24-1733

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

VERIZON COMMUNICATIONS INC.,

Petitioner,

v.

UNITED STATES FEDERAL COMMUNICATIONS COMMISSION;
UNITED STATES OF AMERICA,

Respondents.

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

BRIEF FOR PETITIONER VERIZON COMMUNICATIONS INC.
****PUBLIC REDACTED****

Scott H. Angstreich
Aaseesh P. Polavarapu
KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900
sangstreich@kellogghansen.com
apolavarapu@kellogghansen.com

Counsel for Petitioner Verizon Communications Inc.

November 4, 2024

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, petitioner Verizon Communications Inc. submits the following corporate disclosure statement:

Verizon Communications Inc. is a publicly traded company. Verizon Communications Inc. has no parent company. No publicly held company owns 10 percent or more of Verizon Communications Inc.'s stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

CONSTITUTION, STATUTES, AND REGULATIONS

LEGISLATIVE MATERIALS

ADMINISTRATIVE MATERIALS

OTHER MATERIALS

PRELIMINARY STATEMENT

Today, smartphones are ubiquitous, and apps on those devices allow users to share their precise location with friends and family, rideshare and tow-truck drivers, and emergency responders. But before that was true, wireless customers still sometimes needed to let others know their location. Wireless carriers like Verizon operated location-based service ("LBS") programs to respond to that customer demand. Verizon's LBS program was in place for roughly a decade. The program completed hundreds of millions of successful, express requests from consumers to provide location information to service providers.

Those service providers (including companies like Life Alert and AAA), after applying and completing a careful vetting process, could obtain a Verizon customer's explicit consent to disclose the rough location — based on cell-tower triangulation — of the customer's cellphone, tablet, or other wireless-enabled device. In addition to vetting service providers, Verizon contractually limited those providers' ability to request device-location information only to specifically approved uses. Verizon retained a third-party auditor to monitor the service providers' compliance, including reviewing the records of the explicit consent that providers had to obtain from customers before requesting their device location.

Despite those and other robust protections, Verizon learned through *New York Times* reporting in May 2018 (though the Federal Communications

Commission ("FCC") had learned about it in 2017) that one participating service provider, Securus, misused many carriers' LBS programs and that a sheriff in Missouri took advantage of Securus's actions to track wireless carriers' customers without their consent. The record here, however, shows that the sheriff successfully obtained device-location information for only 11 Verizon customers, with those successful requests occurring [redacted]. The record contains no evidence of any other participating service provider making an unauthorized or unconsented request for a Verizon customer's device location at any point in time.

Immediately after the *New York Times* story, Verizon terminated Securus from the LBS program and launched an investigation. Verizon was the first major wireless provider to announce that it had decided to shut down its LBS program entirely, making that decision within 30 days of the article's publication. By November 2018, Verizon had largely terminated its LBS program, phasing it out thoughtfully so Verizon customers who relied on these location-based services could make other plans. As the only exception, Verizon allowed certain roadside service providers to continue in the LBS program through March 2019 so Verizon customers who relied on these services for roadside assistance were not left stranded during the holiday travel season and winter months. As Verizon wound

down the program to its eventual end, Verizon also implemented additional safeguards to protect its customers' data.

More than five years later, in April 2024, the FCC issued a Forfeiture Order. The FCC affirmed its February 2020 Notice of Apparent Liability ("NAL"), held Verizon liable for violating the agency's rules governing the protection of customer proprietary network information ("CPNI"), and imposed a penalty of nearly $47 million, which it ordered Verizon to pay within 30 days.

The FCC, however, did not punish Verizon for Securus's or the sheriff's actions — which were the only unauthorized requests for or misuse of customer device information by any service provider participating in Verizon's LBS program. The FCC acknowledged that those actions occurred outside the statute of limitations, so they could not support a forfeiture penalty. And, by the time of the NAL, Verizon had shut down its LBS program nearly one year earlier, eliminating any potential current or going-forward liability. The FCC, therefore, adopted a novel approach to generate an eye-popping penalty amount. The FCC punished Verizon for not terminating *every other* service provider from the LBS program on a faster timeline. Specifically, the FCC imposed a forfeiture penalty for each day — starting 30 days after the *New York Times* article — that each of the 63 service providers remained able to use the LBS program, despite not being involved in any wrongdoing (and despite customers' continuing need for services from those

providers, including for roadside assistance). The FCC treated each of those 63 service providers as a separate violation, blowing past the inflation-adjusted statutory limit ($2,048,915) on forfeitures for "any single act or failure to act." 47 U.S.C. § 503(b)(2)(B).

Verizon's petition for review stems from the multiple and significant errors that the FCC, in purporting to enforce statutory consumer data privacy provisions, made in overstepping its authority. The FCC's Forfeiture Order violated both the Communications Act and the Constitution, while failing to benefit the consumers it purported to protect.

First, the FCC found that Verizon's LBS program did not reasonably protect CPNI. But the device-location information the LBS program disclosed is *not* CPNI. Verizon did not obtain it "solely by virtue of" its common-carrier (voice service) relationship with its customers. *Id.* § 222(h)(1)(A). Verizon obtained that information because a device was turned on and Verizon's network could find it (roughly), regardless of whether the customer was using, or had purchased, a common-carrier (voice) service. In addition, the only location information that qualifies as CPNI by statute is call-location information; the device-location information used in the LBS program is not CPNI.

Second, the FCC erred in treating the lone LBS program breach by a participating service provider as dispositive evidence that Verizon had failed to

"take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a). In doing so, the FCC treated Securus's actions and the sheriff's exploitation of them as conclusive evidence that Verizon's program safeguards were insufficient. But, as the FCC itself has recognized, bad actors can circumvent even the best safeguards. When viewed against the backdrop of a multi-year program with scores of other service providers and hundreds of millions of device-location requests, Verizon's and its third-party auditor's failure to identify the 11 customers subjected to unauthorized requests hardly shows the existence of a "significant loophole" in Verizon's procedures. Forfeiture Order ¶ 48 (JA64). If anything, the relatively small number of unauthorized requests shows that the program safeguards were effective and reasonable. In concluding otherwise, the FCC effectively (and improperly) imposed a strict liability standard and did so without providing fair notice.

Third, the FCC's nearly $47 million forfeiture violates the inflation-adjusted statutory maximum of approximately $2 million for "any single act or failure to act." 47 U.S.C. § 503(b)(2)(B). The only violation the FCC identified was with Verizon's LBS program safeguards, which Verizon applied uniformly to all participating providers. That is only one "act or failure to act," not more than 60 as the FCC claimed. The FCC's retort that it could have chosen instead to find tens

of millions of violations — one for each Verizon subscriber — confirms that the agency treats Congress's express limit on its forfeiture authority as meaningless.

Fourth, the FCC's Forfeiture Order violates the Constitution. The Supreme Court's recent decision in *SEC v. Jarkesy*, 144 S. Ct. 2117 (2024), controls here. Just like for Mr. Jarkesy, the Constitution guarantees Verizon a jury trial — not an administrative adjudication — before it faces an order compelling it to pay a forfeiture. That the Forfeiture Order imposes a punitive monetary penalty is "all but dispositive" of the constitutional violation, *id.* at 2129, though the "close relationship" to common-law actions confirms that the order does not address a public right, *id.* at 2130. And Verizon's "option" of violating the FCC's order by not paying, waiting up to five years for the Department of Justice to initiate a collection proceeding, and then potentially getting a jury at the risk of waiving its legal challenges does not cure the constitutional problem *Jarkesy* identifies. The Forfeiture Order is no mere complaint alleging violations and initiating a federal court proceeding; it is an adjudication of liability and order to pay money, which has harmful collateral consequences even while the forfeiture remains unpaid.

The agency ignored the limits of its authority in these multiple ways, in an effort to show force against a large company that did nothing wrong. The Court should vacate the Forfeiture Order.

JURISDICTIONAL STATEMENT

The FCC imposed a forfeiture on Verizon in the amount of $46,901,250, which Verizon paid under protest on May 22, 2024. This Court therefore has jurisdiction pursuant to 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1). *See ABC, Inc. v. FCC*, 404 F. App'x 530, 534 (2d Cir. 2011) (summary order); *AT&T Corp. v. FCC*, 323 F.3d 1081, 1083-85 (D.C. Cir. 2003). Verizon timely filed the petition for review within 60 days of the entry of the Forfeiture Order. *See* 28 U.S.C. § 2344.

Verizon has its principal office in this judicial circuit. Venue is therefore proper in this Court under 28 U.S.C. § 2343.

ISSUES PRESENTED

1. Whether the FCC erroneously concluded that device-location information is CPNI under 47 U.S.C. § 222(h)(1).

2. Whether the FCC's conclusion that Verizon acted unreasonably to protect customers' device-location information was arbitrary, capricious, or otherwise contrary to law.

