proposed "a base forfeiture of $40,000 for the first day of such a violation," beginning 30 days after the *New York Times* article put Verizon on notice, "along with a $2,500 forfeiture for * * * each successive day that the violation continued." *Ibid.* The Commission also proposed a "substantial" 50% upward adjustment in light of the egregiousness of Verizon's conduct. *Id.* ¶¶ 90–92 (JA141–42).

3. After considering Verizon's responses to the Notice of Apparent Liability and all evidence in the record, the Commission issued its Forfeiture Order adopting the proposed forfeiture (apart from a slight revision to the penalty amount). *See* JA45–90 (*Order*).

The Commission first determined that customers' location data "falls squarely within" the statutory definition of CPNI. *Order* ¶¶ 22–34 (JA53–58). Relying on plain meaning and ordinary tools of statutory interpretation, the Commission reasoned that customer location data "relates to the location of a telecommunications service—i.e., Verizon's commercial mobile service." *Id.* ¶¶ 23–28 (JA54–56). Likewise, "the location information at issue was obtained by Verizon solely by virtue of its customer–carrier relationship" because Verizon's customers provided their location to Verizon to use the services they purchase from it, not for some unrelated reason. *Id.* ¶¶ 29–33 (JA56–58).

The Commission next concluded that Verizon "violated section 222 of the Act and section 64.2010 of [the Commission's] rules by failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information." *Order* ¶ 42 (JA61); *see id.* ¶¶ 46–58 (JA63–68). "[T]he record not only shows that Verizon did not have reasonable protections in place prior to [the]

2018 *New York Times* article detailing the Securus/Hutcheson breaches, but also that Verizon failed to promptly address its demonstrably inadequate CPNI safeguards after [the] Securus/Hutcheson disclosure." *Id.* ¶ 46 (JA63). Verizon relied almost exclusively on contractual arrangements to govern the use of location data, without any reliable means to "assure that location-based service providers comply with [their] contractual obligation to access location information only after furnishing proper notice and receiving customer consent." *Id.* ¶ 48 (JA65). And even after the *New York Times* article revealed serious abuses, "rather than promptly implementing reasonable safeguards, Verizon continued to sell access to its customers' location information under (for all intents and purposes) the *same system* that was exploited by Securus and Hutcheson." *Id.* ¶ 52 (JA65–66).

The Commission rejected Verizon's arguments that the forfeiture procedures violated the Constitution. *Order* ¶¶ 90–100 (JA77–83). Among other things, Verizon's Seventh Amendment objection failed because Verizon would be "entitled to a trial *de novo* in federal district court before it [could] be required to pay the forfeiture," *id.* ¶ 91 (JA78), and because the forfeiture involves public rights rather than private rights covered by the Seventh Amendment, *id.* ¶¶ 97–98 (JA80–82).

The Commission ultimately found that "Verizon is liable for a total forfeiture of $46,901,250" for its violations, "a reduction of $1,417,500" from the forfeiture proposed in the Notice of Apparent Liability. *Order* ¶ 66 (JA70–71). The Commission generally adopted the proposed forfeiture calculation from the Notice of Apparent Liability, *see NAL* ¶¶ 86–87, 90–93 (JA140–42), but reduced the amount based on new information from Verizon that "two of the 65 entities cited in the *NAL* did not actually participate in the program," *Order* ¶¶ 85–86 (JA76).

4. Verizon did not wait for the government to bring a civil suit to recover the forfeiture under Section 504(a), which would have provided it the opportunity to pursue a de novo jury trial in district court. *See* 47 U.S.C. § 504(a). Instead, Verizon elected to forgo that opportunity and paid the forfeiture penalty in order to pretermit any trial and pursue direct appellate review in this Court. *See* Pet'r Br. 7 (citing *AT&T Corp.*, 323 F.3d at 1083–85, and *ABC, Inc. v. FCC*, 404 F. App'x 530 (2d Cir. 2011) (unpublished summary order)).

STANDARD OF REVIEW

Under the Administrative Procedure Act, a court may overturn agency action only if it is arbitrary, capricious, or otherwise contrary to law. *See* 5 U.S.C. § 706(2). The APA "mandate[s] that judicial review of

agency policymaking and factfinding be deferential." *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 392 (2024). "'An agency's factual findings must be supported by substantial evidence,' which means 'such relevant evidence as a reasonable mind might accept as adequate to support a conclusion.'" *Cablevision Sys. Corp. v. FCC*, 570 F.3d 83, 91 (2d Cir. 2009).

The Court reviews constitutional issues de novo. *Cablevision*, 570 F.3d at 91. Courts also "must exercise their independent judgment in deciding whether an agency has acted within its statutory authority." *Loper Bright*, 603 U.S. at 412. "In exercising such judgment, though," courts may appropriately "seek aid from the interpretations of" the implementing agency. *Id.* at 394; *see also id.* at 412–13.

SUMMARY OF THE ARGUMENT

I. The Commission properly concluded that the statutory definition of "customer proprietary network information" includes the customer location data at issue here. Section 222 of the Communications Act expressly covers "location" information, and Verizon customers share that information with Verizon solely because they must do so to use the services they purchase from it, not for some unrelated reason. Verizon's effort to restrict CPNI to only "*call* location information" is at odds with

its own prior practice as well as with the statute itself, which defines CPNI to include all "location" information while using the narrower phrase "call location information" elsewhere. *Compare* 47 U.S.C. § 222(h)(1)(A) *with id.* § 222(d)(4) *and id.* § 222(f)(1).

II. The Commission's conclusion that Verizon failed to protect its customers' location information is reasonable and well-supported by the record. "[T]he record not only shows that Verizon did not have reasonable protections in place prior to [the] 2018 *New York Times* article detailing the Securus/Hutcheson breaches, but also that Verizon failed to promptly address its demonstrably inadequate CPNI safeguards after [the] Securus/Hutcheson disclosure." *Order* ¶ 46 (JA63); *see id.* ¶¶ 46–58 (JA63–67).

The Commission assessed a forfeiture penalty only for the period after Verizon was put on notice by the *New York Times* article that its protections were ineffective and that it was not meaningfully in control of its customers' location information when providing access to outside parties. The forfeiture is fully justified based on Verizon's failure to promptly identify and address the vulnerabilities, or to stop sharing customer location information until it could do so. The Commission identified numerous steps that Verizon could have taken, but Verizon

instead continued to put its customers' location data at risk by persisting in selling access to that information for the better part of a year under essentially the same system that was exploited by Securus and Hutcheson.

As independent support for the forfeiture, Verizon's practices also were inadequate even before the Securus disclosures came to light. Verizon did not itself provide customer notice and obtain or verify customer approval, but instead relied principally on an attenuated chain of contractual arrangements directing aggregators and LBS providers to do so. This reliance on contractual provisions was not reasonable because Verizon had no reliable means to assure that location-based service providers complied with their contractual obligations and that the customer data was not being misused. Indeed, the Commission warned in the *2007 CPNI Order* that a carrier does not satisfy its obligation to protect CPNI simply by adopting "contractual safeguards" that purport to assign the responsibility to others. Verizon likewise had no means to verify whether its third-party auditor, Aegis, was doing its job, and the perfunctory reviews performed by Aegis were incapable of detecting certain abuses—as Verizon was warned in a 2017 internal report which found that it was possible for LBS providers to falsify consent records and obtain customer location data without the customers' consent.

The Commission's calculation of the forfeiture amount was likewise appropriate. Consistent with the Communications Act and established agency practice, the Commission found that Verizon committed 63 continuing violations of the Act—one for each entity to which Verizon provided access to its customers' location data without effective safeguards. Verizon points to nothing in the statute, the Commission's rules, or past practice that compels a contrary approach.

