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

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

Scott H. Angstreich
Aaseesh P. Polavarapu
Daren G. Zhang
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
dzhang@kellogghansen.com

Counsel for Petitioner Verizon Communications Inc.

February 7, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES AND REGULATIONS

ADMINISTRATIVE DECISIONS

OTHER MATERIALS

INTRODUCTION AND SUMMARY OF ARGUMENT

For roughly a decade, Verizon operated a location-based service ("LBS") program. That program processed hundreds of millions of requests from Verizon customers who provided their affirmative consent to share their device-location information to receive beneficial services they sought from third party providers, including for roadside assistance or life-saving care. The FCC imposed nearly $200 million in penalties collectively against Verizon and three other wireless carriers that operated similar programs, asserting that they had allowed unauthorized access to device-location information for "hundreds of people." FCC Br. 3. But for Verizon, only 11 customers' device-location information was accessed without authorization — all during [redacted] and all by a single sheriff who obtained it from a single third-party service provider.

The magnitude of the FCC's penalty on Verizon (nearly $47 million) is disproportionate to any breach involving just 11 customers. The penalty is even more unreasonable given that the breach occurred outside the statute of limitations and the FCC penalized Verizon for actions within the limitations period during which there was no evidence of any attempted, let alone successful, breach. The FCC, however, claims that the unauthorized access of 11 customers' device location information revealed that Verizon's many safeguards for its customers'

device-location information were so woefully inadequate that Verizon had to shut down its LBS program much faster than it did. But the FCC knew about the sheriff's misuse of wireless carriers' LBS programs long before Verizon and did *nothing*, belying its claims that Verizon's safeguards had fundamental flaws that required immediate corrective action. In fact, outside the sheriff's misconduct, Verizon's safeguards worked extremely well to protect its customers' information, which Verizon secured because of its sensitivity, not because it is CPNI.

The FCC's Forfeiture Order rests on four errors that each independently require vacatur. It unlawfully concludes that device-location information is CPNI, arbitrarily finds Verizon's safeguards unreasonable, breaches Congress's clear limit on maximum forfeitures, and violates the Seventh Amendment's jury trial guarantee. The FCC's brief fails to show otherwise.

I. ***Device-Location Information Is Not CPNI.*** Verizon did not receive device-location information "solely by virtue of the carrier-customer relationship," and it does not relate to the "location . . . of" or the "location . . . of use of" a "telecommunications service." 47 U.S.C. § 222(h)(1)(A). The FCC's brief confirms the agency cannot satisfy either criterion, yet it must satisfy both to prevail.

The FCC buries its effort to give "solely" meaning in a footnote that confirms the FCC reads the word out of the statute. The Court should also reject

the FCC's attempt to expand "carrier-customer relationship" to include the sale of non-common-carrier services, like internet access and text messaging. "Carrier," in § 222, is shorthand for "telecommunications carrier" — a term Congress defined to include providers only while they are selling a common-carrier service (here, voice service).

In addition, device-location information is not the "location . . . of" or "location . . . of use of" a "telecommunications service." The word "location" in the CPNI definition refers to the same "call location" information Congress referenced in two other statutory provisions, all added to § 222 at the same time. The FCC declared this the "straightforward" reading of "location" in 2013 — in a decision it now ignores — and its new, expansive reading of "location" yields absurd results.

II. ***Verizon's Safeguards Were Reasonable.*** The FCC acted arbitrarily and capriciously in concluding that evidence a bad actor got device-location information for 11 Verizon customers revealed glaring flaws in Verizon's safeguards. As the FCC acknowledges (at 9), its own rules require reasonable measures to protect CPNI, not perfection. The record shows that Verizon's numerous affirmative measures to safeguard its customers' device-location data were both reasonable and highly effective.

To justify downplaying the extent and efficacy of Verizon's safeguards, the FCC takes out of context one sentence from an internal 2017 document describing a hypothetical risk the program might face, while ignoring its own inaction when given evidence of actual misuse, long before Verizon learned of it. That inaction — and what the FCC now calls a "grace period" after the *New York Times* story — undermine the agency's current claim that Verizon's protections for its customers' information had fundamental shortcomings. It was also reasonable for Verizon to rely on its many safeguards and a trusted contractor to monitor compliance with those safeguards, particularly when the only evidence of any breaches of the safeguards that contractor oversaw is so sparse. The FCC's unsubstantiated speculation that other breaches must have occurred is inadequate to support its finding of liability.

