United States Court of Appeals
For the Second Circuit

August Term 2024
Argued: April 29, 2025
Decided: September 10, 2025

No. 24-1733

VERIZON COMMUNICATIONS INC.,

Petitioner,

v.

FEDERAL COMMUNICATIONS COMMISSION,

UNITED STATES OF AMERICA,

Respondents.[*]

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

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

Before: Lynch, Lee, and Nathan, *Circuit Judge*s.

Verizon Communications Inc. (Verizon) petitions for review of a forfeiture order of the Federal Communications Commission (FCC) imposing a $46.9 million penalty for violating § 222 of the Communications Act and its implementing regulations. The FCC imposed the forfeiture due to Verizon's purported failure to reasonably safeguard a category of statutorily protected information known as "customer proprietary network information."

On appeal, Verizon argues that (1) § 222 does not cover device-location data, (2) the FCC's liability finding was arbitrary and capricious, (3) the penalty exceeds the statutory cap, and (4) the imposition of the forfeiture, without a jury trial, violated its Seventh Amendment rights.

We conclude that device-location data is statutorily protected, that the FCC reasonably determined Verizon's liability, and that the forfeiture order neither violates the applicable statutory limits nor Verizon's asserted Seventh Amendment rights. Accordingly, we **DENY** the petition.

SCOTT H. ANGSTREICH (Aaseesh P. Polavarapu, *on the brief*), Kellogg, Hansen, Todd, Figel & Frederick, PLLC, Washington, D.C., *for Petitioner*.

SCOTT M. NOVECK, Counsel (P. Michele Ellison, General Counsel, Jacob M. Lewis, Deputy General Counsel, Sarah E. Citrin, Deputy Associate General Counsel, *on the brief*), *for Respondent Federal Communications Commission*;

Doha G. Mekki, Acting Assistant Attorney General, Robert B. Nicholson, Matthew A. Waring, Attorneys, *on the brief*, U.S. Department of Justice, Washington, D.C., *for Respondent United States of America.*

NATHAN, *Circuit Judge*:

In the wake of news reporting about Verizon Communications Inc.'s (Verizon) mishandling of its customers' location data, the Federal Communications Commission (FCC or the Commission) commenced an enforcement action against the company. Exercising its authority to pursue monetary forfeitures, *see* 47 U.S.C. § 503(b)(1)(B), (b)(4), the Commission preliminarily concluded that Verizon violated § 222 of the Communications Act and § 64.2010 of

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

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

We disagree. The customer data at issue plainly qualifies as customer proprietary network information, triggering the Communication Act's privacy protections. And the forfeiture order both soundly imposed liability and remained within the strictures of the penalty cap. Nothing about the Commission's proceedings, moreover, transgressed the Seventh Amendment's jury trial

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

guarantee. Indeed, Verizon had, and chose to forgo, the opportunity for a jury trial in federal court. Thus, we **DENY** Verizon's petition.

BACKGROUND

I. Legal Background

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

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

One such form of protected customer data is customer proprietary network information. This category of information is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." *Id.* § 222(h)(1)(A). By statute, a carrier "shall only use, disclose, or

permit access to individually identifiable customer proprietary network information" to provide "the telecommunications service from which such information is derived" or "services necessary to, or used in" providing that service "[e]xcept as required by law or *with the approval of the customer*." *Id.* § 222(c)(1) (emphasis added).

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

Congress authorized the FCC to enforce § 222 and the agency's rules through monetary forfeitures. *See* 47 U.S.C. § 503(b)(1)(B). Section 503(b) of the Communications Act provides two routes by which the Commission may pursue such a forfeiture. *See AT&T Corp. v. Fed. Commc'ns Comm'n*, 323 F.3d 1081, 1083 (D.C. Cir. 2003). Under § 503(b)(3), the FCC may initiate a formal adjudication before an administrative law judge (ALJ) or the Commission itself. 47 U.S.C. § 503(b)(3)(A). Any resulting forfeiture order is reviewable in a court of appeals. *Id.* "If the penalty remains unpaid once the forfeiture determination becomes final, the United States may bring a collection action in district court." *AT&T Corp.*, 323 F.3d at 1083 (citing 47 U.S.C. § 503(b)(3)(B)).