III. The Commission's forfeiture procedures did not deprive Verizon of any Seventh Amendment jury-trial right because Verizon had the opportunity to demand a de novo jury trial in a Section 504(a) enforcement suit before the government could make it pay the forfeiture. Instead, it waived that opportunity by electing to pay the penalty and seeking direct review in this Court instead. In any event, the Seventh Amendment provides no jury-trial right for claims that, like those here, involve public rights, rather than private rights with a common-law analogue.

ARGUMENT

I. THE COMMISSION PROPERLY CONCLUDED THAT CUSTOMER LOCATION DATA IS CPNI PROTECTED BY SECTION 222.

The customer location data at issue here falls comfortably within the statutory definition of CPNI. *See Order* ¶¶ 22–34 (JA53–58). Section

222(h)(1)(A) defines CPNI to include "information that relates to the quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and that "is made available to the carrier by the customer solely by virtue of the carrier–customer relationship." 47 U.S.C. § 222(h)(1)(A) (emphasis added). Both prongs are satisfied here: the statute specifically protects "location" information, and customers share their location with Verizon solely to use the services they purchase from it, not for some unrelated reason.

A. The Location Data Is "Information That Relates To The * * * Location" Of A Telecommunications Service.

To start, the customer location data at issue is "information that relates to the * * * location * * * of a telecommunications service," 47 U.S.C. § 222(h)(1)(A)—here, "Verizon's commercial mobile service." *Order* ¶ 23 (JA54). A wireless carrier "'must be aware of and use [a] device's location in order for it to enable customers to send and receive calls,'" and "Verizon does not dispute * * * that customers' devices and Verizon's network regularly exchange information" to "ensur[e] that they can receive incoming calls and place outgoing calls." *Id.* ¶¶ 23, 26 (JA54–55). This is true "'regardless of whether the device is actively in use for

a call'" or merely idle, since the device must continuously maintain a connection to the carrier's network for any incoming call to be received. *Id.* ¶ 23 (JA54).

Verizon's relabeling of this data as "device-location information" (Br. 28, 33) is therefore a misnomer. A carrier knows a device's location *only when it is in service* (whether engaged in a call or not), not when the device is powered off or wireless service is disabled. The data is more precisely described as "information that relates to the * * * location" where the customer is receiving "telecommunications service," 47 U.S.C. § 222(h)(1)(A); it does not contain information on where a device might be located when the customer is not receiving service.

Verizon now contends (Br. 33–36) that "information that relates to the * * * location * * * of a telecommunications service" in Section 222(h)(1)(A) should be read to mean only "*call* location information"—*i.e.*, information identifying where a particular call was made or received. That position is at odds with Verizon's own prior practice, in which it admittedly "treated both call location information and non-call location information in the same way for consent purposes and maintained the same protections for both in connection with" its location-based services programs. Resp. to Supp. Letter of Inquiry at 7 (JA14).

The Court should reject Verizon's effort to rewrite the statute. By its plain terms, Section 222 covers any "information that relates to the * * * location * * * of a telecommunications service," 47 U.S.C. § 222(h)(1)(A), not just information that relates to the location of a call. *See Order* ¶ 28 (JA56) ("All *location* information is protected as CPNI under [Section 222](h)(1)(A)."). It is undisputed that a wireless phone must continuously share its location with a carrier to enable it to receive incoming calls—a key part of the telecommunications service Verizon offers—even when not engaged in a call. *Id.* ¶¶ 23–26 (JA54–55). Section 222(h)(1)(A)'s use of the phrase "information that *relates to* * * * location" reinforces that it must be construed broadly, because "as the Supreme Court has recognized, Congress's use of the phrase 'relating to' in federal legislation generally signals its expansive intent." *Mizrahi v. Gonzales*, 492 F.3d 156, 159 (2d Cir. 2007).

What is more, Section 222(h)(1)(A)'s unadorned use of the bare term "location" contrasts with use of the narrower phrase "call location" elsewhere in Section 222. *Compare* 47 U.S.C. § 222(h)(1)(A) *with id.* § 222(d)(4) (addressing "call location information") *and id.* § 222(f)(1) (same). "'[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally

presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion,'" *Russello v. United States*, 464 U.S. 16, 23 (1983), and the "negative implications raised by disparate provisions are strongest when the [provisions] were being considered simultaneously," *Lindh v. Murphy*, 521 U.S. 320, 330 (1997); *see also Crescenzi v. City of New York*, 939 F.3d 511, 515 (2d Cir. 2019) ("[T]he striking differences in the wording of the two clauses actually prove[s] * * * that a textually sound interpretation * * * must assign a *different* meaning to each clause."); Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* § 25, at 170 (2012) ("[A] material variation in terms suggests a variation in meaning."). Had Congress wished to limit protection to call location information, as Verizon now contends, it could have used a term like "call location" in Section 222(h)(1)(A)—as it did elsewhere in the statute—instead of affording protection more broadly to all "information that relates to the * * * location" of service.

Contrary to Verizon's arguments (Br. 34–35), there is nothing "nonsensical" about permitting carriers to disclose call-location information to first responders without first securing consent "in order to respond to the user's call for emergency services," 47 U.S.C.

§ 222(d)(4)(A), yet requiring customer approval to disclose broader location data. Congress reasonably may presume that a user who calls an emergency-services number will want and expect to share the location they are currently calling from, yet may be more reluctant to give law enforcement and other authorities *carte blanche* access to *all* of the user's location information that may have nothing to do with a present emergency. Nor is Verizon correct to suggest (Br. 35) that it is irrational for Congress to require heightened consent for the use or disclosure of call-location information, 47 U.S.C. § 222(f)(1), but not necessarily for other forms of location information under Section 222(c)(1). Data that shows where a user was located when making particular calls may reveal information that even a broader set of location data alone (without linking locations to calls) does not. In any event, given the Commission's regulations generally requiring opt-in approval for use or disclosure of CPNI, there is in practice no meaningful difference in the form of consent that applies for different types of location information.[3]

---

[3] Amicus CTIA—but not Verizon—focuses on the words "of use" to argue that a customer must be actively engaged in making a call for their location to constitute CPNI. *See* CTIA Br. 10–15. The statutory phrase "of use," however, modifies the immediately preceding word "amount," not the entire preceding list. *See Order* ¶ 24 (JA54); (cont'd)

B. The Location Data Was "Made Available To The Carrier * * * Solely By Virtue Of The Carrier–Customer Relationship."

The location data here is likewise information that was "made available to the carrier"—that is, to Verizon—"by the customer solely by virtue of the carrier–customer relationship." 47 U.S.C. § 222(h)(1)(A). As the Commission explained, "'Verizon's customers provided their wireless location data to Verizon because of their customer–carrier relationship with Verizon,'" *Order* ¶ 29 (JA56), since the wireless phone service they purchased from Verizon requires this information to operate, *id.* ¶¶ 23, 26, 31 (JA54, 55, 57).

The carrier–customer relationship is the "sole[]" reason that customers provide this information to Verizon. Customers share their location with Verizon solely to use the services they purchase from it, not

---

Lockhart v. United States, 577 U.S. 347, 351 (2016) ("a limiting clause or phrase * * * should ordinarily be read as modifying only the noun or phrase that it immediately follows"). Indeed, it would make little sense to read Section 222(h)(1)(A) to refer to the "technical configuration * * * of use." And even if "of use" did modify the word "location," it would not alter it to mean "call location." "When customers' devices are exchanging communications with Verizon's network, and thereby ensuring that they can receive incoming calls and place outgoing calls, * * * 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." *Order* ¶ 26 (JA55).

for some unrelated reason. If they were not Verizon customers, they would not share their location with Verizon.[4]

Verizon contends (Br. 29–32) that it did not obtain customer location data "solely by virtue of the carrier–customer relationship" because most of the customers who provided their location by using wireless telephone service, which is a "telecommunications service" covered by Section 222(c)(1), also provided the same location information to use text messaging or wireless internet service, which are classified as "information services" rather than "telecommunications services." That argument fails because the "solely by virtue of" language does not ask whether the carrier obtained the CPNI solely through *its telecommunications service*; instead, by its terms, it asks whether the

---

[4] Verizon is wrong (Br. 31) that the Commission's approach "reads that phrase out of the statute." The "solely by virtue of the carrier–customer relationship" language in Section 222(h)(1)(A) distinguishes customer information obtained through the carrier's provision of service to a customer from information obtained through some unrelated means. For instance, if Verizon's website invited prospective customers to submit their names and home addresses to obtain more information about services available at their locations, it would obtain those addresses independent of any carrier–customer relationship. Use of these addresses collected prior to or outside of any carrier–customer relationship would not be covered by the Commission's CPNI rules, whereas use of any information obtained solely through a carrier–customer relationship would be.

carrier obtained the CPNI through "the carrier–customer *relationship*." 47 U.S.C. § 222(h)(1)(A) (emphasis added).