III. ***The Penalty Exceeds the Statutory Cap.*** Because the FCC identified only a "single act or failure to act," 47 U.S.C. § 503(b)(2)(B) — Verizon's allegedly insufficient safeguards for device-location information — the statutory maximum forfeiture was about $2 million. The FCC's defense of its decision to blow past that limit by disaggregating that one set of safeguards into 63 violations fails. The FCC had no "established practice" of doing so, citing only one non-final and unappealed 2014 decision that had disaggregated a single violation. And the violation the FCC found was in the procedures Verizon applied *after* admitting

third parties to the program, so Verizon's individual vetting of applicants cannot justify the disaggregation. The FCC should direct to Congress any complaints that the statutory cap is too low, not disregard it.

IV. ***The Forfeiture Order Violates the Seventh Amendment.*** The FCC does not dispute that its forfeiture is punitive, which is "all but dispositive" of the constitutional question. *SEC v. Jarkesy*, 603 U.S. 109, 123 (2024). And while not necessary under *Jarkesy*, the same kind of "close relationship" to common-law actions exists here that the Supreme Court found in *Jarkesy*. Nothing about the statutory privacy protection for CPNI falls within the limited public rights exception *Jarkesy* recognizes.

The FCC is thus left asserting that § 504(a) cures the Seventh Amendment violation. But the FCC does not treat its Forfeiture Order as a mere hortatory prelude to a later complaint. It is a final agency action with ordering clauses adjudicating liability and demanding prompt payment. As a final order, it has real-world consequences — including that the FCC will rely on its findings in later proceedings to increase future fines or deny license applications, and that Verizon must account for the associated liability on its books. And if Verizon does not pay the penalty, it is subject to nationwide venue, so the DOJ can bring its collection action in a forum where existing case law would preclude Verizon from raising legal defenses. That is not the kind of trial the Seventh Amendment requires.

ARGUMENT

I. DEVICE-LOCATION INFORMATION IS NOT CPNI

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

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). As the Supreme Court put it in a case the FCC ignores, the nearly identical phrase "solely by reason of" means "only if" and that there is "no reason other than" than the listed one. *Husted v. A. Philip Randolph Inst.*, 584 U.S. 756, 768 (2018).

The FCC does not dispute the key facts that show device-location information fails this test. First, Verizon provides its customers with only one common-carrier service: wireless voice service. *See* Verizon Br. 29-30. Second, Verizon can obtain device-location information even if the customer has not bought — or never uses — a wireless voice service from Verizon. *See id.* at 30. Therefore, Verizon's sale of voice service to wireless customers is not the sole reason Verizon obtains device-location information. That is dispositive of the question whether device-location information is CPNI. It is not, so the FCC's CPNI rules cannot support the Forfeiture Order.

The FCC's defense of the Forfeiture Order's contrary interpretation of "solely by virtue of" — buried in a footnote — gives no meaning to the word

"solely." The FCC contends (at 30 n.4) that Congress was "distinguish[ing] customer information obtained through the carrier's provision of service to a customer" on the one hand, "from information obtained through some unrelated means," such as from prospective customers, on the other. But the statute would draw the FCC's distinction even if it did not contain the word "solely" and instead merely said "by virtue of the carrier-customer relationship." The FCC thus impermissibly reads "solely" out of the statute. *See*, *e.g.*, *United States v. Davis*, 961 F.3d 181, 188-89 (2d Cir. 2020) (applying "'anti-surplusage' canon").

Failing in its effort to give meaning to "solely," the FCC argues (at 30-33) for a reading of "carrier-customer relationship" so expansive that it includes the sale of non-common-carrier services to customers. But contrary to the FCC's claim (at 32-33), "carrier" in "carrier-customer" unambiguously means "telecommunications carrier" and CPNI thus encompasses only common-carrier services — here, voice services.

First, Congress defined CPNI as certain information from a "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). The "customer" in the "carrier-customer relationship" is a "customer of a telecommunications carrier," and the second and third appearances

of "carrier" are thus shorthand for "telecommunications carrier." Congress also used this same shorthand throughout § 222.[1]

Second, "telecommunications carrier" is a defined term in the Communications Act. A company meets that definition "only to the extent that it is engaged in providing telecommunications services" — that is, common-carrier services. 47 U.S.C. § 153(51); *see FTC v. AT&T Mobility LLC*, 883 F.3d 848, 850 (9th Cir. 2018) (en banc) (holding that telecommunications carrier status is "activity-based"). The only carrier-customer relationship here involves Verizon's sale of wireless voice service.

