United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued March 24, 2025 Decided August 15, 2025

No. 24-1224

SPRINT CORPORATION,
PETITIONER

v.

FEDERAL COMMUNICATIONS COMMISSION AND UNITED STATES OF AMERICA,
RESPONDENTS

Consolidated with 24-1225

On Petitions for Review of Orders
of the Federal Communications Commission

Helgi C. Walker argued the cause for petitioners. With her on the briefs were *Russell B. Balikian*, *Zachary E. Tyree*, and *Nathaniel J. Tisa*.

Joshua S. Turner, *Sara M. Baxenberg*, *Boyd Garriott*, and *Stephen J. Conley* were on the brief for *amicus curiae* CTIA - The Wireless Association in support of petitioners.

Mariel A. Brookins was on the brief for *amicus curiae* the Chamber of Commerce of the United States of America in support of petitioners.

John R. Grimm, Counsel, Federal Communications Commission, argued the cause for respondents. With him on the brief were *Robert B. Nicholson* and *Matthew A. Waring*, Attorneys, U.S. Department of Justice, *Jacob M. Lewis*, Deputy General Counsel, Federal Communications Commission, and *Sarah E. Citrin*, Deputy Associate General Counsel. *Robert J. Wiggers*, Attorney, U.S. Department of Justice, and *Adam Sorensen*, Attorney, Federal Communications Commission, entered appearances.

Alan Butler, *Christopher Frascella*, *Samir Jain*, *Eric Null*, and *Aaron Mackey* were on the brief for *amici curiae* the Electronic Privacy Information Center, et al. in support of respondents.

Before: HENDERSON, PAN, and GARCIA, *Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* PAN.

PAN, *Circuit Judge*: Every cell phone is a tracking device. To receive service, a cell phone must periodically connect with the nearest tower in a wireless carrier's network. Each time it does, it sends the carrier a record of the phone's location and, by extension, the location of the customer who owns it. Over time, this information becomes an exhaustive history of a customer's whereabouts and "provides an intimate window into [that] person's life." *Carpenter v. United States*, 585 U.S. 296, 311 (2018).

Congress recognized the highly sensitive nature of this data. In 1999, it amended the Communications Act to impose on telecommunications carriers "a duty to protect the confidentiality" of customer location information (CLI). 47 U.S.C. § 222(a); *see also* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286. The Act forbids carriers, in most circumstances, from sharing that information with third parties absent affirmative customer consent. 47 U.S.C. § 222(c)(2). An implementing regulation further requires carriers to take "reasonable measures" to protect CLI from unauthorized access by third parties. 47 C.F.R. § 64.2010(a).

This case concerns whether two carriers — Sprint Corporation and T-Mobile USA, Inc. — violated their "duty to protect the confidentiality" of CLI. 47 U.S.C. § 222(a). For years, Sprint and T-Mobile sold CLI to third parties. In theory, Sprint and T-Mobile required those third parties to obtain customer consent. But in practice, the third parties did not always do so, and Sprint and T-Mobile provided the CLI without verifying compliance. Several bad actors abused Sprint and T-Mobile's programs to illicitly access CLI without the customers' knowledge, let alone consent. And even after Sprint and T-Mobile became aware of those abuses, they continued to sell CLI for some time without adopting new safeguards. Based on those facts, the Federal Communications Commission concluded that Sprint and T-Mobile violated the Communications Act and fined them a combined $92 million.

Sprint and T-Mobile (collectively, "the Carriers") now petition for our review. Neither denies what happened. Instead, they argue that the undisputed facts do not amount to a violation of the law. The Carriers also argue that the Commission misinterpreted the Communications Act, miscalculated the penalties, and violated the Seventh

Amendment by not affording them a jury trial. Because the Carriers' arguments lack merit, we deny the petitions for review.

I.

A.

The Communications Act requires telecommunications carriers to "protect the confidentiality" of "customer proprietary network information," or CPNI. 47 U.S.C. § 222(a), (c)(1). The Act defines CPNI to include certain customer location information — the data at issue in this case. *See id.* § 222(h)(1)(A). Subject to a handful of exceptions, carriers must obtain affirmative customer consent before disclosing CPNI to third parties. *Id.* § 222(c); *see also* 47 C.F.R. § 64.2007(b). And "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a). If a carrier "willfully or repeatedly fail[s] to comply" with its duty to protect CPNI, the carrier "shall be liable to the United States for a forfeiture penalty." 47 U.S.C. § 503(b)(1)(B).

When the Commission suspects that a carrier has committed a violation, it can initiate an investigation by sending a letter of inquiry to the carrier, which asks the carrier to "answer questions and produce documents relevant to evaluating whether a violation has occurred." Fed. Commc'ns Comm'n, *Enforcement Primer*, https://perma.cc/V7BS-8QGN.

If, following an investigation, the Commission thinks a violation was committed, the Commission has two procedural options for pursuing a forfeiture penalty. Under the first option, it may issue a "notice of opportunity" for "a formal hearing" "conducted by an administrative law judge."

47 C.F.R. § 1.80(h); *see also* 47 U.S.C. § 503(b)(3)(A). In such a proceeding, the ALJ hears evidence from the Commission and the carrier, and then issues an initial decision, which can be appealed to the Commission. 47 C.F.R. § 1.80(h)(1); *see also id.* §§ 1.243, 1.250–82. The Commission's ruling, in turn, is subject to direct review in a court of appeals. 47 U.S.C. § 503(b)(3)(A); *see also id.* § 402(a).

Under the second option, the Commission may issue a "notice of apparent liability" (NAL) to the carrier. 47 U.S.C. § 503(b)(4). The NAL must, among other things, identify the provisions of law alleged to have been violated, set forth the facts underlying the violation, and propose a penalty amount. *Id.*; *see also* 47 C.F.R. § 1.80(g)(1). The carrier is then afforded a reasonable opportunity to submit affidavits and "to show, in writing, . . . why no such forfeiture penalty should be imposed" or why the proposed penalty amount should be reduced. 47 U.S.C. § 503(b)(4); *see also* 47 C.F.R. § 1.80(g)(3). The Commission then decides, "upon considering all relevant information available to it," whether to affirm, cancel, or modify the NAL. 47 C.F.R. § 1.80(g)(4). If the Commission affirms the NAL, the carrier has two options: It may either pay the penalty and seek direct review in a court of appeals, *see AT&T Corp. v. FCC*, 323 F.3d 1081, 1083–84 (D.C. Cir. 2003); or it can "do nothing at all until it is served with a complaint, at which point it is entitled," by statute, "to a trial de novo in district court," *Action for Children's Television v. FCC*, 59 F.3d 1249, 1261 (D.C. Cir. 1995); *see also* 47 U.S.C. § 504(a).