3. Whether the FCC violated 47 U.S.C. § 503(b)(2)(B)'s maximum forfeiture, or otherwise acted arbitrarily and capriciously, by treating each service provider subject to Verizon's uniform LBS program policies that remained in the program more than 30 days after the *New York Times* article as a separate act or failure to act.

4. Whether the Forfeiture Order violates the Seventh Amendment to the Constitution.

STATEMENT OF THE CASE

A. Section 222 of the Communications Act Only Covers a Specific, Limited Category of Information

In the Communications Act, Congress divided communications services into two broad categories: common-carrier services and private-carrier services. Congress imposed certain privacy-related duties on providers of common-carrier services — also known as telecommunications carriers — in 47 U.S.C. § 222.[1] Wireless voice services are common-carrier services. *See* 47 U.S.C. § 332(c)(1)(A); Forfeiture Order ¶ 2 n.7 (JA46). But wireless data services — both text messaging and internet access — are not common-carrier services. Instead, both are regulated as non-common-carrier information services and private mobile services.[2] Both types of wireless data services are thus immune from common-

[1] *See* 47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty . . . ."); *id.* § 222(c)(1) ("Except as required by law or with the approval of the customer, a telecommunications carrier . . . shall . . . .").

[2] Declaratory Ruling, *Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service*, 33 FCC Rcd 12075 (2018) (text messaging); Declaratory Ruling, Report and Order, and Order, *Restoring Internet Freedom*, 33 FCC Rcd 311 (2018) (broadband internet access). In 2024, the FCC issued an order that would treat broadband internet access as a common-carrier service. Declaratory Ruling, Order, Report and Order, and Order on Reconsideration, *Safeguarding and Securing the Open Internet*, WC Docket Nos. 23-320 & 17-108, FCC 24-52 (rel. May 7, 2024) ("*Open Internet Order*"). But on August 1, 2024, the Sixth Circuit stayed that order pending judicial review. *See In re MCP No. 185*, 2024 WL 3650468, at *1 (6th Cir. Aug. 1, 2024) (per curiam). Even if the FCC's order takes effect, that order would apply prospectively and would not impact the outcome here.

carrier regulation, including under § 222. *See* 47 U.S.C. §§ 153(51), 332(c)(2); *Cellco P'ship v. FCC*, 700 F.3d 534, 538 (D.C. Cir. 2012) ("[M]obile-data providers are statutorily immune, perhaps twice over, from treatment as common carriers.").[3] More than [redacted] of the traffic on Verizon's network is associated with data services. *See* Altland Decl. ¶ 2 (JA166).

Section 222 restricts common carriers (here, wireless voice providers) from using, disclosing, or permitting access to CPNI without customer consent. 47 U.S.C. § 222(c)(1).[4] As originally enacted in 1996, Congress defined CPNI as

> information that relates to the quantity, technical configuration, type, destination, 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(f)(1)(A) (1996). That definition does not mention location.

Three years later, Congress enacted the Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286. Among other things, Congress amended § 222 to allow common carriers, despite § 222(c)(1), to

---

[3] The Federal Trade Commission has authority to act against non-common-carrier communications providers that engage in unfair or deceptive practices, including related to consumer privacy. *See FTC v. AT&T Mobility LLC*, 883 F.3d 848, 861 (9th Cir. 2018) (en banc).

[4] Section 222 contains exceptions to that consent requirement, which are generally not relevant here. *See* 47 U.S.C. § 222(c)(1) ("Except as required by law . . . ."); *id.* § 222(d)(1)-(3) (authorizing use, disclosure, and permitting access without consent in certain circumstances).

disclose "call location information concerning the user of a commercial mobile service," without that user's consent, to emergency responders and immediate family members during a life-threatening emergency. *Id.* § 5(1) (adding 47 U.S.C. § 222(d)(4)). Congress also defined consent for purposes of § 222(c)(1) to mean "express prior authorization" in the case of "call location information concerning the user of a commercial mobile service" and "automatic crash notification information," if disclosed outside the "operation of an automatic crash notification system." *Id.* § 5(2) (adding 47 U.S.C. § 222(f)). Consistent with those two additions to the statute, Congress also added "location" to the definition of CPNI, now found in § 222(h)(1)(A). *Id.* § 5(3).

The FCC has never adopted a rule defining "location" in § 222(h)(1)(A). In 2002, the FCC expressly declined to initiate a rulemaking to do so. *See* Order, *Request by CTIA to Commence Rulemaking to Establish Fair Location Information Practices*, 17 FCC Rcd 14832, ¶ 5 n.18 (2002). The FCC, however, has acknowledged as recently as 2024 that the "central underpinnings" of its CPNI rules are "focused on addressing problems in the *voice service* context." *Open Internet Order* ¶ 359 (emphasis added); *see also* Report and Order, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd 13911, ¶ 39 (2016) ("[O]ur existing rules have been focused on voice services.").

In a 2007 order, the FCC extended its CPNI rules to another voice service, Voice over Internet Protocol, or VoIP. *See* Report and Order and Further Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996*, 22 FCC Rcd 6927, ¶¶ 54-59 (2007). As part of that rulemaking, the FCC also addressed "pretexting" — a then-widespread practice of bad actors pretending to be a customer to "obtain access to that customer's call detail or other private communications records." *Id.* ¶ 1 n.1. The FCC adopted a rule requiring telecommunications carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a).

B. The Communications Act's Forfeiture Provisions

Congress has authorized the FCC to enforce the Communications Act and the agency's rules through monetary forfeitures. 47 U.S.C. § 503(b)(1)(B). Congress capped the maximum "forfeiture penalty" at "$100,000 for each violation or each day of a continuing violation," with the total forfeiture for "any continuing violation . . . not [to] exceed a total of $1,000,000 for any single act or failure to act." *Id.* § 503(b)(2)(B). Federal law allows for inflation adjustments of civil penalties; in 2020, the maximum for a § 503(b)(2)(B) forfeiture was $2,048,915. *See* Order, *Amendment of Section 1.80(b) of the Commission's Rules*, 34 FCC Rcd 12824, ¶ 1 (Enf. Bur. 2019).

The FCC may — and nearly always does (as it did here) — itself investigate a potential violation and then issue an NAL. 47 U.S.C. § 503(b)(4). If the subject of the NAL objects in writing, *see id.* § 503(b)(4)(C); 47 C.F.R. § 1.80(g), the FCC then decides whether to affirm its NAL, including the proposed penalty, 47 C.F.R. § 1.80(g)(4).

If the FCC affirms the NAL, its forfeiture order will "stat[e] the date by which the forfeiture must be paid." *Id.* The subject of the forfeiture order may pay that amount and then petition for review. *See ABC*, 404 F. App'x at 534; *AT&T*, 323 F.3d at 1085. Alternatively, "[i]f the forfeiture is not paid," the FCC will refer the matter "to the Department of Justice for collection." 47 C.F.R. § 1.80(g)(5). The Department may bring "a civil suit . . . in any district through which the . . . system of the carrier runs," 47 U.S.C. § 504(a), subject to a five-year statute of limitations, *see* 28 U.S.C. § 2462. While a "suit for the recovery of a forfeiture . . . shall be a trial de novo," 47 U.S.C. § 504(a), some courts of appeals have held that the defendant may challenge only the forfeiture order's factual findings, not its "legal validity." *E.g.*, *United States v. Stevens*, 691 F.3d 620, 622-23 (5th Cir. 2012).

C. Verizon's LBS Program

Until fully shutting it down in March 2019, Verizon operated its LBS program so its customers — after providing affirmative, opt-in consent — could

disclose the approximate location of their wireless device to obtain certain pre-approved beneficial services that they wanted. Letter of Inquiry ("LOI") Resp. at 1-3 (JA96-98); Supp. LOI Resp. at 2 (JA9). For example, Life Alert could use that information to dispatch first responders to customers in urgent need of medical care. LOI Resp. at 1-2, 6 (JA96-97, 101). AAA could use that information to dispatch roadside assistance to customers broken down on the side of the highway. *Id.* at 2, 5 (JA97, 100). Or Capital One could use it to confirm a customer's approximate location to reduce fraud and secure online transactions. *Id.* at 2, 6 (JA97, 101). The FCC has recognized the benefits of these services and that they "may at times be helpful to consumers." NAL ¶ 11 (JA117).

To effectuate its LBS program, Verizon worked directly with two companies, LocationSmart and Zumigo, which also worked with other wireless carriers and thus served as location aggregators. LOI Resp. at 4 (JA99). This enabled service providers to request location information for a customer, after obtaining express consent, from a single entity, without needing to learn the identity of the customer's wireless service provider. Donnellan Decl. ¶ 6 (JA42-43).