There is nothing "obscure" or "elliptical," FCC Br. 33, about Congress intending for its contemporaneously enacted definition to apply to its use of that defined term throughout § 222, including in the CPNI definition. The definitions in 47 U.S.C. § 153 apply "[f]or the purposes of this chapter" — Chapter 5, which includes § 222 — "unless the context otherwise requires." The FCC identifies no context that would give the defined term a different meaning in § 222. In addition, Congress added the "telecommunications carrier" definition and § 222 in the same

[1] *See*, *e.g.*, 47 U.S.C. § 222(b) (referring to a "telecommunications carrier" and "another carrier"); *id.* § 222(d)(2) (referring to a "telecommunications carrier" and, later, "the carrier" and "other carriers"); *id.* § 222(g) (referring to a "telecommunications carrier" and "other carriers").

statute, so they "are presumed to have the same meaning." *Robers v. United States*, 572 U.S. 639, 643 (2014).

The FCC, however, claims (at 31) that, if a carrier "leverages" its wireless voice service to sell non-common-carrier services to customers, those other services are "encompassed within the carrier-customer relationship." That both ignores the holding of *AT&T Mobility* (which the FCC supported as an amicus[2]) and the record evidence that more than [redacted] of Verizon's wireless traffic is data traffic. *See* Altland Decl. ¶ 2 (JA166). If any "leveraging" were going on, the record shows it would operate in the opposite direction, with demand for non-common-carrier data services driving the purchase of common-carrier voice services.

The FCC also cites (at 31) two defined terms in its rules that it claims support expanding the breadth of the carrier-customer relationship. Yet the FCC uses those defined terms only once in its substantive rules. That lone rule merely limits a telecommunications carrier's use of CPNI "for the purpose of marketing communications-related services," which can include non-common-carrier

[2] *See* FCC Amicus Br. in Supp. of FTC at 9-12, *FTC v. AT&T Mobility LLC*, No. 15-16585 (9th Cir. filed May 30, 2017), https://bit.ly/42CsrLy.

services, to its existing voice service customers. 47 C.F.R. § 64.2007(b).[3] Nothing in that rule — or any other — attempts to make into CPNI information obtained in whole or in part because of a customer's purchase of a non-common-carrier service.

Finally, the FCC asserts (at 31-32) that, absent its expansive reading of the CPNI definition, carriers could easily evade § 222. That is wrong. Verizon obtains CPNI — such as about the voice plans to which a customer subscribes or the specific calls a customer dials or answers — solely by virtue of providing common-carrier voice services to that customer. *See* Verizon Br. 30. The former includes information that qualifies as CPNI because it relates to the quantity (how many lines), technical configuration (what kind of voice technology), and type (e.g., unlimited or a "bucket" of minutes) of the voice service. The latter includes information about the voice service that qualifies as CPNI because it relates to the destination (who is called), location (where the customer is during the call), and amount (how long are the calls) of any calls. That customer's purchase of a bundle that includes voice service along with internet access and text messaging does not

[3] The second defined term the FCC cites — "Information services typically provided by telecommunications carriers" — is only used within the definition of the first term ("Communications-related services"). 47 C.F.R. § 64.2003(e), (i).

change the fact that Verizon obtained the voice plan and call information solely because of the carrier-customer relationship.

Device-location information is different, as now-Chairman Carr noted in his dissent: "The carrier could have obtained the customer's location . . . even in the absence of a voice plan." Forfeiture Order at 44 (JA88). Information provided to Verizon through *both* a carrier-customer relationship and an internet access provider-customer relationship is not provided *solely* by virtue of either.