If the Commission assesses a penalty, it first determines a base amount and then evaluates whether an upward or downward adjustment is warranted. In making those determinations, the Act directs the Commission to 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). Applicable regulations provide that an upward variance may be warranted based on considerations such as the carrier's "ability to pay," whether the carrier committed "egregious misconduct," whether the violation was "repeated or continuous," and whether the violation caused "substantial harm." 47 C.F.R. § 1.80(b)(11) Table 3 (cleaned up). A downward variance may be appropriate if, for example, the violation was "minor"; the carrier acted in "good faith"; or the carrier's ability to pay is limited, such that a smaller penalty could provide adequate disincentive. *Id.* (cleaned up).

B.

Sprint and T-Mobile are wireless carriers that provide both voice and data services to customers throughout the United States. Customer devices must stay connected to a carrier's network by periodically registering with the nearest cell tower in the network. That enables the devices to send and receive calls, and to transmit data. *In re T-Mobile USA, Inc.*, FCC 24-43, at 10 ¶ 23 (Apr. 29, 2024), https://perma.cc/B4JF-5BE4 [hereinafter *T-Mobile Order*].[1] Each time a device registers, it provides the carrier with information regarding the customer's real-time location. *Id.*

Until 2019, Sprint and T-Mobile operated location-based service (LBS) programs, through which they sold CLI to two third-party "location information aggregators," LocationSmart and Zumigo. *T-Mobile Order*, at 4 ¶ 8. Those aggregators, in turn, resold the CLI — either directly or through "sub-

[1] The Commission issued separate orders against Sprint and T-Mobile. Those orders are substantially similar, and we cite primarily to the order against T-Mobile, except where indicated.

aggregators" — to third-party "service providers" that used the information to deliver location-based services, like roadside assistance and bank-fraud prevention. *Id.* at 4–5 ¶¶ 8–9. Neither Sprint nor T-Mobile directly contracted with the sub-aggregators or service providers who participated in their LBS programs. *See id.*

To protect CLI, Sprint and T-Mobile largely relied on their contracts with the aggregators. The aggregators agreed to ensure that sub-aggregators and service providers obtained customer consent and abided by certain industry standards before accessing CLI. *T-Mobile Order*, at 5 ¶¶ 9–10; *see also In re Sprint Corp.*, FCC 24-42, at 5 ¶¶ 9–10, https://perma.cc/5ZL8-SJFN [hereinafter *Sprint Order*]. But T-Mobile "did not independently verify the customers' consent before providing access to the location data." *T-Mobile Order*, at 5 ¶ 9. And Sprint similarly did not "notify customers and collect affirmative customer consent" before disclosing CLI. *Sprint Order*, at 5 ¶ 9.

T-Mobile also required participants in its LBS program to submit information about their privacy policies and how they proposed to use the customer location data. T-Mobile referred to each proposed use of CLI as a "campaign" and assigned each approved campaign an ID number. *T-Mobile Order*, at 5 ¶ 10. The provider included the ID number on every information request, which theoretically allowed T-Mobile to monitor all the campaigns. *Id.* Similarly, Sprint required the aggregators to certify that sub-aggregators and providers abided by Sprint's data privacy and security requirements. *Sprint Order*, at 5 ¶ 10.

Under their contracts with the aggregators, the Carriers had "broad authority" to terminate any third party's access to CLI if they "believed [the party] was not complying with its obligations." *T-Mobile Order*, at 5 ¶ 11. They also had

authority to audit the aggregators. *Id.* at 6 ¶ 12. The Commission found "no evidence," however, that Sprint ever conducted an audit prior to 2018. *Sprint Order*, at 6 ¶ 12. T-Mobile, on the other hand, conducted two "risk assessments" — one in 2016 and one in 2018. *T-Mobile Order*, at 6 ¶ 12. But those assessments apparently failed to detect abuses committed by several third parties participating in T-Mobile's LBS program. *See id.* at 21 ¶ 48.

C.

Around July 2017, T-Mobile "learned through a third party" that an unidentified service provider was misusing its customer location data. *T-Mobile Order*, at 6 ¶ 13. After an investigation, T-Mobile identified the culprit as LocateUrCell. *Id.* T-Mobile had approved LocateUrCell for one campaign — helping customers find their missing devices. *Id.* But LocateUrCell had been misusing its approved-campaign ID to provide location data — without customer consent — to companies in the bail-bonds industry. *Id.* In September 2017, T-Mobile informed the relevant aggregator, LocationSmart, of LocateUrCell's abuses. *Id.* LocationSmart told T-Mobile that it had terminated LocateUrCell's access to T-Mobile's customer location data earlier that month. *Id.* Because LocateUrCell had used its approved-campaign ID for all information requests, T-Mobile was unable to differentiate between authorized and unauthorized requests for CLI. *Id.*

In May 2018, the *New York Times* reported that another service provider, Securus Technologies, was abusing its access to the LBS programs of Sprint, T-Mobile, and several other wireless carriers. *See* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. TIMES (May 10, 2018), https://perma.cc/3BBU-XWMQ. Both Sprint and T-Mobile had authorized Securus to access their

CLI — through aggregator LocationSmart and sub-aggregator 3CInteractive — for the purpose of monitoring prisoner phone calls and ensuring that the caller was not located in the immediate vicinity of the prison. But Securus began using its access for an unapproved purpose: providing law enforcement with CLI without customer knowledge or consent. *T-Mobile Order*, at 7 ¶ 14. Ostensibly, Securus required law enforcement to submit "legal authorization," such as a warrant, for any request. *Id.* But Securus did not verify the validity of the uploaded documents. This allowed a sheriffs' deputy in Missouri to access CLI "for non-law enforcement purposes." *Id.* The deputy would upload irrelevant documents like his car-insurance policy as the "legal authorization" for the information request. *Id.* at 7 ¶ 15. Neither Sprint nor T-Mobile had any safeguards that alerted them to the Securus breach.

The day after the *New York Times* published the Securus article, T-Mobile terminated Securus and 3CInteractive's access to CLI. *T-Mobile Order*, at 8 ¶ 16. Five months later, in October 2018, T-Mobile notified its aggregators, LocationSmart and Zumigo, that it would let their contracts expire in another five months, which would effectively end T-Mobile's LBS program by March 2019. *Id.*

Sprint, for its part, terminated Securus's access within a week of the *New York Times* article. *Sprint Order*, at 8 ¶ 15. Another week later, Sprint suspended LocationSmart from its LBS program. *Id.* And within a month, in June 2018, Sprint notified Zumigo that its access would end in September. *Id.*

But Sprint planned a relaunch of its LBS program. *Sprint Order*, at 8 ¶ 16. It devised new procedures to "complement" its existing contractual provisions. *Id.* Under the new procedures, aggregators would be required to commission third-party audits and to submit more detailed reports to Sprint.

Sprint relaunched its LBS program in August 2018, restoring LocationSmart's access for two preapproved service providers. *Id.* at 9 ¶ 17. In October 2018, Sprint fully restored Zumigo's access, which Sprint had terminated the prior month. *Id.*

Not long after, in January 2019, another breach came to light. *Vice News* reported that a service provider called Microbilt had sold CLI from Sprint and T-Mobile to bounty hunters without customer consent. *See* Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, VICE NEWS (Jan. 8, 2019), https://perma.cc/259D-ZNZU. Sprint was entirely unaware that Zumigo had given Microbilt access to Sprint customer location data. *Sprint Order*, at 9 ¶ 18. And although T-Mobile had authorized Microbilt to access T-Mobile data, T-Mobile did not know that Microbilt was sharing the data with additional third parties. *See T-Mobile Order*, at 8 ¶ 17.