That "carrier–customer relationship" may encompass multiple services, including information services. *See Order* ¶ 32 (JA57) (reasoning that a carrier's "provision of multiple services to its telecommunications customers (including [information] service[s])" does not "take[] the resulting *relationship* outside the scope of the 'carrier–customer' relationship"). If a carrier like Verizon leverages the wireless telephone service that it provides a customer to sell that customer additional services as part of a package, all of those services are reasonably encompassed within the carrier–customer relationship. Indeed, the Commission's CPNI rules specifically recognize that the "communications-related services" provided by carriers include "information services * * * that are typically provided by telecommunications providers, such as Internet access or voice mail services." 47 C.F.R. § 64.2003(e) & (*i*).

The statute's focus on the "carrier–customer relationship" as a whole makes sense, whereas Verizon's contrary approach would all but eviscerate Section 222's protections. The duty to protect CPNI attaches

under Section 222 when a customer's purchase of telecommunications service provides the carrier with protected information. Under Verizon's reading, however, carriers could then negate that obligation simply by bundling additional information services like text messaging with their wireless telephone service (as virtually all wireless carriers now do). It is not plausible that Congress intended for wireless carriers to be able to nullify the protections of Section 222 by simply bundling non-telecommunications services together with their telecommunications services.

Searching for support outside of Section 222, Verizon cites (Br. 29–30) the Act's definition of "telecommunications carrier," which states that "[a] telecommunications carrier shall be treated as a common carrier under [this Act] only to the extent that it is engaged in providing telecommunications service," 47 U.S.C. § 153(51), to argue that "carrier–customer relationship" encompasses only its telecommunications services and not its information services. But the terms "carrier" and "customer" are used in Section 222(h)(1)(A) simply to identify the relevant parties via their relationship to one another—in the phrase "made available by the customer to the carrier" and in the phrase

"carrier–customer relationship"—rather than to distinguish among different services encompassed within that relationship. It is unreasonable to think that Congress would try to draw the distinction Verizon seeks in such an obscure and elliptical manner, especially given the unnatural consequence it would have of effectively negating wireless carriers' responsibility to protect CPNI if they bundle their wireless telephone service with text messaging or wireless internet service.

II. THE COMMISSION'S FORFEITURE DETERMINATION IS REASONABLE AND SUPPORTED BY THE RECORD.

Courts review the Commission's forfeiture determinations under the traditional arbitrary-and-capricious standard. *Grid Radio v. FCC*, 278 F.3d 1314, 1322 (D.C. Cir. 2002). Under that "narrow and particularly deferential" standard, the Court asks whether the agency has offered "a reasoned connection between the facts it found and the choice it made" and will "reverse the agency only when there has been a 'clear error in judgment.'" *Envtl. Def. Fund v. U.S. EPA*, 369 F.3d 193, 201 (2d Cir. 2004); *see also Grid Radio*, 278 F.3d at 1322 ("As in any arbitrary-and-capricious challenge, we 'presume the validity' of the agency's action"'). The Commission's forfeiture order easily clears that bar.

A. The Commission Reasonably Found That Verizon Failed To Protect Customer Location Data.

The Commission reasonably concluded that "Verizon violated section 222 of the Act and section 64.2010 of [the Commission's] rules by failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information." *Order* ¶ 42 (JA61). As the Commission explained, the record shows that "Verizon failed to promptly address its demonstrably inadequate CPNI safeguards after [the] Securus/ Hutcheson disclosure" was revealed by the *New York Times* in May 2018, and that it separately "did not have reasonable protections in place prior to [the] 2018 *New York Times* article." *Order* ¶ 46 (JA63).

1. The Commission imposed a forfeiture penalty only for the period *after* Verizon was put on notice by the *New York Times* article that Securus and Hutcheson were able to obtain unauthorized access to its customers' location data (and only after an additional 30-day grace period to take appropriate action). *See Order* ¶¶ 66, 81 (JA70–71, 75); *NAL* ¶¶ 86–87 & tbl.1 (JA140–41); *see also NAL* ¶ 74 (JA135) ("[W]e focus on the actions that Verizon took, or failed to take, after discovery of that breach.").

Verizon points (Br. 36–37) to various protections it supposedly had in place, but it ignores that the Securus disclosures "revealed fundamental shortcomings in Verizon's safeguards," *Order* ¶ 53 (JA66), and put Verizon on notice that it was not meaningfully in control of its customers' location information when providing access to outside parties. *See NAL* ¶ 74 (JA135) ("Setting aside the inadequacy of Verizon's safeguards before disclosure of the Securus and Hutcheson breaches, Verizon was on clear notice that its safeguards were inadequate after the disclosure"). "Continu[ing] to sell access to its customers' location information under (for all intents and purposes) the *same system* that was exploited by Securus and Hutcheson" was not reasonable when Verizon was on notice that its existing measures failed to prevent unauthorized access to and disclosure of protected information. *Order* ¶ 52 (JA65–66).

The Commission identified "numerous steps that could have been taken to squarely address the proven vulnerability, up to and including deploying enhanced measures to verify consumer consent (even directly verifying consumer consent) and shutting down the LBS program." *Order* ¶ 57 (JA67). But "[r]ather than taking reasonable steps to safeguard its customers' location information after the Securus/ Hutcheson disclosures were reported, Verizon placed its customers'

location information at continuing risk of unauthorized access through its failure to terminate its program or impose reasonable safeguards to protect its customers' location information." *Id.* ¶ 65 (JA70).

Verizon states that it "immediately cut off access to * * * Securus" and "ceased taking new applications to join the program" (Br. 38), but "those actions did not improve the safeguards for consumers whose location information could be disclosed under the location data sharing arrangements that remained in place." *Order* ¶ 55 (JA66). Verizon did not even "suspend the access of LocationSmart, the Aggregator that had the contractual obligations to monitor Securus." *NAL* ¶ 75 (JA135). Nor is there any indication that Verizon acted "to promptly ascertain the full scope and extent of the Securus breach" or "to determine whether the Securus incident was an isolated occurrence, or whether it was indicative of a broader vulnerability with Verizon's program." *Id.* ¶¶ 76–77 (JA136). Verizon states that it "had Aegis strengthen the transaction verification process to identify any anomalies in the data" (Br. 38), but the Commission found no "reason to believe that those particular measures were likely to have identified the problem that enabled the Securus and Hutcheson breaches" or "remedied those shortcomings." *Order* ¶ 55 (JA65). And in any event, improving detection of improper

disclosures *after* they occur does not remedy those disclosures and is no substitute for preventing improper disclosures from occurring in the first place.