Verizon took numerous measures to protect its subscribers' information and to ensure that a service provider obtained affirmative consent to share device-location information before requesting that information. First, Verizon carefully

vetted would-be participants in the LBS program. LOI Resp. at 3 (JA98). Verizon hired a third-party auditor (Aegis) to vet each applicant for legitimacy (e.g., by confirming it had a federal tax ID) and good corporate standing, as well as searching for criminal convictions or civil judgments, including for fraud. *Id.*; Supp. LOI Resp. at 14-15 (JA21-22). Each applicant had to submit (i) a detailed description of its use case; (ii) specific details of how customers would be informed about the use of their location information; (iii) a detailed description of the affirmative, opt-in consent process; and (iv) a full description of the process for customers to opt out. LOI Resp. at 3 (JA98); Supp. LOI Resp. at 14-15 (JA21-22). Both Aegis and Verizon reviewed these submissions. LOI Resp. at 3 (JA98); Supp. LOI Resp. at 14-15 (JA21-22). Not every applicant passed that review. NAL ¶ 61 & n.157 (JA131) (citing VZ-0000295).

Second, even after the initial approval, Verizon directed Aegis to conduct ongoing reviews, as well as regular audits, of each provider to ensure that customers had affirmatively consented to the sharing of their location information and that the participant used the information only as authorized. Supp. LOI Resp. at 14 (JA21); Bruner Supp. Decl. ¶ 4 (JA37). Aegis conducted these reviews at least annually, and more frequently for participants with higher transaction volumes. Bruner Supp. Decl. ¶ 4 (JA37). Aegis looked for significant company changes (such as to ownership), validated and reconciled consent records, and monitored opt-in and

opt-out procedures, including through "secret shoppers." *Id.* ¶¶ 4, 6 (JA37-38). If these reviews turned up issues, the participant would have to correct them or face suspension from Verizon's LBS program. Supp. LOI Resp. at 17-18 (JA24-25).

Third, although Verizon-approved service providers contracted with LocationSmart or Zumigo, Verizon's contracts with those two companies governed the terms of the downstream contracts. *Id.* at 8 (JA15); NAL ¶ 14 (JA118-19). Verizon insisted that contracts with any service provider participating in the LBS program include the requirement to obtain affirmative, opt-in consent from Verizon's customers before requesting their location information, and to provide Verizon's subscribers with clear and conspicuous notice about how their location information would be accessed, used, copied, stored, or disclosed. Supp. LOI Resp. at 8 (JA15); NAL ¶ 14 (JA118-19). Verizon and Aegis reviewed LBS providers' notice-and-consent processes. Supp. LOI Resp. at 9 (JA16). Verizon also mandated that the contracts require the participating service providers to implement and maintain multiple types of security controls, to prevent unauthorized disclosure of Verizon's data, and to comply with consumer protection laws, data privacy laws, and industry best practices, including CTIA's "Best Practices and Guidelines for Location-Based Services." NAL ¶ 15 & n.54 (JA119).

Once in the LBS program, a provider would obtain the subscriber's informed, express, opt-in consent before making a request to LocationSmart or Zumigo for that subscriber's device-location information. LOI Resp. at 4-5 (JA99-100); Donnellan Decl. ¶ 6 (JA42). The provider would include in the request a record of the subscriber's consent. Donnellan Decl. ¶ 6 (JA42-43). LocationSmart or Zumigo, in turn, would request that Verizon use its network to ping the subscriber's device to determine its approximate location. *Id.* For the ping to return location information, the subscriber's device only had to be turned on and connected to the Verizon network. *Id.* ¶¶ 5, 7 (JA42-43).[5] The subscriber did not need to be using the device or to have subscribed to any particular wireless service. *Id.* ¶¶ 5, 9 (JA42-43).

Each day, LocationSmart and Zumigo would send Aegis records of each customer's consent. Bruner Decl. ¶ 3 (JA33). Aegis would then match the requests for location data Verizon had received to a consent record. *Id.* Aegis was able to match 99.95% of all requests to a consent record. *Id.* ¶ 6 (JA34). For the remaining 0.05%, Aegis investigated a statistically significant, randomly selected sample to ensure that consent records existed for those requests as well. *See id.*

[5] The location information was the approximate latitude and longitude of a customer's device, accurate to within 1,000 meters, derived from the location of the Verizon cell sites that pinged the device. *See* LOI Resp. at 4 (JA99).

Every time Aegis did so, it found a consent record for the location request. *See id.* As another check, Aegis compared aggregated transaction records submitted by LBS program participants against Verizon's LBS platform records to verify that the participants had submitted accurate records. Bruner Supp. Decl. ¶ 6 (JA38). Aegis also used fraud analytics techniques to assess whether requests were characteristic of what appeared to be normal operations and to flag potential issues for follow-up investigation. Bruner Decl. ¶ 7 (JA34); Bruner Supp. Decl. ¶¶ 7-8 (JA38). Aegis did not uncover any material issues through this analysis. Bruner Decl. ¶ 7 (JA35); Bruner Supp. Decl. ¶ 8 (JA38).

D. The *New York Times* Article

More than 60 companies participated in Verizon's LBS program. LOI Resp. at 5-6 (JA100-01). One of those companies was Securus, which provides payphone calling services in prisons and jails. Supp. LOI Resp. at 15 (JA22). Verizon approved Securus to join the LBS program for one purpose: as a security measure to confirm that wireless callers were a certain distance away from the prison or jail at the time of the call. LOI Resp. at 11 (JA106); Supp. LOI Resp. at 15 (JA22). Like other participants, Securus entered a contract in which it agreed to

obtain subscribers' affirmative consent and to access location information solely for that approved purpose. Supp. LOI Resp. at 8 (JA15); NAL ¶ 14 (JA118-19).

Securus, however, misused its access to Verizon's LBS program (and other wireless carriers' similar programs). Securus accepted requests from law enforcement to use the LBS programs to identify a suspect's location information, without that person's consent, by uploading a judicial warrant or other legal authorization. Forfeiture Order ¶ 14 (JA51). Securus did not disclose that additional use case to Verizon or Aegis. *Id.* ¶ 13 (JA50-51).[6] And Securus did not actually review the documents law enforcement personnel uploaded. *Id.* That failure by Securus allowed a Missouri sheriff, Cory Hutcheson, to make requests for location information through Securus without any legal authorization. *Id.* ¶ 14 (JA51).

The FCC learned of Securus's and Hutcheson's actions in 2017, while reviewing Securus's application for approval of a change of control. Consumer advocates notified the FCC of the criminal case against Hutcheson, which they explained "involved the use of Securus' Location Based Service to 'ping' the cell phones of five other county employees." Wright Petitioners Ex Parte Letter at 2,

[6] Verizon had well-established procedures for legitimate law enforcement requests for customer location data, which were handled outside the LBS program. *See* LOI Resp. at 10-11 (JA105-06).

WC Docket No. 17-126 (FCC filed Aug. 4, 2017).[7] The advocates noted that a Securus employee had testified at Hutcheson's trial "to explain how Securus' Location Based Service was used to track" certain "individuals who had not provided their 'express prior authorization.'" *Id.* In approving the change of control, the FCC noted the allegations about Securus and Hutcheson, but found they "are better handled in the context of an enforcement proceeding." Memorandum Opinion and Order, *Joint Application to Transfer Indirect Ownership and Control of Licenses*, 32 FCC Rcd 9564, ¶¶ 8, 28 (2017). To Verizon's knowledge, the FCC did not initiate an enforcement proceeding against Securus. And the FCC did not inform Verizon of the allegations.

Instead, Verizon first learned of Hutcheson's actions and Securus's involvement in May 2018, when the *New York Times* reported on them. Supp. LOI Resp. at 15-16 (JA22-23). Verizon subsequently learned, based on records the Department of Justice turned over and on which the FCC relied, *see* NAL ¶ 50 n.134 (JA128), that Hutcheson [redacted], Verizon NAL Resp. at 19-20 & n.16 (JA162-63). Verizon's own data show that requests for only 11 of those

[7] The filing is available at https://www.fcc.gov/ecfs/document/10804689721322/1.

customers were successfully transmitted to Verizon. Bruner Supp. Decl. ¶ 9 (JA39).

E. Verizon Takes Action To Further Safeguard Customer Information

The day after the *New York Times* article, Verizon directed LocationSmart to terminate Securus from the LBS program. Supp. LOI Resp. at 15-16 (JA22-23).

Verizon then undertook a review to better understand how Securus was able to evade the LBS program's many protections. LOI Resp. at 12 (JA107). Verizon concluded that Aegis's regular auditing likely did not reveal Securus's actions because the volume of unauthorized location requests from Securus was so small that the total volume was consistent with the amount Aegis would expect based on Securus's approved use case. *Id.*; Bruner Supp. Decl. ¶ 9 (JA38-39). Verizon also investigated the other service providers, but neither Verizon nor Aegis identified any other service provider that had failed to obtain express customer consent before accessing location information or had obtained location information for a non-approved purpose in the same (or similar) manner as Securus. LOI Resp. at 12-13 (JA107-08); Supp. LOI Resp. at 16-17 (JA23-24); Bruner Decl. ¶ 7 (JA34-35); Bruner Supp. Decl. ¶ 11 (JA39).