B. "Location" in the CPNI Definition Means Call Location

Device-location information does not qualify as CPNI for an additional, independent reason: it is not information that "relates to" either the "location . . . of" or the "location . . . of use of a telecommunications service." 47 U.S.C. § 222(h)(1)(A). No matter how "of use" is applied grammatically to the preceding words in the definition,[4] the only location information that can be CPNI is call location information. As the FCC recognized more than a decade ago, that is the "straightforward" reading of the definition: "the location of the device at the time of . . . calls" is CPNI. Declaratory Ruling, *Implementation of the Telecommunications Act of 1996*, 28 FCC Rcd 9609, ¶ 22 (2013); *see also id.* ("The location of a customer's use of a telecommunications service also clearly qualifies as CPNI.").

[4] *Compare* CTIA Amicus Br. 10-15, *with* FCC Br. 28 n.3.

In the Forfeiture Order, the FCC made a feeble attempt to dismiss the 2013 order. *See* Verizon Br. 35-36 (addressing Forfeiture Order ¶ 28 & n.100 (JA56)). In its brief, the FCC ignores that order. But as Verizon showed (at 33-36), and as now-Chairman Carr explained, *see* Forfeiture Order at 44 (JA88), the FCC was right then and is wrong now.

In its brief, the FCC contrasts Congress's addition of "location" to the definition of CPNI with its use of "call location" in two other, simultaneously enacted provisions of § 222. *See* FCC Br. 26-27. "[T]he mere possibility of clearer phrasing cannot defeat the most natural reading of a statute." *Caraco Pharm. Lab'ys, Ltd. v. Novo Nordisk A/S*, 566 U.S. 399, 416 (2012) (rejecting interpretation based on canon of meaningful variation); *Yale New Haven Hosp. v. Becerra*, 56 F.4th 9, 21 (2d Cir. 2022) (same). And the most natural reading is that Congress used "location" in § 222(h)(1)(A) to reference the same "call location" information it addressed in §§ 222(d)(4) and 222(f)(1).[5]

Any other reading also yields nonsensical results, *see* Verizon Br. 34-35, and the FCC's effort to avoid that nonsense fails. The FCC notes (at 27-28) that the

[5] Indeed, "call location" would have fit uncomfortably within the pre-existing CPNI definition. Using "location . . . of" or the "location . . . of use of a telecommunications service" to mean call location yields a far more natural sentence than if Congress had amended the definition to say "call location . . . of" or "call location . . . of use of a telecommunications service."

exception in § 222(d)(4)(A) — allowing a carrier to provide call location information to emergency service providers — applies when they "respond to the user's call for emergency services." But the FCC ignores that, during an emergency, a customer may not be able to call for help. And the FCC says nothing about the other two exceptions, which permit carriers to disclose call location information to a customer's immediate family "in an emergency situation that involves the risk of death or serious physical harm" or to third parties that process information when "assisting in the delivery of emergency services in response to an emergency." 47 U.S.C. § 222(d)(4)(B)-(C). If device-location information were CPNI, as the FCC claims, carriers could not disclose that information to immediate family or those assisting emergency service providers when a customer is incapacitated and cannot make a call. The FCC attempts no explanation for why Congress would draw such an absurd line.[6]

The same is true of Congress's decision to impose a heightened consent requirement only for call location information, but not also for device-location

[6] Verizon is thus not suggesting, as the FCC implies (at 28), that there is anything absurd about congressional reluctance to create an exception that would permit disclosure of "*all* of the user's location information that may have nothing to do with a present emergency." It is the FCC that has no answer for why Congress would both make device-location CPNI and preclude carriers from disclosing the location of a device during an emergency to immediate family and those assisting first responders.

information (if that were CPNI). The FCC's own amici explain why device-location information, untethered to any calls, has far greater implications for privacy than call location information. *See* EPIC Amicus Br. 15-28. As do a host of news articles.[7] And it is Verizon's recognition of the sensitivity of device-location information — not a belief that it is CPNI, *see* FCC Br. 25 — that leads Verizon to protect that information for the benefit of its customers.

For these reasons, the fact that wireless devices like smartphones maintain a connection to Verizon's network while they are turned on, *see id.* at 24-25, is irrelevant. Information about that connection is not call location information.

In addition, the FCC's argument ignores the record. To generate the location information that Verizon disclosed through its LBS program, Verizon had to specially "ping" the wireless device, "separately from the normal course network communications with customer devices for the purpose of . . . provid[ing] services" to them. Donnellan Decl. ¶ 7 (JA43). If the FCC were correct that Verizon already had that information simply because a device was turned on, the special-purpose pinging would have been unnecessary.