As it did before the Commission, Verizon argues (Br. 22, 40 n.16) that it was justified in continuing to operate a flawed program for the better part of a year by pointing to the purported benefits that location-based services provide to customers. In essence, Verizon argues that these benefits outweigh the risk of harm. But Section 222 mandates that carriers "protect the confidentiality of proprietary information of * * * customers" in all circumstances and forbids unlawful use or disclosure of CPNI "[e]xcept * * * with the approval of the customer," irrespective of any purported benefits of doing otherwise. 47 U.S.C. § 222(a) & (c)(1). And "these purported benefits simply assume that customers had in fact consented for such uses—a premise Verizon should not have relied on given its own findings" that LBS providers could falsify the consent records. *NAL* ¶ 81 (JA138); *see Order* ¶ 12 (JA50) (discussing an internal report finding that "it is possible for [LBS] program companies * * * to falsify consent records and obtain [Verizon] subscriber data without their consent"); *id.* ¶ 43 (JA62) (none of the location requests made through

Securus "evinced a customer's actual opt-in consent"). Under Section 222, "[i]f Verizon could not reasonably safeguard the customer location information that it sold access to, then it should have ceased to sell access to that information." *NAL* ¶ 79 (JA137).

Verizon's insistence that it lacked fair notice of the need to act (Br. 40–41) is baseless. The fair-notice doctrine "provides redress only if an agency's interpretation is so far from a reasonable person's understanding of the [law] that they could not have fairly informed the regulated party of the agency's perspective." *Order* ¶ 37 (JA59) (quoting *Miss. Comm'n on Envtl. Quality v. EPA*, 790 F.3d 138, 186 (D.C. Cir. 2015)); *see*, *e.g.*, *United States v. Gasperini*, 894 F.3d 482, 487 (2d Cir. 2018). Here, a reasonable person who had actual notice that the existing protections for using or accessing CPNI under Section 222 were ineffective would have little trouble realizing that they must promptly identify and fix the vulnerabilities, or else stop using or sharing this information until they can do so. That is especially so for Verizon, a "sophisticated" actor well versed in the statute and the Commission's regulatory policies. *Cf. United States v. Chestman*, 947 F.2d 551, 564 (2d Cir. 1991).

2. As an alternative and independent justification for the forfeiture, Verizon's practices also were inadequate even before the Securus disclosures came to light. *See Order* ¶ 48 (JA64); *NAL* ¶¶ 60–73 (JA131–35).

Verizon did not provide customer notice and obtain or verify customer approval itself. Instead, it relied on an attenuated chain of contractual requirements that aggregators and LBS providers supply notice and obtain customer consent to use location data, that these entities do so only for preapproved use cases, and that they otherwise adhere to applicable laws and industry best practices. *Order* ¶ 9 (JA48–49). "Verizon entered into contracts with the Aggregators," and "the Aggregators [in turn] entered into their own contracts with various LBS providers." *Id.* (JA48). "This arrangement meant that it was typically the LBS providers who were obligated 'to provide notice and obtain consent' from consumers—not the Aggregators or Verizon." *Id.* (JA49); *see NAL* ¶ 69 (JA134) ("In other words, these contractual requirements were largely passed down to the entities responsible for obtaining consent and that used the location information * * * through an attenuated chain of downstream contracts.").

This reliance on contractual safeguards "w[as] not reasonable" because Verizon had no reliable means to "assure that location-based service providers comply with [their] contractual obligation to access location information only after furnishing proper notice and receiving customer consent." *Order* ¶ 48 (JA64); *cf. NAL* ¶ 69 (JA134) ("To enforce the requirements, Verizon would have needed to take steps to determine whether they were actually being followed."). The Commission specifically cautioned in the *2007 CPNI Order* that a carrier does not satisfy its obligation to protect CPNI simply by adopting "contractual safeguards" that purport to assign its responsibility to others. *2007 CPNI Order*, 22 FCC Rcd. at 6952–53 ¶ 49. Indeed, the Communications Act specifically provides that the "failure of any officer, agent, or other person acting for or employed by any common carrier * * * shall in every case be also deemed to be the act, omission, or failure of such carrier." 47 U.S.C. § 217. And the Commission has likewise warned that "a carrier that practices willful blindness" regarding the protection of CPNI likely "would not be able to demonstrate that it has taken sufficient measures" to comply with Section 222 and the Commission's rules. *2007 CPNI Order*, 22 FCC Rcd. at 6946 ¶ 35.

Verizon also maintains (Br. 17–18, 36) that it contracted with a third-party auditor, Aegis, to "review * * * consent records" and "otherwise monitor" the program. As with its other contractual agreements, however, Verizon had no means to verify whether Aegis was doing its job. *Cf. Order* ¶ 64 (JA70). And Aegis's "review" of consent records consisted essentially of comparing the list of "location requests" provided by an LBS provider with the list of purported "consent records" *also provided by the LBS provider*—a system that "assumed that the location requests and consent records provided by the [providers] would be legitimate in the first instance," and could not detect if an LBS provider simply fabricated the consent records. *NAL* ¶ 67 (JA133). Indeed, an internal report Verizon produced in 2017 specifically warned that "it is possible for [LBS] program companies * * * to falsify consent records and obtain [Verizon] subscriber data without their consent." *Order* ¶ 12 (JA50). Likewise, Aegis "was unable to distinguish location requests unrelated to [an] authorized use case," and Securus's location requests for unauthorized uses "did not trigger any review by Aegis." *Id.* ¶ 43 (JA62). Aegis's perfunctory "audits" were thus incapable of detecting that "Securus was able to set up a separate program to access and disclose customer location information and operate it *for at least four years* in a manner inconsistent

with its contract." *NAL* ¶ 63 (JA132). "A system allegedly designed to monitor customer consents but that is incapable of detecting its opposite is not a 'reasonable measure' to detect unauthorized uses of or access to CPNI." *Order* ¶ 48 (JA64) (quoting *NAL* ¶ 70 (JA134)).

Instead of contractually passing the buck for protecting CPNI to others, Verizon could have provided the required notice and verified consent itself, as demonstrated by the "Direct Location Services" program it later tested in 2018. *NAL* ¶ 78 (JA137). Under that program, third-party providers "could access Verizon customer location information upon consent for specific use cases, but Verizon itself obtained consent from its customers" by "sending its customer a text message seeking affirmative consent to share the customer's location information." *Id.* ¶ 33 (JA124–25). This would have allowed Verizon to ensure proper notice and customer approval, and to verify location requests against its own records rather than provider-supplied records that could be falsified.

3. Verizon seeks to downplay its lapses (Br. 41) as supposedly affecting only "a handful of customers through one participating service provider that slipped through Verizon's safeguards." Yet because Verizon was "incapable of detecting" providers who used or disclosed customer location data unlawfully, the full extent to which the program was

exploited may never be known. *Order* ¶¶ 48, 58 (JA64, 68) (quoting *NAL* ¶ 70 (JA134)); *cf. Order* ¶ 49 (JA65) ("reject[ing]" the "theory that the reasonableness of those measures can be inferred from the fact that even more unauthorized disclosures have not been publicly identified"). And Section 222 imposes upon carriers an affirmative duty to employ adequate safeguards to protect their customers' data; violations are not limited to situations involving a known misappropriation of customer data.

Verizon fails to grapple with the Commission's undisputed factual findings about the harm to consumers. Verizon was selling access to the location data of millions of its customers without *any* meaningful way of verifying that those customers consented to such access, or that its downstream contractual partners were not abusing the system. The risk posed by this scheme "was not merely theoretical." *NAL* ¶ 91 (JA142). It was actually exploited—by Hutcheson to "'submit[] thousands of Securus LBS requests and [to] obtain[] the location data of hundreds of individual phone subscribers,'" *Order* ¶ 14 (JA51), and more broadly by "Securus's entire location-finding service * * * every time Securus submitted a request for location information under the guise of its approved use case (a use case that required consumer consent) and Verizon provided the requested location information" without consent and for a different use

case, *id.* ¶ 43 (JA61–62). And Verizon did nothing to ensure that the same exploits were not possible across other location-based service providers to which it gave access.