Nevertheless, Verizon decided to end the LBS program less than a month after the *New York Times* article and notified LocationSmart and Zumigo of its decision on June 12, 2018. LOI Resp. at 9 (JA104). While Verizon ceased

accepting new applications from service providers to participate in the program, Verizon decided against abruptly terminating its program for current participants. *Id.* at 9-10 (JA104-05); Supp. LOI Resp. at 2 (JA9). Verizon subscribers relied on the LBS program for certain necessary services, and ending the program abruptly would have had endangered those consumers. For example, Verizon did not want to interfere with services like roadside assistance until consumers relying on the LBS program had the opportunity to make alternative arrangements to share their location with service providers. Supp. LOI Resp. at 2 (JA9). Verizon therefore allowed some time for an orderly transition, terminating nearly all service providers' access on November 30, 2018. *Id.* That included all the service providers that contracted with Zumigo or LocationSmart, except for those providing roadside assistance. *Id.* For those remaining participants, Verizon terminated access no later than March 30, 2019. *Id.* However, many participants ceased making requests through the program before their termination date. Bruner Supp. Decl. ¶ 12 (JA39); Verizon NAL Resp. Ex. D (JA167-72).

During the phase-down of the LBS program, Verizon instituted additional program safeguards. Verizon had Aegis strengthen the transaction verification process to identify anomalies in consent requests. LOI Resp. at 10 (JA105). Aegis also examined Securus's transaction history to better inform and refine its data analytics. Bruner Supp. Decl. ¶ 11 (JA39).

F. The FCC Issues a Notice of Apparent Liability

Nearly a year after Verizon completed the shutdown of its LBS program, the FCC issued an NAL against Verizon, concluding that it "apparently" violated § 222 of the Communications Act by failing to protect its customers' location data. NAL ¶ 3 (JA113). The FCC recognized that the one-year statute of limitations had expired as to Hutcheson's and Securus's actions. *See id.* ¶ 89 (JA141). The FCC instead based its proposed penalty of more than $48 million on each day that each of 65 LBS program participants remained in Verizon's LBS program, starting 30 days after publication of the *New York Times* article. *Id.* ¶¶ 87, 93 (JA140, 142). The FCC issued similar NALs against AT&T, T-Mobile, and Sprint.[8]

Verizon responded to the NAL in writing in May 2020.

G. The FCC Issues a Forfeiture Order More than Four Years After the NAL

In April 2024, a divided FCC (by a 3-2 vote) affirmed its NAL and issued the Forfeiture Order. The FCC reduced the proposed forfeiture by approximately $1.4 million — accepting Verizon's evidence that two companies the NAL included in its calculation had never participated in the LBS program — but

[8] *See* Notice of Apparent Liability for Forfeiture and Admonishment, *AT&T Inc.*, 35 FCC Rcd 1743 (2020); Notice of Apparent Liability for Forfeiture and Admonishment, *T-Mobile USA, Inc.*, 35 FCC Rcd 1785 (2020); Notice of Apparent Liability for Forfeiture and Admonishment, *Sprint Corp.*, 35 FCC Rcd 1655 (2020).

otherwise affirmed the NAL in full. Forfeiture Order ¶¶ 85-86 (JA76). The FCC ordered Verizon to pay the $46.9 million penalty in 30 days. *Id.* ¶ 103 (JA83).

The FCC first concluded that device-location data is CPNI, rejecting Verizon's arguments that it did not receive the data "solely" because of its provision of common-carrier services and that device-location information is not CPNI. *See id.* ¶¶ 22-34 (JA53-58). The FCC also concluded that Securus's actions revealed "fundamental shortcomings in Verizon's safeguards" and that Verizon's additional measures after publication of the *New York Times* article did not remedy "those shortcomings." *Id.* ¶¶ 53, 55 (JA66-67). With respect to its decision to calculate one penalty for every other LBS program participant, the FCC described the approach as "eminently *conservative*," claiming that it could instead "have chosen to look to the total number of Verizon subscribers" — "tens of millions" — "when determining the number of violations." *Id.* ¶ 80 (JA74). The FCC also defended the constitutionality of its forfeiture authority, arguing that the Fifth Circuit had wrongly decided *Jarkesy*, that this forfeiture proceeding involves a "public right" exempt from the Seventh Amendment jury-trial right, and that Verizon has a statutory right to a de novo jury trial in federal district court under 47 U.S.C. § 504(a). *See id.* ¶¶ 97-98 (JA80-82).

Commissioners Carr and Simington dissented. Commissioner Carr argued that § 222 does not cover device-location data, which Verizon "could gather . . .

even if the customer did not have a voice plan." Forfeiture Order at 44 (JA88). Commissioner Simington disputed the majority's view "that a single, systemic failure to follow the Commission's rules . . . may constitute however many separate and continuing violations the Commission chooses to find." *Id.* at 46 (JA90). To the contrary, "[i]t is simply not plausible that Congress intended that the Commission . . . arrive at forfeitures of any size" by choosing "whatever" inputs it wants "to arrive at whatever forfeiture amount suits a preordained outcome." *Id.*[9]

SUMMARY OF ARGUMENT

This Court should grant Verizon's petition for review and vacate the Forfeiture Order.

I. Verizon's LBS program used device-location information, and device-location information is not CPNI. First, information is CPNI only if it "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). But Verizon can obtain

[9] On the same day, the FCC also issued three more forfeiture orders, against AT&T, T-Mobile, and Sprint. *See* Forfeiture Order, *AT&T Inc.*, FCC 24-40 (rel. Apr. 29, 2024); Forfeiture Order, *T-Mobile USA, Inc.*, FCC 24-43 (rel. Apr. 29, 2024); Forfeiture Order, *Sprint Corp.*, FCC 24-42 (rel. Apr. 29, 2024). AT&T petitioned for review in the Fifth Circuit. *See AT&T Inc. v. FCC*, No. 24-60223 (5th Cir. filed May 9, 2024). T-Mobile, which had since acquired Sprint, petitioned for review of both orders in the D.C. Circuit. *See Sprint Corp. v. FCC*, Nos. 24-1224 & 24-1225 (D.C. Cir. filed June 27, 2024).

device-location data whenever it provides any wireless service to customers, including from customers who purchase no common-carrier services at all. Second, "location" in the CPNI definition means call-location information, not device-location information.

II. The FCC's finding that Verizon did not "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI," 47 C.F.R. § 64.2010(a), is arbitrary and capricious. The FCC was aware of Securus's unauthorized use of the LBS program — and Hutcheson's misuse of Securus's access — long before Verizon, yet never informed Verizon or initiated an enforcement action against Securus. And Verizon's failure to discover unauthorized requests for 11 customers, occurring at two discrete times spread over many years well outside the statute of limitations, is not evidence that Verizon's multi-layered protections were unreasonable. The FCC's conclusion otherwise effectively applies a strict liability standard that cannot be squared with the agency's rules and for which the FCC provided no fair notice.

III. The $46.9 million forfeiture penalty exceeds the statutory limit on the agency's forfeiture authority. The FCC identified only one violation: Verizon's alleged failure to implement reasonable LBS program policies, which it applied uniformly to all participants in that program. The FCC's assertion that it could disaggregate that one act (or failure to act) into either 63 separate acts (one for each

participant) or tens of millions of separate acts (one for each customer) shows the FCC's disregard of Congress's statutory limit on its authority.

IV. The Supreme Court's decision in *Jarkesy* confirms that the Forfeiture Order is unconstitutional. An agency that seeks to impose monetary penalties triggers the Seventh Amendment's jury-trial guarantee. *See* 144 S. Ct. at 2129. The Forfeiture Order falls squarely within *Jarkesy*; it does not vindicate a public right. Nor is the FCC correct that the constitutional violation is cured because Verizon could refuse to comply with the binding FCC order — suffering the consequences that follow — while waiting up to five years for the Department of Justice to bring a case in which Verizon would risk being unable to challenge the FCC's legal theories.

STANDARD OF REVIEW

This Court reviews constitutional claims and questions of law, including whether an agency properly interpreted a statute, de novo. *See Loper Bright Enters. v. Raimondo*, 144 S. Ct. 2244, 2273 (2024); *Pierre v. Holder*, 588 F.3d 767, 772 (2d Cir. 2009). The Court must set aside an agency's factual findings if they are "unsupported by substantial evidence." *Metro-N. Commuter R.R. Co. v. U.S. Dep't of Lab.*, 886 F.3d 97, 106 (2d Cir. 2018).