[7] *See*, *e.g.*, Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://nyti.ms/42G0jqV; Jeremy Hsu, *The Strava Heat Map and the End of Secrets*, Wired (Jan. 29, 2018), https://bit.ly/42zPruD.

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

Verizon put in place numerous, multi-layered safeguards to protect its customers' device-location information. *See* Verizon Br. 36-37. Those measures included vetting third parties before allowing them to join the LBS program; limiting participants to preapproved use cases; imposing information security requirements and adherence to industry best practices on participants; reviewing participants' notice-and-consent language; requiring the production of consent records on a daily basis; and retaining a third-party expert (Aegis) to review those consent records, analyze program data to find any potential issues, and otherwise monitor the program and participants. *See id.*

The record demonstrates these safeguards were effective. Over the many years, scores of participants, and hundreds of millions of transactions in Verizon's LBS program, the FCC identified only one participating service provider (Securus) that circumvented Verizon's protections and only 11 affected customers.[8] And after the *New York Times* article, Verizon implemented additional safeguards.

[8] The FCC notes (at 41-42) that Securus made its unauthorized program available to law enforcement for years. But there is no evidence that a single request — other than those Hutcheson submitted — came to Verizon through that unauthorized Securus program. Verizon had well-established procedures for legitimate law enforcement requests for customer location data, which Verizon processed outside the LBS program. *See* Verizon Br. 19 n.6.

Verizon immediately cut off Securus' access to the LBS program; ceased taking new applications; and had Aegis both strengthen the transaction verification process and scrutinize Securus' transaction history to better detect any issues with other participating service providers. *See* Verizon Br. 38.

The fact that Verizon's protections failed as to 11 customers, during [redacted], does not show that Verizon's protections were unreasonable — just that they were not perfect. The FCC "agree[d] with Verizon that section 64.2010 of the Commission's rules requires only reasonable measures — not perfect ones." Forfeiture Order ¶ 58 (JA67). Indeed, while the FCC repeatedly asserts (at 3, 12, 43) that the sheriff obtained device-location information for "hundreds" of people, the fact that only 11 were Verizon customers confirms the effectiveness of Verizon's safeguards.

But the FCC imposed a massive forfeiture penalty anyway. If the FCC truly thought that Securus' and the sheriff's actions "revealed fundamental shortcomings in Verizon's safeguards," Forfeiture Order ¶ 53 (JA66), it would have done *something* when it learned of them more than nine months before Verizon did, *see* Verizon Br. 19-20, 38. The FCC likewise would not have provided what it now calls a "grace period" before imposing fines. *See id.* at 40

n.16. The FCC is silent about its months of inaction and repeats (at 34) — but does not explain or defend — the Forfeiture Order's "grace period" language.[9]

The FCC instead claims (at 3, 11, 22, 41) that a 2017 internal Verizon document identified a weakness in Verizon's protections. But as the Forfeiture Order noted — though the FCC's brief does not — the document concluded that the weakness was theoretical because existing "program management processes and oversight that is in place today" made it "unlikely [that] any current program companies are performing fraudulent activities to obtain [Verizon] subscriber information." Forfeiture Order ¶ 49 (JA65). In addition, Verizon prepared that document after receiving an anonymous allegation that an unidentified bail bonds company had obtained unauthorized access to device-location data through the LBS program. *See* Supp. LOI Resp. 12-13 (JA19-20). Verizon's investigation determined that the company the tipster referenced likely was one that Verizon *rejected* during the vetting process, underscoring the efficacy of Verizon's oversight measures. *Id.* at 12 (JA19).

[9] The NAL did not describe the 30-day period as a "grace period." *See* Verizon Br. 40 n.16; NAL ¶ 87 (JA140). If the FCC in fact decided 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 the FCC offers no defense of such a decision in its brief.

The FCC also suggests (at 40) that the use of a third-party expert (Aegis) to help monitor LBS program participant compliance was itself unreasonable. But relying on a company with special competence in this area is the opposite of unreasonable. That is especially true when Aegis initially matched 99.95% of requests to valid consent records, and then reviewed a statistically significant, randomly selected sample of the remainder that identified no mismatches. *See* Verizon Br. 37. The FCC's focus (at 41-42) on Verizon's contractor's failure to catch the small number of unauthorized requests for 11 Verizon customers' device-location data underscores that the FCC inappropriately seeks "strict liability" where the law requires "*reasonable* care." *SEC v. Rashid*, 96 F.4th 233, 242 (2d Cir. 2024).