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

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

II. Factual Background

Petitioner Verizon provides its customers with mobile-voice and data services through its wireless network. To enable a customer

[3] This is the first time in a published opinion that we have stated that, as long as the carrier pays the forfeiture amount, courts of appeals have jurisdiction to review a forfeiture order issued pursuant to § 503(b)(4). The parties do not dispute that Verizon's payment of the forfeiture amount preserves our jurisdiction to review the FCC's forfeiture order. In any event, we find that, for the reasons articulated by the D.C. Circuit in *AT&T Corp.*, 323 F.3d at 1084–85, we have jurisdiction to review Verizon's appeal.

to make and receive calls and to transmit data, customers' devices and a carrier's cell towers must regularly exchange information, which we refer to as "pinging" each other. Because carriers know the locations of their towers, and because customers typically carry their phones on their person or nearby, carriers like Verizon generally know their customers' location at all times.

Until March 2019, Verizon, like many other carriers, ran a "location-based services" program that sold access to certain kinds of wireless customer location data. As part of that program, Verizon contracted with "location information aggregators," which collected customer data and resold it to third-party location-based services providers. Verizon had arrangements with two aggregators, LocationSmart and Zumigo, which in turn contracted with 63 third-party entities.[4] These entities purportedly used customer location data for six specific types of purposes or "[u]se [c]ases": "call routing, roadside assistance, proximity marketing, transportation and logistics, fraud mitigation/identity management, and mobile gaming/lottery." *In re Verizon Commc'ns*, No. 24-41, 2024 WL 1905229, at *4 (F.C.C. Apr. 29, 2024) (quotation marks omitted).

Verizon did not itself provide notice and obtain or verify consent to access customer location data. Rather, it largely delegated those functions via contract. Verizon's contracts with the aggregators, for example, required that location-based services providers give notice and seek affirmative, opt-in consent before accessing customer

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

information. And prior to joining the program, providers had to submit an application describing the company's intended use case and its notice-and-consent process. To verify that customers were indeed consenting to disclosure of their data, Verizon relied primarily on an external auditor, Aegis Mobile, LLC, which collected and matched customer location requests and consent events on a daily basis.[5] Both sets of records were submitted to Aegis by the aggregators, who in turn collected them from the third-party providers. If a contracting party failed to meet Verizon's standards, Verizon could cut off access to customer location data at any time.

On May 10, 2018, the *New York Times* published an article reporting security breaches involving Verizon's (and other major carriers') location-based services program. According to the *New York Times*, a company called Securus Technologies, Inc. (Securus) was misusing the program to enable law enforcement officers to access location data *without* customers' knowledge or consent, so long as the officers uploaded a warrant or some other legal authorization. But, as Verizon concedes, Securus had been approved for a different use case altogether. And because Securus did not actually review the documents that law enforcement personnel uploaded, a now-former Missouri sheriff, Cory Hutcheson, was able to access customer data with no legal process at all. Instead of providing warrants or other legal authorization, Hutcheson uploaded utterly irrelevant materials, such as "his health insurance policy, his auto insurance policy, and pages selected from Sheriff training materials." *Verizon Commc'ns*,

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

2024 WL 1905229, at *5 (quotation marks omitted).

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

Soon after the *New York Times* article, the FCC's Enforcement Bureau launched an investigation into Verizon's location-based services program. And in February 2020, the Commission issued Verizon a Notice of Apparent Liability for its apparent violations of § 222 of the Communications Act and § 64.2010 of the agency's regulations by failing to protect its customers' proprietary network information. After considering Verizon's responses, the Commission affirmed the notice and issued a forfeiture order.