The FCC's decision "cannot be upheld if it is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law, or is contrary to

constitutional . . . power, or is in excess of statutory jurisdiction, authority, or limitations." *Town of Deerfield v. FCC*, 992 F.2d 420, 427 (2d Cir. 1993) (citations omitted). The arbitrary-and-capricious standard requires courts to ensure that "the agency has acted within a zone of reasonableness and, in particular, has reasonably considered the relevant issues and reasonably explained the decision." *FCC v. Prometheus Radio Project*, 592 U.S. 414, 423 (2021).

ARGUMENT

I. DEVICE-LOCATION INFORMATION IS NOT CPNI

The Forfeiture Order turns, initially, on the FCC's claim that the device-location information available through Verizon's former LBS program is CPNI. *See* Forfeiture Order ¶ 22 (JA53-54) (concluding that the "the customer location information disclosed in Verizon's LBS program is CPNI under the Act and our rules"). The FCC is wrong.

To qualify as CPNI, information must meet two independent conditions. First, the information (whatever its content) must come into the carrier's possession in a certain way: it must be "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). Second, the content of the information must "relate[] 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." *Id.* The FCC's conclusion that device-location information is CPNI fails both prongs. A failure on either is sufficient to vacate the Forfeiture Order.

A. The Location Information Was Not Made Available to Verizon "Solely by Virtue of the Customer-Carrier Relationship"

Verizon has access to device-location information for all its customers' devices. The LBS program relied on Verizon's ability to ping a device while turned on and connected to its network and to use the location of Verizon's cell sites to determine roughly (within 1,000 meters) the device's location. Donnellan Decl. ¶¶ 5, 7-9 (JA42-44); LOI Resp. at 4 (JA99). But that location information was not "made available to [Verizon] by the customer *solely by virtue of* the carrier-customer relationship," 47 U.S.C. § 222(h)(1)(A) (emphasis added).

"Solely" means "to the exclusion of all else" or "without another." *Solely*, *Merriam-Webster's Collegiate Dictionary* 1118 (10th ed. 1997);[10] *see also Helvering v. Sw. Consol. Corp.*, 315 U.S. 194, 198 (1942) ("'Solely' leaves no leeway."). And Verizon is a carrier (i.e., a common carrier) only while it is providing telecommunications services or commercial mobile services. *See* 47

[10] This Court regularly relies on this dictionary when considering late 1990s laws. *See*, *e.g.*, *Int'l Union, United Auto., Aerospace & Agric. Implement Workers of Am., AFL-CIO v. NLRB*, 520 F.3d 192, 197 (2d Cir. 2008); *United States v. Badmus*, 325 F.3d 133, 140 n.4 (2d Cir. 2003) (per curiam); *Albertson v. Apfel*, 247 F.3d 448, 449 (2d Cir. 2001) (per curiam); *Burgo v. Gen. Dynamics Corp.*, 122 F.3d 140, 143 (2d Cir. 1997).

U.S.C. §§ 153(51), 332(c)(1)-(2). Yet the only common-carrier service Verizon offered wireless customers was voice service, as both text messaging and internet access were (and are) non-common-carrier services.[11] Therefore, information is CPNI if Verizon has it *only* because of Verizon's provision of voice service to its customers.

Lots of information easily satisfies that standard, such as information about the voice plan to which a customer subscribes or the specific calls a customer dials or answers. Verizon obtains that information solely by virtue of its provision of a common-carrier voice service to that customer. But that is not true of device-location information. The record is clear that Verizon could ping any turned-on wireless device connected to the Verizon network. Verizon thus can obtain device-location information even if the customer is not using — or has not purchased — a Verizon voice service (e.g., a data-only customer). *See* Donnellan Decl. ¶¶ 8-9 (JA43-44); Forfeiture Order ¶¶ 27, 31, 33 (JA55, 57-58). The record also showed that more than [redacted] of the traffic on Verizon's network is associated with data services. *See* Altland Decl. ¶ 2 (JA166). Therefore, the location data was not made available to Verizon "*solely* by virtue of" any carrier-customer relationship it has with its customers.

[11] *See supra* note 2.

In finding this prong satisfied, the Forfeiture Order reads that phrase out of the statute. The FCC begins with the fact that customers who buy both voice and data services "have *a* carrier-customer relationship" with Verizon. Forfeiture Order ¶ 29 (JA56) (emphasis added). But if having a carrier-customer relationship were sufficient, the CPNI definition would say that it includes information "made available to the carrier by a customer with which it has a carrier-customer relationship." That is not the language Congress enacted. *See SAS Inst., Inc. v. Iancu*, 584 U.S. 357, 363 (2018) ("Where a statute's language carries a plain meaning, the duty of an administrative agency is to follow its commands as written, not to supplant those commands with others it may prefer.").

The FCC next notes that buying common-carrier voice service is sufficient to make device-location data available to Verizon and that voice customers could not prevent Verizon from obtaining that information. *See* Forfeiture Order ¶ 31 (JA57). But the statutory phrase "solely by virtue of" means a single condition that is both necessary *and* sufficient, not merely sufficient. *See Husted v. A. Philip Randolph Inst.*, 584 U.S. 756, 768 (2018) (interpreting "solely by reason of" to mean "only if" the condition is met and "for no reason other than" the condition). And here, a carrier-customer relationship was not a necessary condition (let alone the sole one) for Verizon to obtain the location information at issue.

The FCC also asserts that Verizon's provision of voice and data services does not "take[] the resulting *relationship* outside the scope of the 'carrier-customer' relationship." *Id.* ¶ 32 (JA57). Of course it does. Congress was clear that a company "shall be treated as a common carrier . . . only to the extent that it is engaged in providing telecommunications services," 47 U.S.C. § 153(51), and only "insofar as such person is . . . engaged" in providing commercial mobile service, *id.* § 332(c)(1)(A). That is why a company's status as a telecommunications carrier is "activity-based" — it wears its common-carrier "hat" only while providing the specific services that make it a common carrier, taking that hat off whenever it is providing other services. *AT&T Mobility*, 883 F.3d at 862. Verizon has no carrier-customer relationship when providing data services.

Finally, the FCC suggests that device-location information would fall outside of the CPNI definition only if Verizon obtained the information "exclusively . . . from non-voice customers." Forfeiture Order ¶ 33 (JA58). But that gets the statute backward. The statute asks whether the location information was made available "solely by virtue of" the carrier-customer relationship. The fact that Verizon "could have obtained the customer's location . . . even in the absence of a voice plan" is what takes the location information outside the CPNI definition. *Id.* at 44 (JA88) (Commissioner Carr, dissenting).

B. The Information Does Not Relate to the Location of a Telecommunications Service

The location information is not CPNI for the additional, independent reason that it reveals only the location of a device, not of a telecommunications service. The FCC recognized as much in the NAL: "The location data was derived from the wireless mobile devices of Verizon's customers communicating with nearby network signal towers to signal *the location of those devices*." NAL ¶ 43 (JA126) (emphasis added). Device-location information is not information that "relates to the . . . location . . . of a telecommunications service." 47 U.S.C. § 222(h)(1)(A).[12] Verizon did not need to wait for a customer to be on a call to obtain location information in response to a customer's express request submitted through the LBS program. Instead, Verizon could ping a device owned by a customer who subscribed to no telecommunications (i.e., voice) service or who was not using (or never used) a telecommunications service. *See* Donnellan Decl. ¶¶ 3, 9 (JA41-42, 43-44); Forfeiture Order ¶¶ 23, 27 (JA54-55).

In concluding otherwise, the FCC ignores that "location" was not in the definition of CPNI in 1996, but rather was added in 1999, along with other

[12] The FCC addresses at some length whether the statute is better read as "location . . . of a telecommunications service" or "location . . . of use of a telecommunications service." Forfeiture Order ¶¶ 24-26 (JA54-55). The Court need not resolve that grammatical dispute. As explained in the text, a wireless device is neither a telecommunications service nor the use of a telecommunications service, and "location" means call location information.

amendments to § 222. Those amendments were intended to allow emergency services to "determine the location of *the caller*" using a "wireless phone[]." S. Rep. No. 106-138, at 2 (1999) (emphasis added). Congress simultaneously wanted to "provide[] privacy protection for *the call location information* of users of wireless phones." *Id.* (emphasis added).

Congress achieved those purposes by creating a new exception to § 222(c)(1)'s prohibition on the nonconsensual use, disclosure, or access to CPNI for "call location information." Wireless carriers can disclose "call location information," without customer consent, to various emergency service providers and to family members in an emergency involving the risk of death or serious physical harm. 47 U.S.C. § 222(d)(4). And Congress clarified that, in the context of "call location information," consent for purposes of § 222(c)(1) means "express prior authorization." *Id.* § 222(f)(1).[13] Consistent with these two provisions, Congress also added "location" to § 222(h)(1)(A), so § 222(c)(1)'s protection of CPNI included that call location.