Finally, the FCC resorts (at 42-43) to speculation, asserting that "the full extent to which the program was exploited may never be known." That, too, is arbitrary and capricious given the FCC's burden to prove liability. *See Sorenson Commc'ns, Inc. v. FCC*, 755 F.3d 702, 708-09 (D.C. Cir. 2014). The FCC cannot impose nearly $47 million in penalties by throwing up its hands and saying it does not know whether or to what extent bad actors tried to misuse, or successfully misused, Verizon's LBS program.

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

In the Forfeiture Order, the FCC found that Verizon engaged in a single, continuing violation of a single rule: Verizon "failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information" under its LBS program. Forfeiture Order ¶ 46 (JA63); *see id.* ¶ 42 (JA61) (citing 47 C.F.R. § 64.2010(a)). Verizon had one set of LBS program policies, which it applied uniformly to all program participants. Because the FCC found only a "single act or failure to act," the statutory maximum forfeiture the FCC could impose was $2,048,915. 47 U.S.C. § 503(b)(2)(B); 47 C.F.R. § 1.80(b) (2020).

The FCC instead imposed a nearly $47 million forfeiture penalty, by treating that single set of policies as 63 violations. *See* Forfeiture Order ¶¶ 77-86 (JA73-76). And the FCC claimed that it instead "could well have chosen to look to the total number of Verizon subscribers when determining the number of violations," with Verizon's "tens of millions" of subscribers permitting a more than $200 *trillion* fine. *Id.* ¶ 80 (JA74); *see* Chamber Amicus Br. 22.

In its brief, the FCC does not defend the Forfeiture Order's assertion that the agency was equally free to find one, 63, or tens of millions of violations. Nor does the FCC offer an interpretation of the statutory phrase "single act or failure to act." The FCC instead appears to endorse the view — which dissenting Commissioner

Simington rightly found "not plausible" — that "Congress intended that the Commission may arrive at forfeitures of any size simply by disaggregating an 'act' . . . to arrive at whatever forfeiture amount suits a preordained outcome." Forfeiture Order at 46 (JA90).

The FCC's violation count, however creative, conflicts with the statutory text and principles of fair notice. The FCC's few defenses of its count lack merit.

First, the FCC claims (at 45) to have an "established practice" of disaggregating "systemic privacy failings" into many violations. Yet the only example the FCC cites (at 45) is a single 2014 notice of apparent liability, decided by a 3-2 vote, in a case that settled before the FCC ever issued a final, appealable forfeiture order. *See* Verizon Br. 43 n.17 (discussing *TerraCom NAL*). A "single decision . . . hardly constitutes a long-standing and well-established practice." *Carter/Mondale Presidential Comm., Inc. v. FEC*, 775 F.2d 1182, 1185 (D.C. Cir. 1985); *cf. Barwin v. Vill. of Oak Park*, 54 F.4th 443, 460 (7th Cir. 2022) ("Single, isolated, or sporadic incidents are typically rejected as insufficient to establish a past practice."). In addition, an interpretation first adopted nearly 20 years after Congress enacted § 222 and not followed for another six years is not the kind of contemporaneous, consistent agency interpretation that can be entitled to "respect." *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 386 (2024).

Second, the FCC asserts (at 46) that, because Verizon individually vetted and approved each LBS program participant, it was reasonable to count each participant as a separate violation. But the Forfeiture Order did not find that the LBS program intake process violated § 222 or any FCC rule. Instead, the FCC took issue with Verizon's subsequent "measures to discover and protect against attempts to gain unauthorized access" to device-location data by or through those in the program. Forfeiture Order ¶ 46 (JA63). The FCC does not claim that those measures differed by participant; the record shows they did not. *See* Verizon Br. 42. It therefore "cannot credibly be argued that" those measures constitute "more than one act relevant for the purposes of forfeiture calculation." Forfeiture Order ¶ 46 (JA90) (Commissioner Simington, dissenting).