Sprint canceled its contract with Zumigo in January 2019 and its remaining contract with LocationSmart in May 2019, ending its LBS program. *Sprint Order*, at 9 ¶¶ 18–19. T-Mobile suspended Microbilt's access to its data in January 2019 and shuttered its entire LBS program in February 2019. *T-Mobile Order*, at 8 ¶¶ 17–18.

D.

The Commission sent letters of inquiry to Sprint and T-Mobile and investigated the apparent misuse of CLI in their LBS programs. Then, in February 2020, the Commission issued NALs to Sprint and T-Mobile. The NALs alleged that both carriers violated the Communications Act by failing to take reasonable measures to safeguard customer location data against attempts to gain unauthorized access. The NALs also

proposed to levy forfeiture penalties against Sprint and T-Mobile.

The Carriers filed written responses, arguing that the NALs should not be affirmed. Among other things, they claimed that the customer location data at issue was not CPNI under the Communications Act and therefore was not subject to CPNI regulation. The Carriers also insisted that, even if the information was CPNI, they satisfied their duty to take reasonable measures to protect it.

The Commission disagreed. In April 2024, it issued orders that affirmed the notices of apparent liability. In the orders, the Commission determined that customer location data "falls squarely within" the statutory definition of CPNI; that Sprint and T-Mobile violated the Communications Act by not properly handling CPNI; and that the Carriers should be assessed forfeiture penalties. *T-Mobile Order*, at 9–10 ¶¶ 21–22.

The Commission concluded that Sprint and T-Mobile not only failed to take reasonable measures to protect CPNI but also failed "to promptly address" their "demonstrably inadequate CPNI safeguards" once the Securus breach came to light. *T-Mobile Order*, at 20 ¶ 45. The Commission explained that the Carriers' safeguards "relied almost entirely upon contractual agreement[s]" with the aggregators, which were "passed on to" the "providers through an attenuated chain of downstream contracts." *Id.* at 20 ¶ 47. "To enforce these safeguards," the Commission reasoned, the Carriers "would have needed to take steps to determine whether they were actually being followed." *Id.* at 21 ¶ 48. But the Carriers did not do that and instead unreasonably relied on "the honor system." *Id.* at 22 ¶ 51. In other words, Sprint and T-Mobile trusted the third parties participating in their LBS programs,

and did not verify whether those third parties were keeping their promises to obtain customer consent for the use of CLI. Nor did either carrier have an effective mechanism for "distinguishing between a legitimate request for customer location information" and "an illegitimate one." *Id.* at 21 ¶ 48.

The Commission also faulted Sprint and T-Mobile for failing to quickly implement effective safeguards after learning of the Securus breach. *T-Mobile Order*, at 22 ¶ 53. Although the carriers promptly terminated Securus's access to CLI, both continued to operate their LBS programs "under [effectively] the *same system* that was exploited by Securus." *Id.* (emphasis in original). And although Sprint suspended LocationSmart's contract and eventually implemented some new procedures under its relaunched program, the Commission deemed those steps inadequate: The temporary suspension of LocationSmart did not improve protections for consumers whose location information still could be disclosed under the LBS program that otherwise remained in place. *Sprint Order*, at 22 ¶ 51. Moreover, Sprint's new procedures still relied on the aggregators' compliance with contractual obligations and there was "little evidence" that Sprint took steps to ensure that compliance. *Id.*

After finding the Carriers liable for violating the Act, the Commission assessed an $80,080,000 forfeiture penalty against T-Mobile and a $12,240,000 penalty against Sprint. *T-Mobile Order*, at 33 ¶ 74; *Sprint Order*, at 27 ¶ 62.

As relevant here, the Communications Act authorizes a penalty of up to $2,048,915 for each violation committed by a common carrier. *See* 47 U.S.C. § 503(b)(2)(B); *see also In re Adjustment of Civil Monetary Penalties to Reflect Inflation*, 34 FCC Rcd. 12824, 12828 (2019) (establishing 2020 inflation-adjusted statutory maximum at $2,048,915). The

Commission rejected the Carriers' argument that they could be fined no more than $2,048,915 each because they each committed, at most, only one violation of the Act by operating a single LBS program without adequate safeguards. Instead, the Commission determined that Sprint and T-Mobile committed "separate continuing violations" for each third party that they allowed to access CLI in the absence of reasonable safeguards after the Carriers learned of the Securus breach. *T-Mobile Order*, at 34 ¶¶ 77–78. "[E]ach unique relationship" between a carrier and a third party, the Commission reasoned, "represented a distinct failure to reasonably protect" CPNI. *Id.* at 35 ¶ 79. And notably, each relationship "relied upon a distinct and unique contractual chain." *Id.*

The Commission calculated the penalties as follows: It started the penalty period thirty days after the Carriers were put on notice of the Securus breach, thereby allowing the Carriers a grace period within which they could have implemented a reasonable response. After the thirtieth day, the Commission assessed penalties for each third-party aggregator, sub-aggregator, and service provider, consisting of $40,000 for the first day and $2,500 for each subsequent day until the carrier canceled the third party's access to CLI. *T-Mobile Order*, at 33–35 ¶¶ 74, 78, 81. Because Sprint terminated, within the grace period, the access of several third parties that partnered with aggregator LocationSmart, the Commission assessed penalties against Sprint for only 11 violations. *See Sprint Order*, at 27 ¶ 62. T-Mobile did not terminate access on a similar scale, so the Commission assessed penalties against T-Mobile for 73 violations. *T-Mobile Order*, at 33 ¶ 74; *see also id.* at 39–40 ¶¶ 93–94. The Commission applied a 75 percent upward variance to T-Mobile's assessed penalties and a 100 percent upward variance to Sprint's. *See T-Mobile Order*, at 33 ¶ 74; *Sprint Order*, at 27 ¶ 62.

The Commission reasoned that the Carriers' conduct was "egregious." *T-Mobile Order*, at 39 ¶ 92; *see also Sprint Order*, at 30 ¶ 72. As the Commission put it, "even after highly publicized incidents put" Sprint and T-Mobile "on notice that [their] safeguards . . . were inadequate," the Carriers "continued to sell access" to CLI without implementing reasonable measures to protect that data. *T-Mobile Order*, at 36 ¶ 84 (cleaned up). Those violations, the Commission explained, were "continuous over an extended period of time." *Id.* at 39 ¶ 92. And the Carriers' "protracted" failure to protect CPNI "caused substantial harm by making it possible for malicious persons to identify the exact locations" of their unsuspecting customers. *Id.* (cleaned up). The Commission also "took into account" the Carriers' "status as . . . major telecommunications provider[s]" to devise a penalty that would meaningfully deter similar misconduct in the future. *Id.*

Two members of the Commission dissented. Commissioner Carr agreed with the Carriers that the information at issue is not CPNI. Commissioner Simington disputed the Commission's conclusion that "a single, systemic failure" could be subdivided into "many separate and continuing violations." *Sprint Order*, at 44.