The FCC, however, concludes that Congress's use of "location" — not "call location" — in § 222(h)(1)(A) means that § 222(c)(1) protects *all* location

[13] Congress created a further exception permitting disclosures in the context of an "automatic crash notification system" — that is, where cars made automated calls to services like OnStar following a car accident, revealing the car's location even if the customer could not speak. 47 U.S.C. § 222(f)(2).

information from nonconsensual disclosure. Forfeiture Order ¶ 28 (JA55-56). But that leads to nonsensical results. It would mean that Verizon may provide call location information to emergency service providers or immediate family in a life-threatening emergency without its customer's consent, *see* 47 U.S.C. § 222(d)(4), but not device-location information. It would mean that only "express prior authorization" counts as consent for call location information, *id.* § 222(f)(1), but lesser forms of consent — including a failure to opt out — could suffice for disclosing device-location information. Yet device-location information, which is available whenever a device is turned on, is even more "obviously sufficiently sensitive" than call location information (which is available only during calls), Forfeiture Order ¶ 28 (JA56), and likely more important in an emergency, as the user may be unconscious or incapable of making a call.

Understanding location in § 222(h)(1)(A) to refer only to call location information is also consistent with the rest of the CPNI definition. A wireless device is not a telecommunications service — Apple sells iPhones, not phone service. The "location . . . of a telecommunications service subscribed to by a[ ] customer," therefore, refers to the location of the device when the customer uses the telecommunications service to make or answer a call. The FCC previously agreed with this, finding it "straightforward" that CPNI includes "the location of the device at the time of . . . calls." Declaratory Ruling, *Implementation of the*

Telecommunications Act of 1996, 28 FCC Rcd 9609, ¶ 22 (2013). The FCC tries to brush aside its prior interpretation, *see* Forfeiture Order ¶ 28 & n.100 (JA56), but this Court owes no deference or even special weight to an agency's novel statutory interpretation, *see Loper Bright*, 144 S. Ct. at 2273.

II. THE FCC'S CONCLUSION THAT VERIZON DID NOT REASONABLY PROTECT CUSTOMERS' LOCATION INFORMATION IS ARBITRARY AND CAPRICIOUS

Verizon had reasonable measures in place to discover and protect against attempts to gain unauthorized access to its customers' location information, both before and after learning of Securus's and Hutcheson's actions. Verizon instituted numerous safeguards to protect its customers' location information in connection with its LBS program. Those measures included vetting and conducting ongoing monitoring of program participants, LOI Resp. at 3 (JA98); Supp. LOI Resp. at 14-15 (JA21-22); limiting the sharing of location information to preapproved use cases, LOI Resp. at 2, 8 (JA97, 103); Supp. LOI Resp. at 14 (JA21); imposing information security requirements and adherence to industry best practices on participants, NAL ¶ 15 & n.54 (JA119) (citing VZ-03-0000007 and VZ-03-0000050); reviewing participants' notice-and-consent language, Supp. LOI Resp. at 8-9 (JA15-16); requiring the production of consent records on a daily basis, Bruner Decl. ¶ 3 (JA33); and retaining Aegis to review those consent records, analyze program data to find any potential issues, and otherwise monitor the

program and participants, Bruner Decl. ¶¶ 6-7 (JA34-35); Bruner Supp. Decl. ¶¶ 6-8 (JA38).

Those safeguards worked. Over the many years and hundreds of millions of transactions in the Verizon LBS program, the FCC identified only one participating service provider (Securus) — out of more than 60 — that violated those protections in connection with access to device-location information for 11 customers. *See* Forfeiture Order ¶¶ 13-14 (JA50-51); Bruner Supp. Decl. ¶ 9 (JA38-39). Some occurred [redacted]. Verizon NAL Resp. at 3, 19-20 & n.16 (JA159, 162-63). That was a "quite small" volume, "as compared to the numbers associated with [Verizon's LBS] program as a whole." Bruner Supp. Decl. ¶ 9 (JA38-39).[14]

The fact that Aegis did not find those few needles in a massive haystack — where it matched 99.95% of requests to valid consent records and validated a statistically significant, randomly selected sample of the remainder, Bruner Decl. ¶ 6 (JA34)[15] — is not evidence of "fundamental shortcomings" or a "significant

[14] The record contains no evidence of requests submitted to Verizon through Securus on behalf of law enforcement officials with a judicial warrant or other legal authorization. Instead, such requests likely were submitted through Verizon's well-established procedures for legitimate law enforcement requests for customer location data, which were handled outside the LBS program. *See* LOI Resp. at 10-11 (JA105-06).

[15] The FCC's assertion that Verizon "fail[ed] to verify the validity of th[e] consent" that LBS program participants obtained from Verizon's customers,

loophole" in Verizon's procedures. Forfeiture Order ¶¶ 48, 53 (JA64, 66). The FCC's own prior conduct confirms this. The FCC failed to take any enforcement action — or even alert Verizon and other wireless carriers — after it learned of Securus's and Hutcheson's actions in mid-2017. That belies its current claim that those actions revealed serious flaws in Verizon's safeguards. Forfeiture Order ¶ 48 (JA64).

Even if Verizon's safeguards before the *New York Times* article were insufficient, Verizon's additional actions in the wake of that article reasonably bolstered its defenses against a recurrence. Verizon immediately cut off access to the LBS program for Securus, shutting off the one known vector for unauthorized requests. Supp. LOI Resp. at 15-16 (JA22-23). And Verizon ceased taking new applications to join the program. LOI Resp. at 10 (JA105). Verizon had Aegis strengthen the transaction verification process to identify any anomalies in the data relating to consent requests that could indicate a potential issue. *Id.* Aegis also scrutinized Securus's transaction history to better inform and refine its data analytics to detect any issues with other participating service providers. Bruner Supp. Decl. ¶ 11 (JA39).

Forfeiture Order ¶ 57 (JA67), thus has no support in the record evidence. *See Metro-N. Commuter R.R.*, 886 F.3d at 106 (vacating agency decision for lack of "substantial evidence," which requires that the record contain evidence that "a reasonable mind might accept as adequate to support a conclusion").

The FCC claims that none of this "improve[d] the safeguards for consumers whose location information could be disclosed under the location data sharing arrangements that remained in place." Forfeiture Order ¶ 55 (JA66). Nonsense. Verizon and Aegis were better positioned to catch the next violator (if there was one) — even if, like Securus, that violator submitted unauthorized requests related to only a handful of customers, spread out over time. And the FCC does not point to a single other violation of the terms of Verizon's LBS program by a participating service provider, much less one that Verizon and Aegis failed to catch.

The touchstone of the FCC's rule requiring common carriers to protect against attempts to gain unauthorized access to CPNI is reasonableness. 47 C.F.R. § 64.2010(a). The FCC's wholesale rejection of Verizon's measures, both before and after the *New York Times* article, refutes the FCC's claim in the Forfeiture Order that it "require[d] only reasonable measures — not perfect ones." Forfeiture Order ¶ 58 (JA67). Only a perfect system — or an unusually lucky one — could have caught the unauthorized location requests for 11 Verizon customers. Verizon's and Aegis's failure to catch them is thus not evidence that Verizon's system "designed to monitor customer consents" was "incapable of detecting its opposite" or that Verizon "did not have a reliable way of confirming customer consent." *Id.* ¶¶ 56, 58 (JA67-68).

Indeed, the FCC's decision to provide a 30-day "grace period," during which Verizon could fix the supposed problems or terminate the program and not face any penalty, *id.* ¶ 54 n.182 (JA66), shows the FCC does not believe its own assertions about the supposed flaws in Verizon's procedures to protect its customers' information. Had the FCC truly considered these flaws to be serious, as the Forfeiture Order asserts, the FCC could not simultaneously take the position that Verizon could have escaped any penalty by shutting down the program faster.[16]

The FCC, contrary to its claims, is thus penalizing Verizon for a "small" "shortcoming in [its] measures," which "results in a strict liability approach" that is "contrary to the reasonableness standard reflected in th[e] rule" that Verizon allegedly violated. *Id.* ¶ 58 (JA67-68). This Court, too, has recognized that, where the law requires "*reasonable* care," it is improper to "effectively" impose "strict liability." *SEC v. Rashid*, 96 F.4th 233, 242 (2d Cir. 2024). Yet that is what the FCC did.

The FCC's adoption of an effective strict liability regime is unlawful for the additional reason that the FCC provided no fair notice of this requirement. Had

[16] Moreover, if the FCC's "grace period" — which is *not* how the FCC described it in the NAL — was in fact a determination that Verizon had to shut down the program in 30 days to avoid a penalty, that was arbitrary and capricious. The FCC had never previously announced such a standard. And imposing an absolute 30-day deadline to shut down the program would have left customers unable to access essential services like Life Alert and roadside assistance.