Finally, the FCC complains (at 47) that the statutory maximum is "insignificant in view of Verizon's $134 billion in annual operating revenues." But such a "policy argument . . . is properly addressed to Congress." *SAS Inst., Inc. v. Iancu*, 584 U.S. 357, 358 (2018); *see also United States v. Razmilovic*, 419 F.3d 134, 141 (2d Cir. 2005) (emphasizing that a policy argument against applying clear "statutory language . . . is a complaint that should be addressed to Congress"). The FCC's dissatisfaction with Congress's limits is not license to ignore them.

IV. THE FORFEITURE ORDER VIOLATES THE SEVENTH AMENDMENT

A. *Jarkesy* Controls Here

As the Supreme Court explained in *Jarkesy*, when deciding whether the Seventh Amendment applies to a statutory claim, the existence of a monetary sanction "designed to punish and deter" is "all but dispositive" and "effectively decides" the matter. *SEC v. Jarkesy*, 603 U.S. 109, 123, 125 (2024). Here, the FCC does not — and cannot — dispute that the Forfeiture Order imposes a punitive monetary sanction. *See* Verizon Br. 45; CTIA Amicus Br. 27; Chamber Amicus Br. 8-9.

The FCC instead disputes the existence of a close relationship between the Forfeiture Order and common-law causes of action. *See* FCC Br. 55-60. But in *Jarkesy*, the Supreme Court reaffirmed that the nature of the "remedy [is] the more important consideration." 603 U.S. at 123; *see also Tull v. United States*, 481 U.S. 412, 421 n.6 (1987) ("reject[ing]" the government's argument that "both the cause of action and the remedy must be legal in nature"). The Court looked to common-law analogs merely to "confirm[ ] th[e] conclusion" it had already reached from the punitive remedy: that the SEC's enforcement action "implicates the Seventh Amendment." 603 U.S. at 125. Nothing in *Jarkesy* suggests the result would have been different if the relationship between the SEC's administrative enforcement and a common-law fraud claim were more attenuated.

In any event, the same kind of close relationship the Court found in *Jarkesy* does exist here. Section 222 provides statutory protection for the privacy of certain information that customers buying voice service provide to telecommunications carriers. The Video Privacy Protection Act similarly provides statutory protection for the privacy of certain information that customers buying or renting video tapes provide to video stores.[10] This Court found that statutory protection to be "closely related to at least one common-law analog . . . : public disclosure of private facts." *Salazar v. NBA*, 118 F.4th 533, 540 (2d Cir. 2024). Similarly, the Eleventh Circuit recently found that another privacy-protecting provision in the Communications Act — this one involving unconsented-to telemarketing calls, *see* 47 U.S.C. § 227(b)(3), rather than unconsented-to disclosure of CPNI — draws upon common-law concepts as well. *Ins. Mktg. Coal. Ltd. v. FCC*, – F.4th –, 2025 WL 289152, at *6 (11th Cir. Jan. 24, 2025). These cases confirm that the privacy protections in § 222 have a sufficiently close relationship to common-law analogs. *Jarkesy* does not require the analog to be "identical" — it may be "narrower" in

[10] That protection is civil, not criminal as the FCC claims (at 59). Congress created a private right of action with statutory damages to enforce the law. *See* 18 U.S.C. § 2710(c). And information about the telephone calls a person makes is at least as "inherently sensitive personal information," FCC Br. 59, as a list of the movies that person rented.

"some respects" and "broader" in others. 603 U.S. at 126; *see also Tull*, 481 U.S. at 421 ("precisely analogous common-law cause of action" not required).

Nor does the FCC's Forfeiture Order fit within the public rights exception to the Seventh Amendment. As *Jarkesy* explains, that exception is limited and covers matters like federal revenue collection, customs enforcement, immigration, relations with Indian tribes, administration of public lands, and the granting of public benefits. *See* 603 U.S. at 128-30. The protection of customers' private information resembles none of those. While the FCC notes (at 61) that spectrum licenses convey public rights, the statutory provisions governing those licenses are in Title III of the Communications Act. *See* 47 U.S.C. § 301 *et seq.* Section 222 does not regulate the public wireless spectrum. Although the privacy obligations in § 222 apply only to common carriers, nearly all companies are subject to comparable federal and state privacy obligations governing their customers' sensitive information.