"Rather than taking reasonable steps to safeguard its customers' location information after the Securus/Hutcheson disclosures were reported," moreover, "Verizon placed its customers' location information at continuing risk of unauthorized access through its failure to terminate its program or impose reasonable safeguards." *Order* ¶ 65 (JA70). And the Commission found that Verizon's "failure to adequately protect CPNI for a protracted amount of time caused substantial harm by making it possible for malicious persons to identify the exact locations of Verizon subscribers who belong to law enforcement, military, government, or other highly sensitive positions—thereby threatening national security and public safety." *Order* ¶ 89 (JA77) (internal quotation marks omitted).

B. The Commission Reasonably Found That Verizon Committed 63 Continuing Violations By Continuing To Share Location Data With 63 Separate Entities.

The Commission reasonably found that Verizon "engaged in [63] continuing violations—one for each ongoing relationship with a third-party LBS provider or aggregator that had access to Verizon customer location information more than 30 days after publication of the *New York*

Times report—and that each violation continued until Verizon terminated the corresponding entity's access to customer location information." *Order* ¶ 66 (JA71); *see NAL* ¶¶ 86–87 (JA140). Given the base forfeiture amount and the upward adjustment for Verizon's "egregious" conduct, *Order* ¶ 89 (JA76–77), this resulted in a total forfeiture penalty of $46,901,250. That conclusion reflects no "clear error of judgment," *Envtl. Def. Fund*, 369 F.3d at 201, and "the scale of the fine imposed" readily satisfies arbitrary-and-capricious review, *see SBC Commc'ns Inc. v. FCC*, 373 F.3d 140, 151 (D.C. Cir. 2004).

Verizon maintains (Br. 42) that its provision of access to 63 separate entities without proper protections, each of which separately contract for that access (either with Verizon or with an aggregator), was "a single act or failure to act" rather than 63 separate violations. Yet Verizon points to nothing in the statute or the Commission's rules that compels its approach. *Order* ¶ 78 (JA74).

Consistent with established practice, the Commission treats systemic privacy failings as "significantly more than a single violation." *Order* ¶ 78 (JA74) (citing *In re TerraCom, Inc.*, 29 FCC Rcd. 13325, 13343 ¶ 50 (2014)). The unit of analysis depends on the nature of the conduct that violated the law. For example, in *TerraCom*, because the penalized

parties had unreasonably exposed customers' documents by storing them on publicly accessible servers, each separate document was a distinct violation. *See id.*

Considering the specific conduct here, the Commission "reasonably exercised its authority to find that each unique relationship between Verizon and an LBS provider or aggregator represented a distinct failure to reasonably protect customer CPNI," because "[e]ach such relationship relied upon a distinct and unique contractual chain," and "specific, individually-approved 'Use Case[s]' * * * had been reviewed and authorized by Verizon." *Order* ¶ 79 (JA74). In other words, each time Verizon agreed to share customer data with another third party without ensuring adequate safeguards for that data, it violated Section 222. Because Verizon treated each third-party provider in its LBS program separately through distinct contractual relationships and individual use-case approvals, it was reasonable for the Commission to do so as well in calculating Verizon's liability.

A contrary method would make little sense. Under Verizon's proposed approach, carriers would be free to maintain that they had a single "systemic" unreasonable practice that they simply applied in numerous instances, as Verizon protests here (Br. 42–43). In such cases,

a carrier that commits a "systemic failure to protect customer information," *Order* ¶ 78 (JA74), would be insulated from anything more than a single capped penalty—which, even at the statutory maximum, would be insignificant in view of Verizon's $134 billion in annual operating revenues. *See* Verizon Commc'ns, Inc., Form 10-K (Feb. 9, 2024).[5] Congress, which directed the Commission to take into account a violator's "ability to pay" in calculating the forfeiture amount, 47 U.S.C. § 503(b)(2)(E), could not have required such an ineffectual result.

III. THE COMMISSION'S FORFEITURE PROCEDURES DID NOT VIOLATE THE SEVENTH AMENDMENT.

Verizon lastly contends (Br. 44–52) that the Commission's forfeiture procedures violated the Seventh Amendment, which provides in relevant part that "[i]n Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved." U.S. Const. Amend. VII. That argument fails for two independent reasons. First, Verizon *had* the opportunity to demand a de novo jury trial in an enforcement suit under Section 504(a) before the government could make it pay the forfeiture, but it waived that

[5] Available at https://www.sec.gov/Archives/edgar/data/732712/000073271224000010/vz-20231231.htm.

opportunity by electing to pay the penalty and seeking direct review in this Court instead. And second, the Seventh Amendment provides no jury trial right for claims that, like those here, involve public rights rather than private rights with a common-law analogue.

A. The Seventh Amendment Is Not Implicated Because Verizon Had (But Chose To Forgo) The Opportunity For A Jury Trial.

Verizon's Seventh Amendment challenge rests on the faulty premise that it was denied the opportunity for a jury trial. That is not so. When the Commission imposes a forfeiture under Section 503(b)(4), after issuing a Notice of Apparent Liability and providing opportunity to respond in writing, the Act directs that the forfeiture penalty "shall be recoverable pursuant to Section 504(a)." 47 U.S.C. § 503(b)(4). And Section 504(a) requires the government to enforce any forfeiture by bringing a civil suit in district court and provides that "any suit for the recovery of a forfeiture imposed * * * shall be a trial de novo." *Id.* § 504(a); *see Order* ¶ 91 (JA78).

Verizon therefore could have declined to pay the forfeiture and pursued the opportunity for a de novo jury trial in district court under Section 504(a), as it eventually concedes (Br. 48–49). "Verizon's claim that a forfeiture order issued under section 503(b) of the Act does not

provide it * * * a trial by jury[] ignores Verizon's statutory right to a trial *de novo* before it can be required to pay the forfeiture." *Order* ¶ 91 (JA78); *accord id.* ¶ 98 (JA81) ("Verizon does, in fact, have the right of a trial *de novo* under Section 504 of the Act here."). Instead, however, Verizon elected to pretermit any Section 504(a) enforcement action—and thereby to forgo its opportunity to seek a jury trial—to instead pursue direct review in this Court. Given that choice, the Seventh Amendment injury Verizon asserts—its lack of a jury trial—is entirely self-inflicted.[6]

Verizon complains (Br. 51) that it might have to wait up to five years for the government to bring an enforcement action, and that it might experience "reputational harm" or other difficulties in the meantime. It is not evident what that has to do with the Seventh

---

[6] Verizon thus misreads (Br. 44) Justice Sotomayor's dissent in *SEC v. Jarkesy*, 603 U.S. 109 (2024). Justice Sotomayor warned that the Court's decision might jeopardize FCC forfeitures assessed through a formal adjudication under Section 503(b)(3), which provides for direct appellate review of the agency's findings without a trial. *See id.* at 200 (Sotomayor, J., dissenting). But the forfeiture here was instead assessed under Section 503(b)(4), which requires the government to pursue any forfeiture penalty through a Section 504(a) enforcement proceeding, which in turn provides for a "trial de novo" before the government can recover the penalty. 47 U.S.C. §§ 503(b)(4), 504(a); *cf. Jarkesy*, 603 U.S at 200 (Sotomayor, J., dissenting) (observing that *Jarkesy*'s impact on agencies that "can pursue civil penalties in both administrative proceedings and federal court" is more limited).