In that order, the FCC concluded that the location data disclosed through Verizon's location-based services program is protected as customer proprietary network information under § 222. And it found that Verizon failed to reasonably protect that information both before and after the Securus/Hutcheson disclosures. Basing its penalty on Verizon's post-disclosure conduct, the

Commission determined that Verizon engaged in 63 continuing violations of § 222 and its implementing regulations: one for each ongoing relationship with an aggregator or location-based services provider that retained access to customer data more than 30 days after publication of the *New York Times* article.[6] It also applied a 50% upward adjustment on top of the base forfeiture amount for, among other things, "egregious" conduct, and it rejected Verizon's constitutional challenges to the forfeiture order. In the end, Verizon was directed to pay $46.9 million within 30 days of the order.

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

STANDARD OF REVIEW

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

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

[6] The FCC's original calculation of the forfeiture included two companies which, as explained above, *see supra* p. 8 n.4, never participated in the location-based services program. But upon Verizon's clarification, the FCC exercised its discretion to exclude these two entities and reduce the forfeiture amount accordingly.

DISCUSSION

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

I. Scope of § 222

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

Section 222(h)(1)(A) defines customer proprietary network information as including "*information that relates to the* quantity, technical configuration, type, destination, *location*, and amount of use *of a telecommunications service* subscribed to by any customer of a telecommunications carrier, and that is *made available to the carrier by the customer solely by virtue of the carrier-customer relationship*." 47 U.S.C. § 222(h)(1)(A) (emphasis added). Thus, to qualify as customer proprietary network information, customer location data must meet two conditions. First, the information must "relate[] to

the . . . location . . . of a telecommunications service." *Id.*[7] And second, the information must be "made available to the carrier . . . solely by virtue of the carrier-customer relationship." *Id.* Device-location data comfortably satisfies both conditions.

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

[7] One of Verizon's amici, CTIA – The Wireless Association (CTIA), but not Verizon, argues that the statute is best read to define customer proprietary network information as that which "relates to the . . . location . . . *of use* of a telecommunications service." 47 U.S.C. § 222(h)(1)(A) (emphasis added). Pursuant to the rule of the last antecedent, however, "a limiting . . . phrase . . . should ordinarily be read as modifying only the noun or phrase that it immediately follows." *Lockhart v. United States*, 577 U.S. 347, 351 (2016) (quotation marks omitted). Although the rule is not absolute and can be overcome by context, *id.*, the context here supports rather than undermines the application of the rule. Reading the phrase "of use" as modifying each category of enumerated information, as opposed to just the word "amount," would create unnecessary anomalies. For example, it would make little sense to read § 222(h)(1)(A) to refer to the "technical configuration . . . of use of a telecommunications service." 47 U.S.C. § 222(h)(1)(A). Moreover, if we were to adopt CTIA's preferred construction, there would be no principled distinction between the statute's references to "quantity of use" and "amount of use," rendering one of those phrases surplusage. *See Quantity*, BLACK'S LAW DICTIONARY (12th ed. 2024) (defining "quantity" as "[t]he amount of something measurable"). By contrast, if "of use" only modifies "amount," we can more readily interpret "quantity . . . of a telecommunications service" as referring to, for example, how many phone lines a customer has purchased, and "amount of use" of such a service as referring to, for example, the number and length of that customer's calls. Since "we construe statutes to avoid surplusage," *Perez v. Westchester Cnty. Dep't of Corr.*, 587 F.3d 143, 155 (2d Cir. 2009), the better reading of § 222(h)(1)(A) is that, to qualify as customer proprietary network information, the information must "relate[] to the . . . location . . . of a telecommunications service," not to the "location . . . of use" of such a service. 47 U.S.C. § 222(h)(1)(A).

owned by a customer who was not using or did not purchase any voice service (e.g., a customer who had a data-only plan, which is not a telecommunications service under the statute, *see infra* p. 15 & n.9). For this reason, Verizon claims, the location-based services program "relates to" "only the location of a device, not of a telecommunications service." *Id.*

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

Verizon suggests that this argument "ignores the record," because to generate the location information that Verizon sold through its location-based services program, the company had to

[8] We would reach the same conclusion even if we construed "of use" to modify all terms in the statutory definition of customer proprietary network information, *see supra* p. 12 n.7, since, as the Commission reasoned, "[w]hen customers' devices are exchanging communications with Verizon's network, and thereby ensuring that they can receive incoming calls and place outgoing calls," they are clearly "using the [telecommunications] service to which they have subscribed, even outside the moments in time when they are engaged in calls." *Verizon Commc'ns*, 2024 WL 1905229, at *9.