Sprint and T-Mobile paid the assessed penalties and timely petitioned for our review. 47 U.S.C. § 402(c). We have jurisdiction under 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1).

II.

This "court will deny a petition for review of an order by the Commission unless it is 'arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.'" *Star Wireless, LLC v. FCC*, 522 F.3d 469, 473 (D.C. Cir. 2008) (quoting 5 U.S.C. § 706(2)(A)). We resolve issues of

constitutional law and statutory interpretation *de novo*. *See Nat'l Lifeline Ass'n v. FCC*, 983 F.3d 498, 507 (D.C. Cir. 2020) (cleaned up); *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 394 (2024). But in determining whether agency action is arbitrary and capricious, our review is "highly deferential." *Nat'l Lifeline Ass'n*, 983 F.3d at 507. We "presume[] the validity of agency action and must affirm unless the Commission failed to consider relevant factors or made a clear error in judgment." *Id.* (quoting *Cellco P'ship v. FCC*, 357 F.3d 88, 93–94 (D.C. Cir. 2004)).

III.

Sprint and T-Mobile raise a slew of challenges to the orders that found them in violation of the Communications Act and levied hefty fines on them. The Carriers claim that: (1) the Commission violated the Seventh Amendment by assessing civil penalties against them without affording them a jury trial; (2) the Commission incorrectly interpreted the Communications Act; (3) even if the Commission's interpretation were correct, regulated parties lacked fair notice of it; (4) the Commission's liability determinations were arbitrary and capricious; and (5) the Commission assessed penalties that were unlawfully excessive. We are unpersuaded.

A.

1.

We start with the Carriers' claim that the Commission violated their right to a jury trial under the Seventh Amendment. But we need not resolve that claim. That is because the statutory procedure at issue allowed the Carriers to obtain a jury trial before suffering any legal consequences. Thus, regardless of whether it was constitutionally guaranteed,

the Carriers had the right to a jury trial. They chose not to wait for such a trial and therefore waived that right.[2]

Under the statutory framework for assessing penalties under the Communications Act, the Commission issued to each carrier a notice of apparent liability. 47 U.S.C. § 503(b)(4). Both carriers had the option of responding to the notices by either (1) paying the penalty and seeking direct review in a court of appeals, *see AT&T Corp.*, 323 F.3d at 1083–84; or (2) "do[ing] nothing at all until [they were] served with a complaint," at which point they would have been "entitled to a trial de novo in district court," *Action for Children's Television*, 59 F.3d at 1261. The Carriers chose to pay their fines and to seek direct review in this court. They thereby "waived" the jury trial that was "available" to them. *Ill. Citizens Comm. for Broad. v. FCC*, 515 F.2d 397, 405–06 (D.C. Cir. 1974). The Carriers may not now complain that they were denied a right they voluntarily surrendered.

---

[2] The Seventh Amendment provides that in "Suits at common law," "the right of trial by jury shall be preserved." U.S. Const. amend. VII. The Supreme Court has clarified that this right "is not limited to" claims that were recognized at common law "when the Seventh Amendment was ratified." *SEC v. Jarkesy*, 603 U.S. 109, 122 (2024). Instead, it extends to all claims that are "legal in nature" — as opposed to claims sounding in equity or admiralty. *Id.* (quoting *Granfinanciera, S.A. v. Nordberg*, 492 U.S. 33, 53 (1989)). Although both parties make substantial arguments, we need not decide whether the claims at issue here are "legal in nature," nor whether the public-rights exception to the Seventh Amendment's jury-trial guarantee should apply. *See id.* at 127 (recognizing that "Congress may assign" matters involving public rights "for decision to an agency without a jury"). Even if the Seventh Amendment applies, it was not violated because the Carriers had the opportunity to put their case before a jury before any "legal rights" would have been "determined" or any "legal relief" awarded. *Lorillard v. Pons*, 434 U.S. 575, 583 (1978).

The Carriers offer two reasons why the option for a jury trial under section 504(a) was insufficient to vindicate their Seventh Amendment rights. Neither holds up.

First, the Carriers note that the government could have brought the enforcement action under section 504(a) in one of the small handful of jurisdictions where defendants in these types of cases are "limited" to factual defenses and barred from challenging an "order's 'legal validity.'" Opening Br. 35 (quoting *United States v. Stevens*, 691 F.3d 620, 622–23 (5th Cir. 2012)). But the Carriers concede, as they must, that this court has not adopted the rule that troubles them. To the contrary, we have held that "all issues of fact and law" are "subject to the trial de novo" in district court under section 504(a), with a subsequent "right of appeal to the court of appeals." *Pleasant Broad. Co. v. FCC*, 564 F.2d 496, 501–02 (D.C. Cir. 1977); *see also AT&T Corp.*, 323 F.3d at 1085. Thus, the Carriers identify no problem with the Communications Act's enforcement scheme as we have interpreted it.

Although it is possible that the Commission could have brought an enforcement action against the Carriers in a jurisdiction where defendants are not permitted to present legal defenses, "[w]e cannot . . . strike down" the enforcement scheme of the Communications Act "on the basis of a hypothetical." *Tilton v. Richardson*, 403 U.S. 672, 682 (1971); *see also Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 449–50 (2008) ("In determining whether a law is facially invalid, we must be careful not to go beyond the statute's facial requirements and speculate about 'hypothetical' or 'imaginary' cases."). Here, no complaint was filed because the Carriers chose to pay the penalties and pursue a direct appeal to this court. Had the Carriers exercised their statutory

right to a jury trial and had the government brought an enforcement action in a jurisdiction with the unfavorable rule, the Carriers could have raised as-applied challenges in those proceedings. *See Cutter v. Wilkinson*, 544 U.S. 709, 726 (2005).[3] But we cannot "invalidate legislation on the basis of . . . hypothetical . . . situations not before" us. *Nat'l Endowment for the Arts v. Finley*, 524 U.S. 569, 584 (1998) (cleaned up).

Second, the Carriers complain about the options with which they were presented. They note that if they had exercised their right to "do nothing at all" until the government brought an enforcement action, they would not have been guaranteed a trial *de novo*, and they would have given up their option under the statute to pay the penalties and pursue a direct review of the Commission's orders in a court of appeals. *Action for Children's Television*, 59 F.3d at 1261. The Carriers correctly acknowledge that if they had waited for enforcement, they would have had the right to appeal the outcome of a trial *de novo*. *See AT&T Corp.*, 323 F.3d at 1085. But the Carriers worry that the government might not have brought an enforcement action within the five-year statute of limitations. In that scenario, the Carriers assert, the Commission's public findings of liability against them would have stayed on the books, never to be reviewed by an Article III court. The Carriers cite a Fifth Circuit case similar to this one, in which the court held that such findings of liability could "cause reputational harm to carriers" and could be used by the Commission as "prior adjudicated offenses in imposing future

---

[3] The Commission contends that the Fifth Circuit decision that worries the Carriers — *United States v. Stevens*, 691 F.3d 620 (5th Cir. 2012) — has been abrogated by the Supreme Court's recent decision in *McLaughlin Chiropractic Associates, Inc. v. McKesson Corp.*, 145 S. Ct. 2006 (June 20, 2025). That issue is not properly before us.

penalties." *AT&T Corp. v. FCC*, 135 F.4th 230, 241–42 (5th Cir. 2025).