Amendment, which requires a jury trial only upon an effort to collect payment of monetary damages; if the government has not yet sought to compel payment, there is no Seventh Amendment injury, and claims of reputational harm or other injury apart from monetary damages do not trigger the Seventh Amendment. Indeed, absent any monetary penalty, reputational harm alone generally does not give rise to a constitutional injury. *See Paul v. Davis*, 424 U.S. 693, 701, 711 (1976); *Rudow v. City of New York*, 822 F.2d 324, 330 (2d Cir. 1987).[7]

Any reputational harm, moreover, stems from the underlying facts showing that Verizon allowed improper access to customers' location data without their consent—facts that are essentially undisputed[8]—not from

---

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

[8] Insofar as the material facts here are undisputed, and the government may therefore be entitled to summary judgment, it is not evident that Verizon would actually be entitled to a jury trial in this case. *See Ex parte Peterson*, 253 U.S. 300, 310 (1920) ("No one is entitled in a civil case to trial by jury, unless and except so far as there are issues of fact to be determined."); *Parklane Hosiery Co. v. Shore*, 439 U.S. 322, 336 (1979) (summary judgment does not violate the Seventh Amendment); *United States v. Peninsula Commc'ns, Inc.*, 335 F. Supp. 2d 1013, 1016–17 (D. Alaska 2004) (holding that summary judgment was (cont'd)

the Commission's decision to impose a forfeiture penalty or from any delay in enforcing that penalty. In any event, that Verizon might need to wait for the government to bring a Section 504(a) enforcement suit "in no way renders [it] an inadequate forum" for Verizon to seek a jury trial, and the D.C. Circuit has suggested that Verizon could pursue a declaratory action if it were "suffering from demonstrably adverse consequences from government delay in initiating the collection proceeding." *Pleasant Broad. Co. v. FCC*, 564 F.2d 496, 502 (D.C. Cir. 1977). And if the government declined to pursue recovery of the forfeiture penalty within the five-year statute of limitations, *see* 28 U.S.C. § 2462, Verizon would be under no obligation to pay and would suffer no Seventh Amendment injury.

Verizon also contends (Br. 49–50) that the trial de novo provided by Section 504(a) is "not the kind of jury trial that * * * the Seventh Amendment requires" because some other courts have supposedly held that the defendant would not be allowed to challenge the FCC's legal

---

appropriate in a Section 504(a) enforcement action). Any purported Seventh Amendment violation would thus be harmless error. *See* 5 U.S.C. § 706 (directing that "due account shall be taken of the rule of prejudicial error"); *Overwell Harvest, Ltd. v. Trading Techs. Int'l, Inc.*, 114 F.4th 852 (7th Cir. 2024) (holding Seventh Amendment error harmless after *Jarkesy*).

interpretations. Again, it is unclear what this has to do with the Seventh Amendment, because the Seventh Amendment provides the right to have a jury resolve only questions of fact—not legal questions. *See*, *e.g.*, *Balt. & Carolina Line, Inc. v. Redman*, 295 U.S. 654, 657 (1935) (the Seventh Amendment "retain[s] the common-law distinction * * * whereby * * * issues of law are to be resolved by the court and issues of fact are to be determined by the jury"); *cf.* Pet'r Br. 50 (maintaining that "the key flaws in the Forfeiture Order are legal," not factual). Verizon is wrong to suggest (Br. 49–50) that any hypothetical disagreement over jury instructions would amount to a Seventh Amendment violation; this Court has upheld verdicts despite supposed errors in the jury instructions.[9] If the jury returns a verdict despite an alleged error in the instructions, that does not deprive a defendant of a jury trial; instead it is a routine claim of legal error to be raised on appeal, subject to the ordinary substantive and procedural rules governing appellate review.

Moreover, Verizon's speculation that it might not be able to pursue legal challenges to the forfeiture order in a Section 504(a) enforcement

---

[9] *See*, *e.g.*, *Terminate Control Corp. v. Horowitz*, 28 F.3d 1335, 1343–46 (2d Cir. 1994); *Galdieri-Ambrosini v. Nat'l Realty & Dev. Corp.*, 136 F.3d 276, 285–86 (2d Cir. 1998).

suit may not hold. Verizon admits (Br. 49 n.19) that this Court has never adopted such a limitation. And none of the out-of-circuit cases it cites are on point. *United States v. Dunifer*, 219 F.3d 1004 (9th Cir. 2000), was an action seeking to enjoin unlicensed radio transmissions in violation of 47 U.S.C. § 301, not an action to enforce a monetary forfeiture under Section 504(a). Similarly, *United States v. Any & All Radio Station Transmission Equipment*, 207 F.3d 458 (8th Cir. 2000), was an action for *in rem* forfeiture of radio equipment under 47 U.S.C. § 510, not an action to enforce a forfeiture under Section 504(a). And *United States v. Stevens*, 691 F.3d 620 (5th Cir. 2012), held that the defendants there, who raised *only* legal challenges and did not identify any factual disputes, could and therefore should have raised those challenges by seeking direct review of the forfeiture order under Section 402(a) rather than wait to raise them in district court. *Stevens* thus would not necessarily apply when the subject of the forfeiture plausibly raises *factual* issues, in addition to legal challenges, of a kind that could not adequately be decided by a court alone on direct review under Section 402(a). *Cf. PDR Network, LLC v. Carlton & Harris Chiropractic, Inc.*, 588 U.S. 1, 7–8 (2019) (citing 5 U.S.C. § 703).

In all events, if Verizon believed that it was improperly limited from raising any legal defenses in a Section 504(a) enforcement action, it should have instead raised that challenge in the district court hearing that action and sought to have the limitation set aside there. If Verizon were right that the enforcement action unlawfully restricted its ability to bring legal challenges, the proper remedy would be merely to eliminate that unlawful restriction, not to invalidate the underlying forfeiture order or to strike down the FCC's forfeiture authority entirely.

B. The Seventh Amendment Is Not Implicated Because This Case Involves Public Rights, Not Private Rights With A Common Law Analogue.

Because the Seventh Amendment simply "preserve[s]" the right to jury trial that applied "[i]n Suits at common law," U.S. Const. Amend. VII, it is not implicated by Section 222, which has no common-law analogue for which defendants were historically entitled to a jury trial. Section 222 is instead an aspect of the public franchise conferred by the government upon licensees of public spectrum and entities engaged in common carriage, and therefore falls within the longstanding public-rights exception.

1. The Supreme Court has construed the Seventh Amendment to ensure the right to jury trial for claims that are "legal in nature" and which bear a "close relationship" to a "common law 'ancestor.'" *SEC v. Jarkesy*, 603 U.S. 109, 122–26 (2024). "To determine whether a suit is legal in nature," courts must "consider the cause of action and the remedy it provides." *Id.* at 122–23.

Section 222 does not implicate the Seventh Amendment because it does not bear a "close relationship" to any common law cause of action. In Section 222(c)(1), Congress crafted a new and reticulated regulatory scheme, unlike any known at common law, restricting how telecommunications carriers "use, disclose, or permit access" to "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service." 47 U.S.C. § 222(c)(1) & (h)(1)(A). This provision does not prescribe or proscribe "the same basic conduct" as any common law claim, nor does it borrow "common law terms of art" or "incorporate[] prohibitions from common law" into the Communications Act. *Cf. Jarkesy*, 603 U.S. at 125. On the contrary, Section 222(c)(1) prescribes new obligations concerning a novel subject matter for a limited set of highly regulated entities. It is not "made of the stuff of the traditional

actions at common law tried by the courts at Westminster in 1789." *Id.* at 128 (internal quotation marks omitted).

Verizon's efforts to analogize Section 222 to various common-law torts (Br. 45–47) miss the mark. Section 222 is not a "common-law negligence claim" (Br. 46). A common-law tort claim requires duty, breach, causation, and damages. *E.g.*, *Integrated Waste Servs., Inc. v. Akzo Nobel Salt, Inc.*, 113 F.3d 296, 299 (2d Cir. 1997). Section 222 is very different:

- Verizon identifies no common-law duty to protect the category of technical network information covered by Section 222(c)(1)—that is, "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service," 47 U.S.C. § 222(h)(1)(A). The technical information in this case happens to be location data, which Verizon suggests might possibly be covered by an invasion-of-privacy or intrusion-upon-seclusion claim (Br. 46), but the potential for overlap in some particular instances hardly makes these different kinds of duties close analogues. (And, as noted below, those intentional privacy torts are fundamentally different from negligence claims.)