B. Section 504(a) Does Not Satisfy the Seventh Amendment

Parties hit with a forfeiture order such as the one here have two options: (1) pay the penalty and appeal or (2) refuse to pay and wait for the Department of Justice to bring a collection suit under 47 U.S.C. § 504(a).[11] The mere existence of

[11] The FCC implies (at 5) that the first option may be unavailable, and this Court might not have jurisdiction to entertain a petition for review. But as the FCC notes, the D.C. Circuit held in a persuasive opinion that courts of appeals have

the second option does not cure the Forfeiture Order's constitutional problem for two reasons.

First, the Forfeiture Order is not like a complaint that starts a case in federal district court. The Forfeiture Order is not an allegation of liability. It is final agency action and determination on the merits. It "order[s]" that Verizon "is liable for a monetary forfeiture" and that "[p]ayment of the forfeiture shall be made . . . within thirty (30) calendar days." Forfeiture Order ¶¶ 102-103 (JA83) (cleaned up). The FCC's assertion (at 51) that Verizon is "under no obligation to pay" ignores that mandatory language.

The FCC is also wrong in asserting (at 49-50) that Verizon would suffer no harm if it flouted the Forfeiture Order's mandatory language. The Forfeiture Order "constitutes an official government determination that [Verizon] is a lawbreaker." Chamber Amicus Br. 16-17. Verizon also must account for the associated liability on its books, impacting its future planning and budgeting. The FCC will use

---

jurisdiction under 47 U.S.C. § 402(a) over petitions for review of forfeiture orders if the petitioner has paid the penalty. *See AT&T Corp. v. FCC*, 323 F.3d 1081, 1083-85 (D.C. Cir. 2003). While the FCC argued against jurisdiction there, it later endorsed the D.C. Circuit's decision to this Court, *see* FCC Br. 1, *ABC, Inc. v. FCC*, No. 08-0841 (2d Cir. filed Aug. 22, 2008), https://bit.ly/3WI4uOT, and this Court exercised jurisdiction, *see ABC, Inc. v. FCC*, 404 F. App'x 530, 531 (2d Cir. 2011) (summary order).

factual findings in a Forfeiture Order — before any § 504(a) trial occurs[12] — as a basis for increasing forfeiture penalties in future orders or for denying requests to transfer licenses. *See id.* at 17-18; Verizon Br. 51-52. Verizon would also have to disclose an unpaid Forfeiture Order when seeking some government contracts. *See* Verizon Br. 51-52.

Second, Verizon is subject to nationwide venue if it does not pay and the DOJ sues to collect, a point which the FCC does not dispute or address. *See id*. at 49 (citing 47 U.S.C. § 504(a)). The DOJ can therefore choose to sue Verizon in a jurisdiction where the court of appeals has already decided that defendants may not challenge FCC legal rulings. The Fifth Circuit, for example, has held that § 504(a) "permits . . . an opportunity to present a factual defense to enforcement of the forfeiture," but not "to challenge the legal validity of a forfeiture order." *United States v. Stevens*, 691 F.3d 620, 622-23 (5th Cir. 2012). It is not mere "speculation" that a district court following *Stevens* would prevent Verizon from making the legal arguments in Parts I and III of this brief. FCC Br. 52.[13] And a

[12] As the Chamber of Commerce notes (at 12), no § 504(a) trial has occurred in at least 50 years.

[13] Nor can *Stevens* be distinguished on the ground that the Stevenses did not challenge the factual basis for the forfeiture. *See* FCC Br. 53. The district court there held that it lacked "jurisdiction to consider . . . legal challenges," and the Fifth Circuit agreed — the presence of factual disputes would not have expanded the Fifth Circuit's view of district court's jurisdiction over legal challenges. *Stevens*, 691 F.3d at 621.

jury trial in which the DOJ can dictate the issues and jury instructions — with the court powerless to reject the FCC's erroneous interpretations of the CPNI definition and the maximum forfeiture amount — is not one the Seventh Amendment recognizes.

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.

Respectfully submitted,

/s/ *Scott H. Angstreich*
Scott H. Angstreich
Aaseesh P. Polavarapu
Daren G. Zhang
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
dzhang@kellogghansen.com

Counsel for Petitioner Verizon Communications Inc.

February 7, 2025

CERTIFICATE OF COMPLIANCE

I certify, pursuant to Federal Rule of Appellate Procedure 32(g), that this reply 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 6,057 words.

I further certify that this reply 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.

February 7, 2025

CERTIFICATE OF SERVICE

I hereby certify that, on February 7, 2025, an electronic copy of the redacted Reply 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.