We are unconvinced that the possibility of nonenforcement renders the jury-trial option insufficient to protect the interests of alleged violators. The Seventh Amendment right to a jury trial is a procedural protection that must be honored before "legal rights are determined" and "legal relief" is awarded. *Lorillard v. Pons*, 434 U.S. 575, 583 (1978). But no legal rights are determined and no legal relief is awarded if the Commission declines to enforce an order affirming a NAL.

First, it is hard to credit the Carriers' concern that they would have suffered injury if the Commission never sought to enforce its orders: If that happened, the Carriers would not be required to pay a dime — the $92 million in proposed penalties would never be collected. That undoubtedly is a positive outcome for the Carriers.

Second, it is plainly incorrect that, absent an enforcement proceeding, the Commission could have used its orders affirming the NALs against the Carriers in future proceedings. Under the Communications Act, the NAL has no legal effect unless and until the defendant either pays the penalty or a court enters a final judgment enforcing the Commission's order. *See* 47 U.S.C. § 504(c) (If the Commission issues a NAL, it is prohibited from using "that fact . . . in any other proceeding . . . to the prejudice of the person to whom such notice was issued, unless (i) the forfeiture has been paid, or (ii) a court of competent jurisdiction has ordered payment of such forfeiture, and such order has become final.").[4]

---

[4] The Commission "does not use the mere issuance or failure to pay [a] NAL to the prejudice of the subject." *Forfeiture Policy*

As for the remote risk of reputational harm, that is a thin reed on which to rest a claim that the statutory scheme before us violates the Seventh Amendment. To start, it is far from clear that unenforced orders — never litigated in court or reviewed on appeal — would reflect so poorly on the Carriers that the risk of nonenforcement renders the statutory scheme unconstitutional. Moreover, this argument relies on the road not taken: Although the Carriers chose direct appellate review under section 402(a), they contend that if they had "do[ne] nothing at all" and no enforcement occurred, they would have had no opportunity to use a court proceeding to cure the supposed reputational injury stemming from the NALs. *Action for Children's Television*, 59 F.3d at 1261. It is difficult to follow how that argument implicates a constitutional right. *Lorillard*, 434 U.S. at 583 (explaining that the Seventh Amendment is implicated when legal rights are to be determined, and legal relief awarded). Not surprisingly, the Carriers cite no authority that supports their unusual theory.[5]

Statement, 12 FCC Rcd. 17087, 17103 (1997). True, the Commission maintains the right to "use the facts *underlying* a violation in a subsequent proceeding." *Id.* at 17102 (emphasis added). But that would be allowed regardless of whether the Commission ever issued a NAL.

[5] The only case that they do rely on, *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239 (2012), is inapposite. There, the Commission argued that Fox's challenge to an order finding Fox in violation of a different Communications Act provision was moot because the Commission had exercised forbearance and declined to impose any penalty. The Court held that Fox's challenge was not moot because the order both inflicted reputational harm on Fox and caused an alteration of legal status — the Commission could use the order to enhance penalties in the future. *See id.* at 255–56. But here, the Communications Act specifically prevents the Commission from using the NALs in question against carriers in future proceedings

2.

The Carriers' remaining constitutional arguments fare no better.

First, the Carriers claim it "offends separation-of-powers principles and due process" for the Commission to act "as rule-maker, investigator, prosecutor, judge, and jury." Opening Br. 37–38. But as the Carriers largely concede, precedents from the Supreme Court and this court confirm that an agency can both prosecute and adjudicate an enforcement action. *See Withrow v. Larkin*, 421 U.S. 35, 58 (1975); *see also In re Zdravkovich*, 634 F.3d 574, 579 (D.C. Cir. 2011). Although the Carriers assert that those cases are "ripe for reconsideration," Opening Br. 38, only the Supreme Court can overrule its own precedents, *see Agostini v. Felton*, 521 U.S. 203, 237 (1997).

Next, the Carriers contend that two members of the Commission's majority "made statements suggesting that they had prejudged the issues." Opening Br. 38. An agency decisionmaker is deemed to have prejudged a case "only where he has demonstrably made up his mind about important and specific factual questions and is impervious to contrary evidence." *Fogo de Chao (Holdings), Inc. v. DHS*, 769 F.3d 1127, 1148 (D.C. Cir. 2014) (quoting *Power v. FLRA*, 146 F.3d 995, 1001–02 (D.C. Cir. 1998)). Neither example of alleged prejudgment satisfies that "high burden." *Id.* First, the Carriers point to Commissioner Starks's statement in the *New York Times* that "wireless carriers have been selling our data in ways

---

unless and until they are either paid or enforced following a jury trial. 47 U.S.C. § 504(c). And in any event, the Court's analysis of mootness in *Fox* has no bearing on the Carriers' claim that the option to pursue a jury trial under the present statutory scheme is inadequate due to the possibility that it carries a risk of reputational harm.

that . . . *appear* to violate the law." Geoffrey Starks, Opinion, *Why It's So Easy for a Bounty Hunter to Find You*, N.Y. TIMES (Apr. 2, 2019) (emphasis added), https://perma.cc/3H3D-GLYR. That does not indicate that Commissioner Starks had come to a fixed conclusion that any carrier had broken the law, let alone the conclusion that Sprint or T-Mobile's specific conduct violated the Communications Act. Second, the Carriers cite Commissioner Rosenworcel's statement accompanying the NALs that the "collection and distribution or sale" of CLI "without [customer] permission or without reasonable safeguards in place" is "a violation of the law." J.A. 156. That is an unremarkable and true statement of what the Communications Act requires, not a fixed conclusion about any "factual questions" relevant to either Sprint or T-Mobile's case. *Fogo de Chao*, 769 F.3d at 1148 (cleaned up).

Finally, the Carriers suggest in a footnote that the Communications Act violates the nondelegation doctrine by giving the Commission two paths for pursuing a forfeiture penalty without articulating an intelligible principle to guide the Commission's decision about which path to pursue. The Carriers do not develop that argument and make no effort to grapple with our prior statements that touch upon this issue. *See Meta Platforms, Inc. v. FTC*, No. 24-5054, 2024 WL 1549732, at *3 (D.C. Cir. Mar. 29, 2024) (per curiam) (holding that the Executive Branch's Article II power to enforce the law encompasses the "prerogative to choose where and how to enforce" a statute within the enforcement options created by Congress). We therefore decline to address this cursory argument. *See Hutchins v. District of Columbia*, 188 F.3d 531, 539 n.3 (D.C. Cir. 1999) (en banc) ("We need not consider cursory arguments made only in a footnote.").