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

Verizon also draws on statutory context and legislative history to support its theory that § 222(h)(1)(A) embraces only call-location information. But its arguments are inconclusive at best and, in any event, cannot override the statute's plain meaning.

By way of background, when Congress enacted the Telecommunications Act in 1996, "location" was not included in the definition of customer proprietary network information. That was

[9] For the same reason, and for reasons explained more fully below, *see infra* pp. 18–20, we reject the argument, to the extent that Verizon makes it, that for data-only customers, the device-location at issue in this case is not "related to" a telecommunications service because the provision of data services is not a telecommunications service under the statute.

added in 1999, along with other amendments to § 222, via the Wireless Communications and Public Safety Act, Pub. L. No. 106–81, § 5(3), 113 Stat. 1286, 1289 (1999). As part of those amendments, Congress crafted a new exception to § 222(c)(1)'s prohibition on the nonconsensual use, disclosure, or access to customer proprietary network information. This exception allows carriers to disclose "call location information," without customer consent, to various emergency services providers and to family members in an emergency involving a risk of death or serious physical harm. 47 U.S.C. § 222(d)(4). Congress also clarified that, in the context of "call location information," consent for purposes of § 222(c)(1) means "express prior authorization." *Id.* § 222(f)(1).

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

Even assuming that those results reflect contrary assumptions about the sensitivity of device-location data, Verizon's arguments

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

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

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

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

[10] Verizon's wireless data services—text messaging and Internet access—are presently regulated as non-common-carrier information services and private mobile services. *See Petitions for Declaratory Ruling on Regul. Status of Wireless Messaging Serv.*, 33 FCC Rcd. at 12082, 12090–94 (text messaging); *Restoring Internet Freedom*, 33 FCC Rcd. 311, 312, 322–34

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

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

To be sure, the Communications Act treats regulated parties as

---

(2018) (broadband Internet access). Although the FCC sought to reclassify broadband Internet access in 2024, *see Safeguarding & Securing the Open Internet Restoring Internet Freedom*, No. 24-52, 2024 WL 2109860, at *3–4 (F.C.C. May 7, 2024), the Sixth Circuit set aside the order earlier this year, *see In re MCP No. 185*, 124 F.4th 993, 1001, 1013 (6th Cir. 2025). *See also N.Y. State Telecomms. Ass'n*, 101 F.4th at 140–41 (discussing the prior reclassifications of broadband Internet access and its regulatory consequences).

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

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

II. Liability Finding

In the alternative, Verizon contends that the FCC's determination that Verizon did not reasonably protect customers' location data was arbitrary and capricious. "However, an agency's decision is arbitrary and capricious only if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an

explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise." *Safe Haven Home Care, Inc. v. U.S. Dep't of Health & Hum. Servs.*, 130 F.4th 305, 323 (2d Cir. 2025) (cleaned up). That was not the case here.

Section 503(b) provides that a person shall be liable for forfeiture for "willfully or repeatedly fail[ing] to comply with any of the provisions of" the Communications Act or rules promulgated by the FCC. 47 U.S.C. § 503(b)(1)(B).[11] In the forfeiture order, the FCC determined that Verizon failed to reasonably protect customer proprietary network information before and after the Securus/Hutcheson disclosures, thereby violating § 222 and § 64.2010 of the agency's rules.

Verizon's challenge to this determination stems from its view that the Securus/Hutcheson disclosures were outlier occurrences that affected a small number of customers and do not speak to any broader systemic issues in its safeguards. Thus, Verizon argues, instead of reasonable measures, the FCC required perfect ones, imposing, without fair notice, a strict liability standard "contrary to the reasonableness standard" in the FCC rule. Pet. Br. at 40 (quotation marks omitted). At bottom, Verizon asks us to find that it was arbitrary and capricious for the FCC to refuse to infer the reasonableness of Verizon's safeguards based on the fact that only the Securus/Hutcheson breaches were publicly identified. But the

[11] For obligations under the Communications Act, "'willful', when used with reference to the commission or omission of any act, means the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision" or FCC rule. 47 U.S.C. § 312(f)(l).