Verizon known the FCC would conclude that the only reasonable response to the Hutcheson requests — for a handful of customers through one participating service provider that slipped through Verizon's safeguards — was for Verizon to end its LBS program within 30 days of the *New York Times* article, Verizon would have done so (despite the harms to consumers that relied on those services) to avoid this massive penalty. The FCC cannot, without fair notice, announce its new rule for the first time in an enforcement proceeding: "[i]t is one thing to expect regulated parties to conform their conduct to an agency's interpretations once the agency announces them," but improper to "require regulated parties to divine the agency's interpretations in advance or else be held liable when the agency announces its interpretations for the first time in an enforcement proceeding." *Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 158-59 (2012); *ABC, Inc. v. FCC*, 475 F. App'x 796, 798 (2d Cir. 2012) (summary order) (citing *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 258 (2012)).

III. THE FCC UNLAWFULLY EVADED CONGRESS'S LIMITS ON ITS FORFEITURE AUTHORITY

Even if the FCC's statutory interpretation were correct and device-location information were CPNI and even if Verizon's safeguards were unreasonable, the FCC's $46.9 million forfeiture penalty violates the Communications Act. In authorizing the FCC to assess forfeitures, Congress set maximum forfeiture amounts. As applicable here, even when finding a "continuing violation," any

forfeiture "shall not exceed a total of" $2,048,915 "for any single act or failure to act." 47 U.S.C. § 503(b)(2)(B); 47 C.F.R. § 1.80(b) (2020). But the FCC issued a forfeiture against Verizon for nearly 23 times that maximum statutory amount.

Here, the FCC found that, in implementing its LBS program, Verizon "failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information." Forfeiture Order ¶ 46 (JA63). That is a "single act or failure to act." 47 U.S.C. § 503(b)(2)(B). Verizon had one set of LBS program policies, which it applied uniformly to all program participants. The FCC's (flawed) finding that those policies "fail[ed]" to "impose reasonable safeguards" describes a single act or failure to act. Forfeiture Order ¶ 65 (JA70); *see also id.* ¶ 80 n.245 (JA74) (similar, referring to "an ongoing failure"); *id.* ¶ 89 (JA77) (similar, referring to Verizon's "failure"). Thus, the maximum forfeiture penalty the FCC could impose was $2,048,915.

To adopt a forfeiture penalty nearly 23 times the statutory limit, the FCC "artificially fragment[ed] a singular act into multiple acts." *Schlaifer Nance & Co. v. Est. of Warhol*, 119 F.3d 91, 98 (2d Cir. 1997). The FCC disaggregated Verizon's single set of uniformly applied LBS program policies into 63 separate failures to implement a reasonable data-security regime — one for each remaining LBS program participant after Verizon kicked out Securus. *See* Forfeiture Order ¶¶ 77-78, 86 (JA73-74, 76). As FCC Commissioner Simington explained in

dissenting from the Forfeiture Order, "[t]here is no valid basis" for treating "a single, systemic failure to follow the Commission's rules" as though it were "many separate and continuing violations." *Id.* at 46 (JA90) (Commissioner Simington, dissenting).

The FCC's defense of its action demonstrates its unlawfulness. The agency chides Verizon for complaining that the FCC found 63 separate violations, describing its count as "eminently *conservative*" — the FCC claims it could instead have found "tens of millions" of violations, one for each customer. *Id.* ¶ 80 (JA74). But as Commissioner Simington correctly noted, it is "simply not plausible" that Congress meant to allow the FCC to "arrive at forfeitures of any size simply by disaggregating an 'act' into its individual constituent parts, counting the members of whatever class of objects may be related to the alleged violation to arrive at whatever forfeiture amount suits a preordained outcome." *Id.* at 46 (JA90) (Commissioner Simington, dissenting).[17]

[17] The FCC cites a 2014 NAL as a past instance in which it similarly disaggregated a single act into multiple acts. *See* Forfeiture Order ¶ 79 (JA74); Notice of Apparent Liability for Forfeiture, *TerraCom, Inc. and YourTel America, Inc.*, 29 FCC Rcd 13325 (2014) ("*TerraCom NAL*"). The *TerraCom NAL* suggested that such disaggregation would allow a $9 *billion* forfeiture, only to propose one of $8.5 *million*. *TerraCom NAL* ¶ 52. That conclusion was in error, but the FCC then settled with TerraCom for $3.5 million, preventing judicial review. *See* Order and Consent Decree, *TerraCom, Inc. and YourTel America, Inc.*, 30 FCC Rcd 7075, ¶ 28 (Enf. Bur. 2015). The *TerraCom NAL* nevertheless is

While the FCC chafes at the limits Congress imposed on its forfeiture authority, those limits are for Congress to change, not the FCC. *See West Virginia v. EPA*, 597 U.S. 697, 723 (2022) ("Agencies have only those powers given to them by Congress.").

IV. THE FORFEITURE ORDER VIOLATES THE SEVENTH AMENDMENT

A. The Supreme Court's Decision in *Jarkesy* Controls Here

In *Jarkesy*, the Supreme Court held that the SEC violated the Seventh Amendment by imposing civil penalties for federal securities fraud through an administrative adjudication, rather than filing a complaint in federal court to initiate litigation in which Mr. Jarkesy could demand a jury trial. *See* 144 S. Ct. at 2127. The Court explained that the SEC's administrative remedy — "money damages" that are "designed to punish or deter," not "solely" to "restore" victims — was "all but dispositive" of the constitutional question. *Id.* at 2129. But the Court noted further that the "close relationship between federal securities fraud and common law fraud" causes of action — even though not "identical" — "confirm[ed]" that the SEC's administrative punishment was "legal in nature." *Id.* at 2129-31. The Court also held that the SEC's administrative adjudication did not fall within the "public rights exception" to the Seventh Amendment, because the

---

instructive, showing the FCC believes that there is no meaningful limit on its forfeiture authority. Yet Congress clearly imposed a binding maximum penalty.

SEC sought a "punitive remedy" and targeted "the same basic conduct as common law fraud." *Id.* at 2135-36. Justice Sotomayor, in dissent, recognized that *Jarkesy* was not limited to the SEC, identifying many agencies, including the FCC, whose practice of "impos[ing] civil penalties in administrative proceedings" would be "upend[ed]." *Id.* at 2173-75 (Sotomayor, J., dissenting).

Justice Sotomayor was right; *Jarkesy* controls here. As in *Jarkesy*, the fact that the FCC seeks "civil penalties . . . designed to punish" is "all but dispositive" of Verizon's entitlement to an Article III court and a jury, rather than an agency prosecutor and adjudicator. *Id.* at 2129. The FCC's $46.9 million forfeiture is "designed to be punitive." *Id.* at 2130. Congress expressly designated FCC forfeitures as a "penalty." 47 U.S.C. § 503(b)(1); *see CBS Corp. v. FCC*, 663 F.3d 122, 134 (3d Cir. 2011) (describing the FCC forfeiture as "punitive"). In setting the amount of the penalty (subject to the cap), the FCC must consider the "gravity of the violation," "the degree of culpability," and "any history of prior offenses," 47 U.S.C. § 503(b)(2)(E) — all considerations that confirm a punitive purpose, *see Jarkesy*, 144 S. Ct. at 2129-30. The FCC also "is not obligated to return any money to victims." *Id.* at 2130. Nor could it, because "forfeitures . . . shall be payable into the Treasury." 47 U.S.C. § 504(a).

The "close relationship between" the FCC's theory of wrongdoing and common-law analogs confirms that the Forfeiture Order is "legal" in nature.

Jarkesy, 144 S. Ct. at 2129-31. The FCC's conclusion that Verizon failed "to take reasonable measures," Forfeiture Order ¶ 42 (JA61), is in substance a common-law negligence claim. Such claims generally concern the "fail[ure] to exercise reasonable care." *Rashid*, 96 F.4th at 240; *see also Ross v. Bernhard*, 396 U.S. 531, 542 (1970) (holding that a statutory cause of action sounding in negligence triggered the Seventh Amendment).

In addition, the FCC is punishing Verizon for violating a rule "designed to protect consumer privacy," Forfeiture Order ¶ 97 (JA81), which is analogous to well-known common-law claims, including for tortious invasion of privacy, intrusion upon seclusion, or trespass. This Court recently concluded that a statute prohibiting the nonconsensual disclosure of video rental information "is closely related to at least one common-law analog traditionally recognized as providing a basis for a lawsuit in American courts: public disclosure of private facts." *Salazar v. NBA*, 118 F.4th 533, 540 (2d Cir. 2024). Other courts of appeals have reached similar results. For example, in *Pichler v. UNITE*, the Third Circuit held that a statute protecting information from an individual's motor vehicle records was "analogous to common law causes of action" for "interference with protected personal or property interests" and required a jury trial. 542 F.3d 380, 388 (3d Cir. 2008) (citing Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213 n.1 (1890)); *see also Bryant v. Compass Grp. USA, Inc.*, 958 F.3d

617, 624 (7th Cir. 2020) (describing statute protecting against "use" of a person's biometric information without informed consent as akin to an action for "trespass"); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (describing statute protecting against disclosure of consumers' personal information as akin to a "right to privacy" that has "long been actionable at common law").