B.

We turn now to the Carriers' argument that the Commission misinterpreted the Communications Act. Section 222 of the Act requires telecommunications carriers to safeguard CPNI, 47 U.S.C. § 222(a), and an implementing regulation further requires carriers to take reasonable measures to protect against unauthorized access to CPNI, 47 C.F.R. § 64.2010(a). The Commission determined that Sprint and T-Mobile violated those provisions. Sprint and T-Mobile argue, however, that the CLI they shared with third parties is not CPNI within the meaning of the Act and is therefore not subject to CPNI regulation. We disagree.

As relevant here, information qualifies as CPNI under the Communications Act if it satisfies two statutory requirements. First, it must "relate[] to the quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer." 47 U.S.C. § 222(h)(1) (emphasis added). Second, it must be "made available to the carrier by the customer solely by virtue of the carrier-customer relationship." *Id.* The Communications Act provides that a "telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services." *Id.* § 153(51); *see also* 47 C.F.R. § 54.5. Telecommunications service includes voice services (*e.g.*, phone calls) but not data services (*e.g.*, web browsing). *See Mozilla Corp. v. FCC*, 940 F.3d 1, 17–18 (D.C. Cir. 2019) (per curiam). At all times relevant to this case, data services were classified as information services, which are not subject to CPNI regulations under the Communications Act. *Id.*

The CLI collected by Sprint and T-Mobile fits the statutory definition of CPNI and therefore is subject to regulation. To start, the CLI at issue plainly "relates to the . . . location . . . of a telecommunications service." 47 U.S.C. § 222(h)(1). The location information was generated when customer devices connected to the nearest cell tower in Sprint or T-Mobile's networks to gain access to a telecommunications service — *i.e.*, the ability to send and receive calls. *T-Mobile Order*, at 10 ¶ 23. Each time a customer's device connected to a cell tower in the Carriers' networks, the Carriers were able to discern the device's approximate location. Thus, the CLI "relates" to the "location" where a "telecommunications service" was made possible. That satisfies the first statutory requirement.

Next, the CLI was "made available" to the Carriers "solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1). Sprint and T-Mobile obtained the location information because their wireless-service customers utilized the Carriers' cell towers to be able to make and receive phone calls, and the cell towers tracked the location of the customers' devices. The CLI was the product of the Carriers' relationship with their customers — it did not come from a third party or through some other means. The information at issue thus plainly satisfies the second element of the CPNI definition.

Sprint and T-Mobile try to resist those straightforward conclusions. First, they parse the definition of CPNI to argue that it includes only the location information of a customer device that is actively on a call. Second, they claim that they did not obtain location information solely by virtue of the "carrier-customer relationship" because they provide data services as well as voice services, which means they do not operate purely as "carriers." These strained interpretations find no support in the text, context, or regulatory history of the Communications Act.

1.

The Carriers assert that the CLI at issue does not relate to the location of a telecommunications service (and therefore does not qualify as location CPNI) unless it was generated when the customer was actively on a voice call. They reason that only voice services qualify as "telecommunications service," and the service is used only when the customer is sending or receiving a call. That is wrong on several different levels.

We begin with the text. The Communications Act refers to the "location . . . of a telecommunications service," not the location of a voice call. 47 U.S.C. § 222(h)(1). And it defines "telecommunications service" as "the offering of telecommunications." *Id.* § 153(53). Recall that cell phones connect periodically to cell towers, and that is what enables the devices to send and receive calls at any moment. Thus, whenever a device connects to the network, the carrier is making telecommunications available. The CLI is generated as a by-product of the interaction between the device and the tower. That information therefore "relates to the . . . location . . . of a telecommunications service," regardless of whether the device is actively engaged in a call. *Id.* § 222(h)(1).

To support their alternative interpretation, the Carriers urge an unnatural reading of the requirement that CPI must be "relate[d] to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer." 47 U.S.C. § 222(h)(1). They contend that the term "of use" modifies not just the word "amount," but also every preceding noun in subsection 222(h)(1)'s list. Thus, according to the Carriers, the relevant phrase we must interpret is information

that "relates to" the "location . . . *of use* of a telecommunications service." *Id.* (emphasis added). But even if this were true, it would not alter our conclusion. In our view, a customer "uses" a telecommunications service whenever his or her device connects to the carrier's network for the purpose of being able to send and receive calls. And the Carriers' reading therefore does not narrow "location . . . of use" to times when the customer is actively on a voice call. Because the Carriers' reading does not change the bottom line, we need not decide whether "of use" modifies every noun in section 222(h)(1)'s list or just "amount."

Turning to statutory context, the Carriers point out that section 222 twice uses the term "call location information." *See* 47 U.S.C. § 222(d)(4), (f)(1). Congress added the references to "call location information" when it amended the definition of CPNI to include the word "location." *See* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286. According to the Carriers, the "fact that Congress simultaneously added 'location' information to the definition of CPNI" and two references to "call location information" to section 222 shows that Congress intended "location" CPNI to "refer specifically to call location information." Opening Br. 44 (cleaned up). We think the opposite inference is more appropriate.

"Where words differ as they differ here," "we normally presume that . . . Congress act[ed] intentionally." *Burlington N. & Santa Fe. Ry. Co. v. White*, 548 U.S. 53, 63 (2006) (cleaned up). That presumption is especially warranted in this case because "there is strong reason to believe that Congress intended the differences that its language suggests." *Id*. Section 222 provides that "[i]n general" "[e]very telecommunications carrier has a duty to protect the confidentiality" of CPNI against unauthorized disclosure. 47

U.S.C. § 222(a). In crafting the definition of CPNI, Congress used the broad term "location . . . of a telecommunications service." *Id.* § 222(h)(1). Congress, by contrast, used the narrower term "call location information" when describing a limited exception to a carrier's general duty to protect CPNI. *See id.* § 222(d)(4). It provided that in certain emergency situations, carriers could disclose a customer's call location information without the customer's consent to emergency responders and certain other persons. *Id.* And Congress clarified that such call location information may not be used or disclosed for purposes "other than in accordance with subsection (d)(4)" without the customer's consent. *Id.* § 222(f). Thus, Congress imposed on carriers a general duty to protect all customer location information, regardless of whether the customer is on a call. But when a customer calls 911, a carrier may disclose that "call location information" to emergency responders without obtaining the customer's consent. In sum, Congress used the broad term "location" in the definition of CPNI and used the narrower term "call location information" to fashion a limited exception to the general prohibition on unauthorized CPNI disclosure. That disproves, rather than supports, the Carriers' interpretation.