Commission "reasonably considered the relevant issues and reasonably explained the decision" to reject that position. *Fed. Commc'ns Comm'n v. Prometheus Radio Project*, 592 U.S. 414, 423 (2021).

As to the period before the Securus/Hutcheson disclosures, the FCC considered the safeguards that Verizon had in place and reasonably found them wanting. In reaching this decision, the agency explained that Verizon relied heavily on a chain of contractual arrangements to satisfy its statutory and regulatory obligations. And it observed that, to enforce its contractual safeguards, Verizon's efforts "apparently mainly consisted of analysis of unverified vendor-created consent records" (through Aegis). *Verizon Commc'ns*, 2024 WL 1905229, at *16 (quotation marks omitted). Specifically, Aegis's review consisted essentially of comparing the list of "location requests" provided by a location-based services provider with the list of purported "consent records" *also provided by the provider*, a system that "assumed that the location requests and consent records provided by the [providers] would be legitimate in the first instance" and could not detect if a provider fabricated the consent records. *Verizon Commc'ns*, 35 FCC Rcd. 1698, 1719 (2020). A 2017 internal report, which warned Verizon that "it is possible for [providers] with delegated consent to falsify consent records and obtain [Verizon] subscriber data without their consent," shows that the company was on notice of this possibility. *Verizon Commc'ns*, 2024 WL 1905229, at *4 (quotation marks omitted) (second alteration in original).

The FCC also emphasized that although allegedly designed to monitor customer consents, Verizon's system was incapable of detecting customers' lack of consent, since the Securus location

requests expressly sought to obtain customer location data without customers' approval. This was, in the agency's view, a "significant loophole." *Id.* at *17. Verizon complains that its failure to identify the 11 customers whose data was improperly accessed by Hutcheson "hardly shows" the existence of any "significant loophole" in its procedures. Pet. Br. at 5.[12] But even if the unauthorized disclosures themselves were not so numerous, it was appropriate for the FCC to consider, in assessing the reasonableness of Verizon's safeguards, that the Securus/Hutcheson requests did not raise *any* red flags despite the fact that they were submitting the opposite of consent records to a system whose central conceit was obtaining customer consent.

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

Second, and more importantly, as to Verizon's response to the Securus/Hutcheson breaches, Verizon again reiterates the measures it

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

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

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

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

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

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

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

III. Forfeiture Amount

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

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

disagree.

In authorizing the FCC to assess forfeitures, Congress set maximum forfeiture amounts. As applicable here, the Communications Act caps the total per-violation forfeiture amount at approximately $200,000 for "each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed" approximately $2 million, as adjusted for inflation, "for any single act or failure to act" that violates the statute or FCC rules. 47 U.S.C. § 503(b)(2)(B); *see also* 47 C.F.R. § 1.80(b)(2), (b)(9)(ii) (2020); *Amend. of Section 1.80(b) of the Comm'n's Rules Adjustment of Civ. Monetary Penalties to Reflect Inflation*, 34 FCC Rcd. 12824, 12828 (2019). Thus, for any given continuing violation, the Act authorizes the FCC to impose a penalty of up to $200,000 for each successive day, so long as the aggregate penalty for any "single act or failure to act" does not exceed $2 million. 47 U.S.C. § 503(b)(2)(B); *Amend. of Section 1.80(b) of the Comm'n's Rules Adjustment of Civ. Monetary Penalties to Reflect Inflation*, 34 FCC Rcd. at 1828. In determining the amount of the forfeiture penalty, the FCC must consider "the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require." 47 U.S.C. § 503(b)(2)(E).