- Unlike a tort claim, Section 222 requires no showing of damages or causation. The Communications Act requires carriers to implement measures to protect CPNI and makes carriers liable for a failure to do so even if there is no known misappropriation of customer information before the failures are corrected. *Cf.* *Order* ¶¶ 49, 73–74 (JA65, 72–73) (Verizon's failure to take sufficient measures to protect CPNI does not require evidence that unauthorized disclosures occurred).
- Even as to the breach element, the statutory requirements that carriers "protect the confidentiality of proprietary information of" their "customers," 47 U.S.C. § 222(a), and "only use, disclose, or permit access to individually identifiable customer proprietary network information" as authorized or required by law or with the approval of the customer, *id.* § 222(c)(1), do not contain any negligence standard. That the Commission's implementing regulations require carriers to implement "reasonable measures" to protect CPNI, 47 C.F.R. § 64.2010(a), without imposing strict liability, does not transform Section 222 into a traditional negligence provision.

Given that Section 222's requirements differ markedly from the elements of a common-law tort claim in nearly every material respect, Section 222 does not evince an "enduring link" to a "common law 'ancestor'" covered by Seventh Amendment jury-trial right. *Jarkesy*, 603 U.S. at 125.

Nor is Section 222 like "common-law claims * * * for tortious invasion of privacy," such as "intrusion upon seclusion" or "'public disclosure of private facts'" (Br. 46). Those are *intentional* torts. *See* Restatement (Second) of Torts § 625A (intrusion upon seclusion applies when one "intentionally intrudes"); *id.* § 625D cmt.a (public disclosure of private facts is "confined to the giving of publicity" and does not cover "a simple disclosure"). And they apply only to disclosures of information that "would be highly offensive to a reasonable person." *Id.* §§ 625A, 625D. By contrast, Section 222 and the Commission's implementing rules are violated whenever a telecommunications carrier fails to take adequate measures to protect customer proprietary network information, even if the carrier does not intentionally disclose the information (and indeed even if no actual disclosure or misappropriation is known to have occurred at all), and applies irrespective of whether anything in the network information is "highly offensive."

Verizon's reliance (Br. 46) on *Salazar v. National Basketball Ass'n*, 118 F.4th 533 (2d Cir. 2024), simply underscores the point. That case involved a private cause of action providing for recovery of actual damages for knowing disclosures (indeed, criminal disclosures) of a narrow category of inherently sensitive personal information. *See* 18 U.S.C. § 2710. This case, by contrast, involves government enforcement of telecommunication carrier's failure (irrespective of intent) to maintain reasonable safeguards for various forms of technical network information. That these matters in some sense all loosely involve "information" does not indicate the kind of "close relationship between the causes of action in this case and common law" necessary to make the Seventh Amendment applicable. *Jarkesy*, 603 U.S. at 125.

This case is thus a far cry from *Jarkesy*, in which securities-fraud claims adjudicated by the SEC "replicate[d] common law fraud," 603 U.S. at 120, including by "deliberately us[ing] 'fraud' and other common law terms of art" and "incorporat[ing] prohibitions from common law fraud into federal securities law," *id.* at 125. Section 222 "d[oes] not borrow its cause of action from the common law," does not "reiterate common law terms of art," and "bring[s] no common law soil with [it]." *Id.* at 136–37.

Lacking any analogous common-law cause of action, Verizon relies heavily (Br. 44–45) on the punitive nature of forfeiture penalties as a remedy. But even if the remedy is "the 'more important' consideration" when an analogous "cause[] of action sound[s] in both law and equity," *Jarkesy*, 603 U.S. at 123, the mere fact that forfeiture penalties may be punitive does not perforce implicate the Seventh Amendment when there is no analogous common-law cause of action at all.

b. The Seventh Amendment jury-trial right does not apply here because this case involves public rights, not private rights. *Order* ¶ 97 (JA80–81). Under the "public rights" exception, which applies in "distinctive areas involving governmental prerogatives," Congress "may assign [a] matter for decision to an agency without a jury, consistent with the Seventh Amendment." *Jarkesy*, 603 U.S. at 120, 127. These matters "include[] relations with Indian tribes, the administration of public lands, and *the granting of public benefits such as* payments to veterans, pensions, and *patent rights*." *Id.* at 130 (citations omitted; emphasis added).

The forfeiture here arises from Verizon's possession and use of a wireless spectrum license to provide wireless communications service, which requires that it comply with the requirements of the

Communications Act, including Section 222. *See* 47 U.S.C. §§ 301, 307(a), 332(c)(1). The rights and responsibilities associated with spectrum licenses are public rights. A spectrum license grants the holder special rights (typically exclusive rights) to use a specific segment of public spectrum, just as a patent grants the holder special rights to use or commercialize an invention.

A spectrum license "has the key features to fall within * * * the public-rights doctrine," *Oil States Energy Servs., LLC v. Greene's Energy Grp., LLC*, 584 U.S. 325, 335 (2018), for the same reasons a patent does. Patents "fall[] squarely within the public-rights doctrine," the Supreme Court recounted in *Oil States*, because

> the grant of a patent involves a matter "arising between the government and others." * * * [T]he grant of a patent is a matter between "'the public, who are the grantors, and * * * the patentee.'" By "issuing * * * patents," the [government] "take[s] from the public rights of immense value and bestow[s] them upon the patentee." Specifically, patents are "public franchises" that the Government grants "to the inventors of new and useful improvements." The franchise gives the patent owner "the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States." That right "did not exist at common law." Rather, it is a "creature of statute law."

Ibid. (citations omitted). Like patents, spectrum licenses are "a public franchise" granted by the government to the licensee, *id.* at 334, subject

to specific conditions (including, as relevant here, the requirement to protect customers' CPNI). The spectrum rights granted by that franchise belong to the public, who are the grantors. *Id.* at 334–35; *see* 47 U.S.C. § 301 (spectrum licenses "provide for the use of such channels, but not the ownership thereof," which belongs to the public); *In re NextWave Pers. Commc'ns, Inc.*, 200 F.3d 43, 50–51 (2d. Cir. 1999). These spectrum rights "did not exist at common law," but "[r]ather [are] a 'creature of statute law.'" *Oil States*, 584 U.S. at 335 (citations and internal quotation marks omitted). And, like patents, spectrum licenses have historically been assigned through administrative proceedings (though today commercial licenses are often awarded via auction). *NextWave*, 200 F.3d at 51.

Because the forfeiture order seeks to enforce a condition closely intertwined with the granting of a public franchise—a wireless spectrum license—the order here concerns public rights, not a private right with a common-law analogue, and therefore falls outside the Seventh Amendment jury-trial right.

c. More generally, regulation of common carriers—including telephone carriers like Verizon—is a matter of public rights because it falls in the "historic categories of adjudications," *Jarkesy*, 603 U.S. at 130,

that "'have been determined exclusively by [the executive and legislative] branches,'" *id.* at 128. "Common carriers exercise a sort of public office, and have duties to perform in which the public is interested." *Munn v. Illinois*, 94 U.S. 113, 130 (1877) (citing *N.J. Steam Nav. Co. v. Merchs.' Bank of Bos.*, 47 U.S. (6 How.) 344, 382 (1848)). "Their business is, therefore, 'affected with a public interest,'" and "when private property is devoted to a public use, it is subject to public regulation." *Ibid.*

This understanding of common-carrier regulation as implicating public rights, rather than private rights, long predates the Founding. As the Supreme Court explained in *Munn*, "when private property is 'affected with a public interest, it ceases to be *juris privati* [literally, of private right] only.'" *Id.* at 126 (quoting Matthew Hale, *De Portibus Maris*, in *A Collection of Tracts Relative To the Law of England* 77–78 (Francis Hargrave ed., 1787)). This concept traces at least as far back as Lord Chief Justice Hale's legal treatises in the 17th Century, "and has been accepted without objection as an essential element in the law of property ever since." *Ibid.*; *see also NetChoice, L.L.C. v. Paxton*, 49 F.4th 439, 469–73 (5th Cir. 2022) (discussing history of common carriage), *vacated and remanded*, 603 U.S. 707 (2024).