Finally, we are not persuaded by the Carriers' resort to regulatory history. The Carriers make much of the fact that in guidance from 2013, the Commission listed some examples of CPNI and, with respect to location CPNI, limited its examples to call location information — *e.g.*, "the location of the device *at the time of the calls*" and "the location, date, and time a handset experiences a network event, *such as a dialed or received telephone call*." *In re Implementation of the Telecommunications Act of 1996*, 28 FCC Rcd. 9609, 9616–17 (2013) (emphases added). The Carriers emphasize that the Commission did not specify that location information other than call location information could qualify as CPNI. But the

Commission made clear that its examples were illustrative, not exhaustive. In fact, the Commission explicitly declined to "set out a comprehensive list" of what constitutes CPNI and what does not. *Id.* at 9617 n.54. Regulatory history therefore cannot rescue the Carriers' strained interpretation. Under the best reading of the statute, location CPNI is not limited to call location information.

2.

Nor is there any merit to the Carriers' argument that the information at issue fails to satisfy the second element of the CPNI definition because it was not "made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1). Although Sprint and T-Mobile concede that they obtained their customers' location information solely because of their relationship with those customers, they contend that the relationship was not solely a "carrier-customer" relationship. As Sprint and T-Mobile put it, they "wear two hats." Reply Br. 24. They act as both telecommunications carriers and information-service providers. That is, they package together and provide customers with both telecommunications service (voice calls) and information service (internet data). *See T-Mobile Order*, at 13 ¶ 30. Thus, in Sprint and T-Mobile's view, because they were acting as both a carrier and an information-service provider when they obtained their customers' location information, they did not obtain the information "*solely* by virtue of the *carrier*-customer relationship." 47 U.S.C. § 222(h)(1) (emphases added).

We are not persuaded. True, a company is a carrier "only to the extent that it is engaged in providing telecommunications services." 47 U.S.C. § 153(51). But Sprint and T-Mobile do not dispute that they were providing telecommunications

service and were therefore acting as carriers for the purposes of their relationship with their customers. *See T-Mobile Order*, at 13 ¶ 30. The fact that Sprint and T-Mobile also provided information service to customers did not "take[] the resulting relationship outside the scope of the 'carrier-customer' relationship." *Id.* at 14 ¶ 32 (cleaned up). In other words, the Carriers did not stop being carriers because they were also information-service providers.

Notably, the Carriers do not suggest that they had two separate relationships with each customer — one as a carrier and one as an information-service provider. To the contrary, the Commission indicated that customers enter a single contract with Sprint and T-Mobile for both telecommunications and information service. *See T-Mobile Order*, at 13 ¶ 30. Sprint and T-Mobile obtained customer location information solely because of this integrated relationship. And because Sprint and T-Mobile were engaged in providing customers with telecommunications services, they were acting as carriers for the purpose of the relationship. In sum, under the best reading of the statute, the information at issue qualifies as CPNI. We therefore reject the Carriers' statutory arguments.

C.

The Carriers have a back-up argument. They claim that even if the Commission correctly interpreted CPNI to include the information at issue here, regulated parties lacked fair notice of that "novel" interpretation. Opening Br. 53.

Under the Due Process Clause of the Fifth Amendment, "laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012). "This

requirement is implicated whenever the government imposes civil penalties." *Bello v. Gacki*, 94 F.4th 1067, 1074 (D.C. Cir. 2024) (cleaned up). To determine whether a regulated party had fair notice, "we ask 'whether the law or regulation provides a discernible standard when legally construed.'" *Id.* (cleaned up) (quoting *Fed. Express Corp. v. Dep't of Com.*, 39 F.4th 756, 773 (D.C. Cir. 2022)). Because "[e]ven trained lawyers may find it necessary to consult legal dictionaries, treatises, and judicial opinions" to ascertain what a statute means, a statute "is considered unconstitutionally vague only if, 'applying the rules for interpreting legal texts, its meaning specifies no standard of conduct at all.'" *Fed. Express*, 39 F.4th at 773 (quoting *United States v. Bronstein*, 849 F.3d 1101, 1107 (D.C. Cir. 2017)). Critically, "[w]e have never applied the fair notice doctrine in a case where the agency's interpretation is the most natural one." *NetworkIP, LLC v. FCC*, 548 F.3d 116, 123 (D.C. Cir. 2008). To the contrary, the requirement of fair notice is generally "satisfied" whenever the agency's "interpretation . . . is the most natural" reading of the statute. *Id.* at 125.

That is the case here. As we have explained, *see supra* Part III.B, the Commission's interpretation is the best and most straightforward interpretation of the Communications Act: The location information at issue plainly constitutes CPNI. The Carriers cannot manufacture a Due Process problem merely by offering a conceivable but less natural alternative reading of the statute. *See NetworkIP*, 548 F.3d at 124–25.

To be sure, in some cases, an agency's interpretation may still pose fair-notice problems even when it is the most natural reading of the law. The Supreme Court explained in *Fox Television* that the Commission violated fair notice by abruptly changing its prior policy and retroactively applying a new, inconsistent policy. *See* 567 U.S. at 246–49, 254. And we

similarly held in *Trinity Broadcasting of Florida, Inc. v. FCC* that the Commission violated fair notice when it adopted an interpretation of a regulation that, although reasonable, was in direct conflict with the Commission's "prior interpretation of a nearly identical regulation." 211 F.3d 618, 629–30 (D.C. Cir. 2000).

But this is not a case where the agency changed its interpretation. As we have explained, *see supra* Part III.B.1, nothing in the Commission's prior guidance conflicts with the interpretation the Commission adopted in this case. And although the Commission had not previously stated that location CPNI encompasses more than just call location information, fair notice does not require agencies to give advance warning of a statute's every possible application. *Cf. FDA v. Wages & White Lion Inv., LLC*, 145 S. Ct. 898, 925 (2025). Agencies, like courts, routinely interpret statutes in the context of a case of first impression. *See Neustar, Inc. v. FCC*, 857 F.3d 886, 895 (D.C. Cir. 2017). And "[e]very case of first impression has a retroactive effect, whether the new principle is announced by a court or by an administrative agency." *NetworkIP*, 548 F.3d at 123 (quoting *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947)). Accordingly, we find no merit to the Carriers' fair-notice argument.

D.

Next, the Carriers challenge the Commission's liability determinations. The Commission concluded that the Carriers violated the Communications Act by not only failing to take reasonable measures to protect CPNI, but also by failing "to promptly address" their inadequate safeguards following news of the Securus breach. *T-Mobile Order*, at 20 ¶ 45; *see also* 47 C.F.R. § 64.2010(a) (requiring carriers to "take reasonable measures to discover and protect against attempts to gain

unauthorized access to CPNI"). The Carriers attack the Commission's determinations as arbitrary and capricious.

Arbitrary-and-capricious review is "highly deferential." *Nat'l Lifeline Ass'n*, 983 F.3d at 507 (cleaned up). We may not substitute our judgment for that of the agency. *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). Thus, we must affirm the Commission's decision if it "made factual findings supported by substantial evidence, considered the relevant factors, and articulated a rational connection between the facts found and the choice made." *EchoStar Commc'ns Corp. v. FCC*, 292 F.3d 749, 752 (D.C. Cir. 2002) (cleaned up). The Commission's liability determinations readily clear the bar.