As previewed above, the FCC found that Verizon "engaged in [63] continuing violations—one for each ongoing relationship with a third-party . . . provider or aggregator that had access to Verizon customer location information more than 30 days after publication of the *New York Times* report—and that each violation continued until

Verizon terminated the corresponding entity's access to customer location information." *Verizon Commc'ns*, 2024 WL 1905229, at *22. In challenging this result, Verizon and its amici contend that the FCC's findings support at most a "single act or failure to act" warranting a forfeiture: that, in maintaining "one set" of flawed policies, it "failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information." Pet. Br. at 42 (quotation marks omitted) In its view, the maximum forfeiture penalty the FCC could impose was about $2 million, *not* nearly $47 million.

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

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

limits[,] . . . ensuring the agency has engaged in reasoned decisionmaking within [the] boundaries [of the authority delegated to it]." *Id.* at 395 (quotation marks omitted).

Here, although Verizon and its amici are correct that determining Verizon's total number of violations involves a question of statutory interpretation, they misidentify the relevant question. The Communications Act does not specifically articulate what qualifies as a "single act or failure to act." Rather, the Act gives the Commission "the discretion" to determine when to issue a forfeiture penalty against a carrier. 47 U.S.C. § 503(b)(3)(A). And when the Commission does issue a penalty, the Act gives the Commission the discretion, within a statutory cap, to determine its amount. *Id.* § 503(b)(2)(B), (E). It also empowers the Commission to determine when someone has "willfully or repeatedly failed to comply with [the Communications Act]." *Id.* § 503(b)(1)(B). Those delegations of authority make sense in the context of the FCC's remedial scheme: because the agency is close to the facts, it is best positioned to determine what, under any given set of circumstances, qualifies as a single violation. So the relevant statutory interpretation question is whether, under the Communications Act, the FCC has the discretion to determine, within reasonable "boundaries," *Loper Bright*, 603 U.S. at 395, when a carrier has engaged in a single violation of the Act. Because the Communications Act explicitly grants the Commission the discretion to determine what qualifies as a violation of the Act, when to issue a forfeiture penalty for violations, and what the size of that forfeiture penalty would be, we conclude, on *de novo* review, that the agency has the authority to determine, within reasonable

boundaries, what qualifies as a "single act or failure to act," for the purpose of remaining within the statutory cap. 47 U.S.C. § 503(b)(2)(B). In short, we are not deferring to the agency's interpretation of the statute. Instead, we conclude—based on our own independent analysis of the statute—that the Communications Act vests the agency with some discretion to select, from a reasonable range of possibilities, the unit of prosecution that can be considered a single violation of the Act under particular circumstances.

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

Verizon may have had one overarching set of flawed policies, which insufficiently protected customer proprietary network information, but those policies were implemented through separate relationships with 63 different entities. Verizon approved and terminated each entity's participation separately. In the weeks following the Securus/Hutcheson disclosures, it had the choice of shoring up its demonstrably flawed safeguards or else cutting off access not just for Securus and 3Cinteractive but also for any one of the other entities that continued to receive customer location data

without adequate safeguards. Its failure to take either of these paths means that each of its ongoing relationships represented an additional risk of security breaches. That is enough to render Verizon's decision to continue selling location data to 63 entities under essentially the same system that produced the Securus/Hutcheson disclosures 63 individual "act[s] or failure[s] to act." 47 U.S.C. § 503(b)(2)(B). Thus, consistent with the FCC's conclusion, Verizon committed 63 continuing violations of § 222 of the Communications Act and § 64.2010 of the FCC's rules.

Verizon and its amici complain that the FCC's interpretation of the statute leads to absurd results. But it's Verizon's approach that makes little sense. In the course of securing customers' data, a regulated party will make many decisions, which will in turn have various ramifications on any number of sub-decisions and any number of potential victims. As we have explained, Verizon made a series of decisions that had various consequences. For example: Verizon relied on a chain of contractual arrangements to satisfy its statutory and regulatory obligations, rather than satisfying those obligations directly itself. It insufficiently validated customer consent records and did not have a system in place that could detect a lack of customer consent. And it took few additional measures after the Securus/ Hutcheson breach to remedy the shortcomings in its data protection systems. *See supra* pp. 21–25. Considering that set of circumstances, we have little trouble concluding that the FCC acted within the boundaries of the discretion that Congress delegated to it when it concluded that Verizon committed 63 continuing violations.