The $46.9 million monetary penalty that the FCC imposed on Verizon is legal in nature, and common-law analogs to the FCC's cause of action confirm it. Under *Jarkesy*, that means the Seventh Amendment applies, and the FCC's imposition of the Forfeiture Order through an administrative process, without a jury and Article III court, is unconstitutional.

B. The FCC's Attempts To Evade *Jarkesy* Lack Merit

Each of the FCC's three attempts in the Forfeiture Order to dodge this constitutional problem fail.

First, the FCC asserted in the Forfeiture Order that the Fifth Circuit's decision in *Jarkesy* was wrong. *See* Forfeiture Order ¶¶ 97-98 (JA80-82). Of course, the Supreme Court rejected that argument when it affirmed the Fifth Circuit's decision shortly after the Forfeiture Order issued. *See* 144 S. Ct. at 2136 ("Congress cannot conjure away the Seventh Amendment by mandating that traditional legal claims be taken to an administrative tribunal.") (cleaned up).

Second, the FCC contended that its forfeiture action involves a public right exempt from the Seventh Amendment. Forfeiture Order ¶ 97 (JA80-81). The FCC is incorrect. *Jarkesy* explains that "public rights are a narrow class defined and limited by history" to, for example, revenue collection, customs enforcement, immigration, relations with Indian tribes, administration of public lands, and the granting of public benefits. 144 S. Ct. at 2131-33; *see id.* at 2146 (Gorsuch, J., concurring). The FCC's monetary penalty for privacy violations is far afield from those categories, and its common-law analogs confirm that. *See id.* at 2132 ("If a suit is in the nature of an action at common law, then the matter presumptively concerns private rights, and adjudication by an Article III court is mandatory."); *see also id.* at 2146 (Gorsuch, J., concurring) ("[D]espite its misleading name, the exception does not refer to *all* matters brought by the government against an individual to remedy public harms.").[18]

Third, the FCC incorrectly claims that the Communications Act's forfeiture provisions present no Seventh Amendment problem because "Verizon is entitled to a trial *de novo*" under 47 U.S.C. § 504(a) "before it can be required to pay the forfeiture." Forfeiture Order ¶ 91 (JA78). The FCC is correct that, if Verizon flouted the FCC's order commanding it to pay $46.9 million within 30 days, *see id.*

[18] Here, the Court need not decide that an FCC forfeiture order could never involve a public right, just that this forfeiture does not.

¶ 103 (JA83), it would face the potential of a Department of Justice suit filed in a federal district court, where Verizon could demand a jury trial.

But that is not the kind of jury trial that *Jarkesy* holds the Seventh Amendment requires. *See* 144 S. Ct. at 2131. First, multiple courts of appeals have held that, in a § 504(a) trial, the defendant cannot challenge the FCC's legal interpretations or raise constitutional challenges. *See Stevens*, 691 F.3d at 622-23; *United States v. Any & All Radio Station Transmission Equip.*, 207 F.3d 458, 463 (8th Cir. 2000) (similar); *United States v. Dunifer*, 219 F.3d 1004, 1008 n.8 (9th Cir. 2000) (similar).[19] And while not every court of appeals has had a chance to address this question, Verizon is subject to nationwide venue under § 504(a): it can be sued not just where it "has its principal operating office," but also "in any district through which [its nationwide wireless] system" runs, which is all of them. 47 U.S.C. § 504(a). Therefore, the Department of Justice could choose to sue Verizon in a district in a circuit that has already foreclosed a defendant's ability to challenge the FCC's legal conclusions in a § 504(a) action.

The right to a trial by jury includes the right to trial by a jury properly instructed on the law. That is why this Court regularly overturns jury verdicts in

[19] This Court has indicated, but not held, that district courts lack jurisdiction to hear constitutional challenges in actions brought under § 504(a). *See Prayze FM v. FCC*, 214 F.3d 245, 250-51 (2d Cir. 2000) (noting jurisdictional question but declining to resolve it).

civil cases where the district court improperly instructed the jury on the law and the erroneous instruction was prejudicial. *See*, *e.g.*, *Palin v. N.Y. Times Co.*, 113 F.4th 245, 277 (2d Cir. 2024); *Utica Mut. Ins. Co. v. Munich Reinsurance Am., Inc.*, 7 F.4th 50, 65 (2d Cir. 2021); *US Airways, Inc. v. Sabre Holdings Corp.*, 938 F.3d 43, 63 (2d Cir. 2019). Here, the key flaws in the Forfeiture Order are legal. A jury instructed according to the FCC's incorrect interpretation of CPNI or of the phrase "single act or failure to act" would clearly prejudice Verizon. Indeed, a jury trial in which a defendant cannot object to — and the trial court must read, unchanged — the plaintiff's proposed instructions on the law that the jury is to apply does not comport with the Seventh Amendment or the normal division of authority between courts and federal agencies. *See Loper Bright*, 144 S. Ct. at 2266 ("abdication in favor of the agency is *least* appropriate" on questions of law). Thus, a § 504(a) collection action would not provide Verizon with a true jury trial on the merits.

Second, even aside from that limitation, the Department of Justice collection lawsuit that § 504(a) authorizes is far afield from the SEC's option to proceed in court against Mr. Jarkesy, which the Supreme Court noted would have complied with the Seventh Amendment. *See Jarkesy*, 144 S. Ct. at 2125, 2138. Such a federal court complaint would have contained mere allegations of wrongdoing — which Mr. Jarkesy could contest — and a request for relief from the jury, filed

within five years of the allegedly wrongful action. *Id.* at 2125; *Gabelli v. SEC*, 568 U.S. 442, 445 (2013). The FCC's Forfeiture Order, in contrast, does not state mere allegations. Instead, it adjudicates liability and orders the payment of a specific sum of money to the federal government. The Department of Justice also could wait until 2029 to bring suit about conduct that ended in March 2019. *See* 47 U.S.C. § 504(a); 28 U.S.C. § 2462 (five-year statute of limitations).[20] Any jury trial at that point would involve stale evidence or faded witness memories of relevant events occurring more than a decade earlier.

In the meantime, the Forfeiture Order would present serious reputational and practical problems for Verizon. Verizon would have to disclose the Forfeiture Order's adverse findings, for example, when seeking government contracts. And the FCC can use its judicially unreviewed factual findings as a basis to enhance future penalties against Verizon. *See* Report and Order, *Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, 12 FCC Rcd 17087, ¶ 34 (1997). On top of that, Verizon would suffer the reputational harms of an adjudication of wrongdoing and the flouting of an agency order compelling payment. *See Fox Television Stations*, 567 U.S. at 255-56.

[20] The delay could be even longer. The FCC has no deadline for deciding whether to convert an NAL into a forfeiture order.

For all these reasons, the trial that § 504(a) contemplates does not cure the constitutional violation in the purely administrative enforcement proceeding that led to this Forfeiture Order.

CONCLUSION

The Court should vacate the Forfeiture Order and direct the FCC to take any steps necessary to ensure that the $46,901,250 Verizon paid is returned to it. *See United Gas Improvement Co. v. Callery Props., Inc.*, 382 U.S. 223, 229 (1965) ("An agency, like a court, can undo what is wrongfully done by virtue of its order."); *TNA Merch. Projects, Inc. v. FERC*, 857 F.3d 354, 361 (D.C. Cir. 2017) (similar).

Respectfully submitted,

/s/ *Scott H. Angstreich*
Scott H. Angstreich
Aaseesh P. Polavarapu
KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900
sangstreich@kellogghansen.com
apolavarapu@kellogghansen.com

Counsel for Petitioner Verizon Communications Inc.

November 4, 2024

CERTIFICATE OF COMPLIANCE

I certify, pursuant to Federal Rule of Appellate Procedure 32(g), that this brief complies with the type-volume limitation of Local Rule 32.1(a)(4) because, excluding the portions of the brief exempted by Federal Rule of Appellate Procedure 32(f), the brief contains 11,882 words.

I further certify that this brief complies with the typeface and type style requirements of Federal Rule of Appellate Procedure 32(a)(5) and (a)(6) and Local Rule 32.1 because it has been prepared using Microsoft Word in a proportionally spaced typeface (Times New Roman, 14 point).

/s/ *Scott H. Angstreich*
Scott H. Angstreich

Counsel for Petitioner Verizon Communications Inc.

November 4, 2024

CERTIFICATE OF SERVICE

I hereby certify that, on November 4, 2024, an electronic copy of the redacted Brief for Petitioner Verizon Communications Inc. was filed with the Clerk of the Court using the ACMS system and thereby served upon all counsel appearing in this case.

/s/ *Scott H. Angstreich*
Scott H. Angstreich

Counsel for Petitioner Verizon Communications Inc.