To start, the Commission reasonably concluded that the Carriers' LBS programs lacked adequate safeguards. *T-Mobile Order*, at 20 ¶ 45. The Carriers emphasize that they "required both aggregators and LBS providers to comply with" industry standards regarding customer consent and data privacy. Opening Br. 58. But as the Commission explained, the Carriers merely relied on the honor system. In other words, the Carriers trusted the aggregators and providers "to honor their contractual commitments" to protect customer location data and failed to take meaningful steps to verify that these commitments "were actually being followed." *T-Mobile Order*, at 20–21 ¶¶ 47–48; *see also Sprint Order*, at 18, 20 ¶¶ 41, 48. The Carriers also lacked any mechanism for distinguishing between authorized and unauthorized information requests. The Commission thus rationally concluded that Sprint and T-Mobile's safeguards for CPNI were unreasonable.

The Carriers next contest the Commission's determination that their response to the Securus breach was unreasonable. *T-*

Mobile Order, at 20 ¶ 45. They emphasize that they both acted quickly to cut off Securus's access to CLI once its abuses came to light. Sprint went a step further and temporarily halted LocationSmart's access as well. But the Commission explained that this response was inadequate because both Carriers otherwise "continued to sell access" to CLI under "the *same system* that was exploited by Securus." *Id.* at 22 ¶ 53 (emphasis in original). Sprint also "undermined" its decision to suspend LocationSmart by "reinstating LocationSmart (and two of its customers)" a few months later without meaningfully improved safeguards. *Sprint Order*, at 22 ¶ 51. Although Sprint had implemented some new procedures, the Commission found "little evidence that Sprint actually followed through with these policies in a way that had any meaningful impact." *Id.* On appeal, Sprint offers no reason to doubt that finding. Further, the Commission explained that Sprint's decision to "cut[] off" access for "some" third parties "did not improve the safeguards for consumers whose location information could be disclosed" under the LBS program that otherwise remained in place. *Id.* Thus, the Commission's reasoning was not arbitrary and capricious.

E.

Finally, the Carriers raise two challenges to the penalties imposed by the Commission, but neither succeeds.

First, the Carriers argue that the Commission exceeded the statutory maximum penalty of $2,048,915 for "any single act or failure to act." 47 U.S.C. § 503(b)(2)(B); *see also In re Adjustment of Civil Monetary Penalties*, 34 FCC Rcd. at 12828. The Carriers renew their claim that "each Company committed, at most, a single" violation by continuing to operate their LBS programs without improved safeguards following the news of the Securus breach. Opening Br. 65.

The Commission saw things differently, and its approach was reasonable.[6] The Commission determined that the Carriers committed separate violations for each third party that accessed their CPNI in the absence of adequate safeguards. That determination was aligned with the Carriers' own certification procedures, which imposed contractual obligations on third parties to safeguard CPNI on a relationship-by-relationship basis. The Carriers' practice was to protect CPNI by vetting, or requiring the aggregators to vet, each sub-aggregator or provider to ensure that their data privacy and customer-consent procedures would include securing customer consent for the disclosure of CLI. *See* Opening Br. 58 ("T-Mobile itself

---

[6] In the orders under review, the Commission interpreted section 503(b) as giving it "discretion" to determine "the number of violations" represented by a carrier's conduct "in the CPNI [and] data security context." *See T-Mobile Order*, at 34–35 ¶¶ 78–79. The Commission then concluded that it was "rational and properly within the Commission's discretion" to regard each third-party relationship as conduct constituting a separate violation. *Id.* at 35 ¶ 79. The thrust of the Carriers' challenge is that the way the Commission viewed the facts was unreasonable. Although the Carriers gesture at an argument that their conduct amounted to only a single "failure to act" within the meaning of the statute, they do so in only "a cursory fashion, without" real analysis of the "relevant statutory text" or any "references to relevant case law or other authority." *Indep. Producers Grp. v. Libr. of Cong.*, 792 F.3d 132, 141 (D.C. Cir. 2015). The Carriers therefore forfeited any statutory challenge to the Commission's determination and "[w]e take the dispute as the parties [have actually] frame[d] it," *i.e.*, as whether the Commission reasonably exercised its discretion. *Creighton Ltd. v. Qatar*, 181 F.3d 118, 125 (D.C. Cir. 1999); *Nat'l Ass'n of Realtors v. United States*, 97 F.4th 951, 957 (D.C. Cir. 2024) ("We adopt the framing of the dispute that is advanced by the parties because in our adversarial system of adjudication, we follow the principle of party presentation." (cleaned up)).

preapproved each LBS campaign after reviewing detailed information about the LBS provider, including clear depictions of the process by which it secured customers' consent."); *id.* at 59 ("Sprint likewise implemented a certification process . . . through which aggregators tested sub-aggregators' and LBS providers' applications to ensure they met Sprint's notice, privacy, and data security requirements."). That process implicitly recognized that every sub-aggregator or service provider that accessed customer data in the absence of reasonable safeguards posed an independent danger of CPNI misuse. Thus, it was reasonable for the Commission to conclude that each third-party relationship in which the Carriers provided CLI without adequate safeguards formed the basis of a distinct violation.

Second, the Carriers argue that the penalties imposed by the Commission were arbitrary and capricious because the underlying conduct was at most a failure to fulfill "statutory or regulatory duties" and did not involve "intentional efforts to defraud or to harm or mislead consumers." Opening Br. 67–68. The Carriers note that the Commission previously had imposed such large fines only in cases involving fraud or intentional efforts to mislead consumers, and they are guilty of neither form of misconduct. The Commission reasonably explained, however, that the Carriers' conduct was "egregious": Even after the Securus breach exposed Sprint and T-Mobile's safeguards as inadequate, both carriers continued to sell access to CLI under a broken system. *See T-Mobile Order*, at 36, 39 ¶¶ 84, 92. The Commission further explained that the Carriers' violations were continuous over an extended period of time. *See id.* at 39 ¶ 92. Moreover, both the Communications Act and the relevant regulations direct the Commission to take into account an offender's ability to pay. *See* 47 U.S.C. § 503(b)(2)(E); 47 C.F.R. § 1.80(b)(11) Table 3. Here, the Commission explicitly considered the Carriers' status

as leading telecommunications companies with the ability to pay large amounts when calculating penalties meaningful enough to deter future misconduct. *See T-Mobile Order*, at 39 ¶ 92. Thus, the Commission adequately explained and reasonably supported its imposition of large penalties in this case.

* * *

As the Commission correctly determined, customer location information is CPNI under the Communications Act. The Carriers therefore had a duty to protect such information from misuse by third parties. The Commission reasonably concluded that the Carriers violated that duty by failing to take reasonable measures to prevent bad actors from abusing access to CLI. Indeed, the Carriers failed to promptly take such measures even after they became aware of serious abuses. The penalties assessed by the Commission were lawful and reasonably accounted for the Carriers' ability to pay and the egregiousness of their conduct. And because the Carriers were provided a statutory right to a jury trial before they would have been required to pay any penalties, their Seventh Amendment claim is without merit. We therefore deny the petitions for review.

So ordered.