Moreover, the purpose of the FCC's forfeiture penalties is to

meaningfully deter and punish violations of the statute. Indeed, in setting the forfeiture amount, the FCC must consider several factors that "concern culpability, deterrence, and recidivism," *Sec. & Exch. Comm'n v. Jarkesy*, 603 U.S. 109, 123–24 (2024), such as the "gravity of the violation," "the degree of culpability," and "any history of prior offenses," 47 U.S.C § 503(b)(2)(E). Forfeitures are also "payable into the Treasury of the United States," which further confirms their deterrent and punitive, as opposed to remedial, function. *Id.* § 504(a). Section 503's legislative history supports this conclusion as well. *See Commission's Forfeiture Pol'y Statement & Amend. of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines (Forfeiture Pol'y Statement)*, 12 FCC Rcd. 17087, 17097 (1997). And yet, interpreting the statutory cap to insulate systemic privacy failures from anything more than a single capped penalty would do little to deter or punish telecommunications giants like Verizon, even with the maximum, approximately $2 million penalty. Given that Congress directed the Commission to consider a violator's "ability to pay" in calculating the forfeiture amount, 47 U.S.C. § 503(b)(2)(E), we doubt that it intended such a result.[14]

Verizon and its amici's complaints of absurdity stem largely from the FCC's claim that the agency's approach was not only lawful but also "eminently *conservative*," as it could have chosen to calculate the number of violations based on "the total number of Verizon subscribers"—"tens of millions"—"whose highly sensitive location

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

information was made vulnerable by Verizon." *Verizon Commc'ns*, 2024 WL 1905229, at *26. But the legality of this methodology is not before us. And, in any event, finding in favor of the FCC here does not mean countenancing the imposition of a penalty in the hundreds of trillions.

To the extent amici also rely on *United States v. WIYN Radio, Inc.*, 614 F.2d 495 (5th Cir. 1980), that decision does not bind our Court. But even if it did, the FCC's interpretation does not run counter to its holding. Indeed, that case focuses on the distinction between single and continuing violations and does not address when or whether the FCC might impose penalties for various continuing violations. *See id.* at 497 (holding that a licensee's failure to provide the required notice of a personal attack on a broadcast was not a repeated violation for which successive daily penalties could be exacted because the rule at issue imposed a "single, pointed duty" that "admitt[ed] of only a single dereliction" once the week-long period to give notice elapsed). Thus, we find that the FCC acted within the limits of its authority when it determined that Verizon engaged in 63 separate failures to implement a reasonable data-security regime in violation of § 222 of the Communications Act and § 64.2010 of the FCC's rules.

Finally, we conclude that Verizon forfeited on appeal any challenge to the FCC's upward adjustment of the forfeiture order amount. Before the Commission, Verizon brought a second objection to the size of the penalty imposed. It argued that the agency's 50% upward adjustment on top of the base forfeiture amount was unwarranted. *See Verizon Commc'ns*, 2024 WL 1905229, at *23. But "we rely on the parties to frame the issues for decision" on appeal.

United States v. Sineneng-Smith, 590 U.S. 371, 375 (2020) (quoting *Greenlaw v. United States*, 554 U.S. 237, 243 (2008)). And an appellant—or petitioner—who fails to raise an argument in his opening brief generally "forfeits" that argument. *Tripathy v. McKoy*, 103 F.4th 106, 118 (2d Cir. 2024).