A straight line runs through the long-settled understanding of common-carriage regulation as implicating public rights (not private rights) and the regulation of telecommunication service providers under the Communications Act. In *Crowell v. Benson*, 285 U.S. 22 (1932)—one of the seminal public-rights decisions cited in *Jarkesy*, 603 U.S. at 130—the Supreme Court listed among the "[f]amiliar illustrations of administrative agencies created for the determination of [public rights]" agencies that "exercise * * * the congressional power as to interstate and foreign commerce," including the Interstate Commerce Commission's oversight of railroad carriers and the Postmaster General's regulation of mail facilities. *Id.* at 51 & n.13 (citing *Virginian Ry. Co. v. United States*, 272 U.S. 658 (1926); *Bates & Guild Co. v. Payne*, 194 U.S. 106 (1904)). The Communications Act and the powers given to the Commission to oversee interstate telecommunications grew directly out of these agencies and their regulation of common carriage. *See Scripps-Howard Radio v. FCC*, 316 U.S. 4, 6–7 (1942) (explaining that the Communications Act combined the Interstate Commerce Commission's "general regulatory authority over telephone and telegraph carriers" and the Postmaster General's authority "to fix rates on government telegrams").

Just as "the political branches ha[ve] traditionally held exclusive power over" categories including "the granting of public benefits such as * * * patent rights," *Jarkesy*, 603 U.S. at 130, so too the political branches hold exclusive power over the wireless spectrum used by telecommunications carriers like Verizon and the public franchises that these carriers have been granted. For these reasons, "Congress [could] assign the matter for decision to an agency without a jury, consistent with the Seventh Amendment," *id.* at 127, even if Verizon did not separately have the opportunity to pursue a jury trial under Section 504(a).

CONCLUSION

The petition for review should be denied.

Dated: January 17, 2025

Respectfully submitted,

/s/ *Scott M. Noveck*

P. Michele Ellison
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

Scott M. Noveck
Counsel

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

Counsel for Respondent Federal Communications Commission

Doha G. Mekki
Acting Assistant Attorney General

Robert B. Nicholson
Matthew A. Waring
Attorneys

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

Counsel for Respondent United States of America

CERTIFICATE OF COMPLIANCE

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

1. This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B) and 2d Cir. Rule 32.1(a)(4)(A) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f):

   ☒ this document contains 13,379 words, *or*

   ☐ this document uses a monospaced typeface and contains ____ lines of text.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   ☒ this document has been prepared in a proportionally spaced typeface using Microsoft Word for Office 365 in 14-point Century Schoolbook, *or*

   ☐ this document has been prepared in a monospaced spaced typeface using _____ with _____.

/s/ Scott M. Noveck
Scott M. Noveck
Counsel for Respondents

STATUTORY ADDENDUM

STATUTORY ADDENDUM CONTENTS

Page

Section 217 of the Communications Act, 47 U.S.C. § 217, provides:

> **Sec. 217 [47 U.S.C. § 217]. Liability of carrier for acts and omissions of agents.**
>
> In construing and enforcing the provisions of [this Act], 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.

Section 222 of the Communications Act, 47 U.S.C. § 222, provides in pertinent part:

> **Sec. 222 [47 U.S.C. § 222]. Privacy of customer information.**
>
> (a) **In General.**—Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.
>
> * * *
>
> (c) **Confidentiality of Customer Proprietary Network Information.**—
>
> (1) **Privacy requirements for telecommunications carriers.**—Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.
>
> * * *

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

* * *

(4) to provide call location information concerning the user of a commercial mobile service * * * —

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

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

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

* * *

(f) **Authority to Use Location Information.**—For purposes of subsection (c)(1), without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

(1) call location information concerning the user of a commercial mobile service * * * other than in accordance with subsection (d)(4); or

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

* * *

(h) **Definitions.**—As used in this section:

(1) **Customer proprietary network information.**—The term "customer proprietary network information" means—

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

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

except that such term does not include subscriber list information.

* * *

Section 503 of the Communications Act, 47 U.S.C. § 503, provides in pertinent part:

Sec. 503 [47 U.S.C. § 503]. Forfeitures.

* * *

(b)(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 Act] or of any rule, regulation, or order issued by the Commission under [this Act] 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 Act]; 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. * * *

(2) * * * (B) If the violator is a common carrier subject to the provisions of [this Act] or an applicant for any common carrier license, permit, certificate, or other instrument of authorization issued by the Commission, the amount of any forfeiture penalty determined under this 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.

* * *

(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.

* * *

(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 Act].

* * *

Section 504 of the Communications Act, 47 U.S.C. § 504, provides in pertinent part:

Sec. 504 [47 U.S.C. § 504]. Provisions Relating to Forfeitures.

(a) The forfeitures provided for in [this Act] 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 Act], 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 Act] 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 Act]. 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 Act]. The costs and expenses of such prosecutions shall be paid from the appropriation for the expenses of the courts of the United States.

* * *

47 C.F.R. § 1.80 provides in pertinent part:

§ 1.80 Forfeiture Proceedings.

* * *

(b) *Limits on the amount of forfeiture assessed—*

* * *

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

* * *

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

Upward Adjustment Criteria:

(1) Egregious misconduct.

(2) Ability to pay/relative disincentive.

(3) Intentional violation.

(4) Substantial harm.

(5) Prior violations of any FCC requirements.

(6) Substantial economic gain.

(7) Repeated or continuous violation.

Downward Adjustment Criteria:

(1) Minor violation.

(2) Good faith or voluntary disclosure.

(3) History of overall compliance.

(4) Inability to pay.

NOTE 2 TO PARAGRAPH (b)(11): *Guidelines for Assessing Forfeitures.* The Commission and its staff may use the guidelines in tables 1 through 4 of this paragraph (b)(11) in particular cases. The Commission and its staff retain the discretion to issue a higher or lower forfeiture than provided in the guidelines, to issue no forfeiture at all, or to apply alternative or additional sanctions as permitted by the statute. The forfeiture ceilings per violation or per day for a continuing violation stated in section 503 of the Communications Act and the Commission's rules are described in paragraph (b)(12) of this section. These statutory maxima became effective September 13, 2013. Forfeitures issued under other sections of the Act are dealt with separately in table 4 to this paragraph (b)(11).

* * *

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

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

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

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

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

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

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

(2) *Delivery*. The notice of apparent liability will be sent to the respondent, by certified mail, at his last known address (see § 1.5).

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

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

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

* * *

47 C.F.R. § 64.2001 provides in pertinent part:

§ 64.2001 Basis and purpose.

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

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

47 C.F.R. § 64.2003 provides in pertinent part:

§ 64.2003 Definitions.

* * *

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

* * *

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

* * *

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

* * *

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

* * *

47 C.F.R. § 64.2007 provides in pertinent part:

> **§ 64.2007 Approval required for use of customer proprietary network information.**
>
> * * *
>
> (b) *Use of opt-out and opt-in approval processes.* A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under § 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

47 C.F.R. § 64.2008 provides in pertinent part:

> **§ 64.2008 Notice required for use of customer proprietary network information.**
>
> * * *
>
> (b) Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.
>
> (c) *Content of notice.* Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI.

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

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

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, carriers may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

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

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

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

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

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

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

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

* * *

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

* * *

47 C.F.R. § 64.2010 provides in pertinent part:

§ 64.2010 Notice required for use of customer proprietary network information.

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

* * *