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

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

IV. Seventh Amendment

Verizon and its amici lastly contend that the FCC's decision to

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

The Seventh Amendment provides that, "[i]n Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved." U.S. CONST. amend. VII. Verizon and its amici's arguments that the FCC violated this constitutional mandate rest on the Supreme Court's recent decision in *Securities & Exchange Commission v. Jarkesy*. There, the Court held that the Securities and Exchange Commission (SEC) could not, consistent with the Seventh Amendment, adjudicate securities fraud claims seeking civil penalties "in-house" before an ALJ "rather than before a jury in federal court." *See Jarkesy*, 603 U.S. at 115. "The Seventh Amendment," the Court explained, "extends to a particular statutory claim if the claim is 'legal in nature,'" which requires examining the cause of action and the remedy it provides. *Id.* at 122–23 (quoting *Granfinanciera, S.A. v. Nordberg*, 492 U.S. 33, 53 (1989)). And, the Court found, because the SEC's action in *Jarkesy* was "legal in nature," it required a jury trial. *Id.* at 126.

We may assume for the sake of argument that Verizon has a Seventh Amendment right to trial by jury on the charges here. Nevertheless, there is no Seventh Amendment problem here, because Verizon could have gotten such a trial. The remedial structure of the Communications Act differs significantly from the securities statutes that the Supreme Court considered in *Jarkesy*. *See* 603 U.S. at 115–18 (explaining the remedial structure imposed by the three securities

fraud statutes that were relevant to the disposition of the case). When the FCC imposes a forfeiture under § 503(b)(4) of the Communications Act, the statute directs that the penalty "shall be recoverable pursuant to Section 504(a)." 47 U.S.C. § 503(b)(4). And § 504(a), in turn, requires the government to enforce any penalty in a "trial de novo" in federal district court. *Id.* § 504(a). Thus, Verizon could have declined to pay the forfeiture and preserved its opportunity for a *de novo* jury trial if the government sought to collect. Instead, it chose to pretermit any § 504(a) enforcement action and seek immediate review in our Court. *Cf. Westchester Day Sch. v. Vill. of Mamaroneck*, 504 F.3d 338, 356 (2d Cir. 2007) (discussing the waiver of the jury-trial right).

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

backdrop, the agency's proceedings before a § 504(a) trial create no Seventh Amendment injury. *Cf. Cap. Traction Co. v. Hof*, 174 U.S. 1, 4, 45–46 (1899) (holding that an initial tribunal may lawfully enter judgment without a full jury trial if the law permits a subsequent "trial [anew] by jury, at the request of either party, in the appellate court").

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

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

that *Jarkesy* tells us is most important for assessing whether the Seventh Amendment applies—would not exist. And ultimately, if the government declined to pursue the collection action within five years, Verizon would be under no obligation to pay and would suffer no Seventh Amendment injury.

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

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

Moreover, given the Supreme Court's recent decision in *McLaughlin Chiropractic Associates, Inc. v. McKesson Corp.*, 606 U.S. 146 (2025), it is questionable whether *Stevens* remains good law at all. In *Stevens*, the Fifth Circuit reasoned that the district court lacked jurisdiction to consider legal challenges to the validity of a forfeiture order in a § 504(a) trial because § 402(a), by reference to the Hobbs Act, vests courts of appeals with "'exclusive jurisdiction . . . to determine the validity of' final FCC forfeiture orders." 691 F.3d at 623 (quoting 28 U.S.C. § 2342). *McLaughlin*, however, teaches that "[t]he Hobbs Act does not preclude district courts in enforcement proceedings from independently assessing whether an agency's interpretation of the relevant statute is correct," so it may well abrogate *Stevens*. 606 U.S. at 152.[16] But even if that were not the case, we would not find *Stevens*' reasoning persuasive. While § 402(a), the Communication Act's general review provision, vests such exclusive jurisdiction in the courts of appeals, "[i]t is a commonplace of statutory construction that the specific governs the general." *Nat'l Labor Rels. Bd. v. SW Gen., Inc.*, 580 U.S. 288, 305 (2017) (quotation

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

marks omitted). And here, § 504(a) creates a specific "exception to [the] general rule" for government actions for the recovery of forfeiture penalties. *AT&T Corp.*, 323 F.3d at 1084. In other words, despite its protestations, Verizon waived any right it had to the same kind of trial the SEC's enforcement targets have post-*Jarkesy*.

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

CONCLUSION

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