ORAL ARGUMENT NOT YET SCHEDULED
Nos. 24-1224, 24-1225

**IN THE UNITED STATES COURT OF APPEALS**
**FOR THE DISTRICT OF COLUMBIA CIRCUIT**

SPRINT CORPORATION,
*Petitioner*,
v.
FEDERAL COMMUNICATIONS COMMISSION and
UNITED STATES OF AMERICA,
*Respondents*.

T-MOBILE USA, INC.,
*Petitioner*,
v.
FEDERAL COMMUNICATIONS COMMISSION and
UNITED STATES OF AMERICA,
*Respondents*.

On Petitions For Review Of Forfeiture Orders In
*In re Sprint Corp.*, File No. EB-TCD-18-00027700, FCC 24-42; and
*In re T-Mobile USA, Inc.*, File No. EB-TCD-18-00027702, FCC 24-43

# PETITIONERS' OPENING BRIEF

Helgi C. Walker
Russell B. Balikian
Zachary E. Tyree
Nathaniel J. Tisa
GIBSON, DUNN & CRUTCHER LLP
1700 M Street, N.W.
Washington, D.C. 20036-4504
hwalker@gibsondunn.com
rbalikian@gibsondunn.com
(202) 955-8500

*Counsel for Petitioners*

## CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28, Petitioners submit this Certificate as to Parties, Rulings, and Related Cases:

### Parties

Petitioners in these consolidated cases are T-Mobile USA, Inc. and Sprint Corporation.[1] Respondents are the Federal Communications Commission and the United States of America. No intervenors or *amici* have been involved to date.

### Rulings Under Review

Petitioners seek review of the FCC's forfeiture orders in *In re Sprint Corp.*, File No. EB-TCD-18-00027700, FCC 24-42, and *In re T-Mobile USA, Inc.*, File No. EB-TCD-18-00027702, FCC 24-43, which were released on April 29, 2024.

### Related Cases

The following cases are related: *AT&T, Inc. v. FCC*, No. 24-60223 (5th Cir.); and *Verizon Commc'ns, Inc. v. FCC*, No. 24-1733 (2d Cir.).

---

[1] Petitioner T-Mobile USA, Inc.'s corporate parent, T-Mobile US, Inc. merged with petitioner Sprint Corp. in 2020. Petitioner Sprint Corp. converted to a limited liability company in 2021 and is now known as Sprint LLC, which is a subsidiary of petitioner T-Mobile USA, Inc.

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

Page(s)

**CASES**

**CONSTITUTIONAL PROVISIONS**



**STATUTES**

**REGULATIONS & ADMINISTRATIVE ORDERS**

**OTHER AUTHORITIES**

## GLOSSARY

| | |
|---|---|
| *2007 CPNI Order* | *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) |
| *2013 CPNI Ruling* | *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609 (2013) |
| Act | The Communications Act of 1934 |
| Companies | Petitioners T-Mobile USA, Inc. and Sprint Corp. |
| CPNI | Customer Proprietary Network Information |
| CTIA Guidelines | CTIA's Best Practices and Guidelines for Location Based Services |
| FCC or Commission | Federal Communications Commission |
| LBS | Location-Based Service |
| NAL | Notice of Apparent Liability |
| Orders | The forfeiture orders imposed on the Companies in *In re Sprint Corp.*, File No. EB-TCD-18-00027700, FCC 24-42 (released Apr. 29, 2024), and *In re T-Mobile USA, Inc.*, File No. EB-TCD-18-00027702, FCC 24-43 (released Apr. 29, 2024) |

## INTRODUCTION

In April 2024, a bare majority of the Federal Communications Commission ("FCC") imposed nearly $200 million in total civil penalties on four major wireless carriers, including more than $92 million in penalties on petitioners T-Mobile USA, Inc. and Sprint Corp. (the "Companies") in the orders under review (the "Orders"). The FCC concluded that essentially the entire wireless industry had violated the law by continuing to operate location-based service ("LBS") programs—programs that enabled wireless customers to access valuable location-based services, like AAA's roadside assistance—after a *New York Times* article reported that a single, rogue actor had misused those programs. The FCC based its retroactive punishment on an utterly novel construction of the governing statute, holding, for the first time, that the mobile-device-location information used in those LBS programs was "customer proprietary network information" ("CPNI") and thus subject to existing FCC rules and enforcement authority.

The Companies care deeply about the privacy of their customers. That is why, throughout the life of their LBS programs, the Companies took numerous, industry-standard measures to protect the device-

location information used in the LBS programs, structuring the programs to ensure that device-location information was made available only with the express consent of the customer. And after the article, they responded swiftly yet prudently by, among other things, quickly shutting off the offending entity's access to device-location information. Within a few months, both Companies decided to wind down their LBS programs completely.

The Orders are fundamentally flawed. For at least five reasons, the Court should vacate them.

*First*, the FCC's unilateral imposition of tens of millions of dollars in civil penalties violates the Companies' jury-trial rights under the Seventh Amendment and Article III. The Supreme Court recently confirmed in *SEC v. Jarkesy*, 144 S. Ct. 2117 (2024), that when an agency seeks civil penalties for alleged statutory violations, the claims must be tried before a jury in a neutral federal court—particularly where, as here, the claims are analogous to common-law claims. Affording each Company a jury trial in an Article III court also protects against the due-process and separation-of-powers problems inherent in the FCC's acting

as rule-maker, investigator, prosecutor, judge, and jury—additional constitutional errors that infected these proceedings.

*Second*, the Orders exceed the FCC's statutory authority because the location information at issue is not CPNI, as required by the Communications Act of 1934, as amended ("Act"). The Orders focus on location information that cell towers generate when a mobile device registers with a wireless network—including when the device is sitting idle or retrieving Internet data. Section 222 of the Act, however, defines CPNI to focus exclusively on "call location information"—*i.e.*, information related to the "location … of use of a telecommunications service"—that is made available to the carrier "solely by virtue of" the customer contracting for *voice* services. 47 U.S.C. § 222(d)(4), (f)(1), (h)(1)(A). The device-location information used in the LBS programs was not call-location information, and it was not made available to the Companies only because of a voice-services relationship between the Companies and the customers. The FCC's claim that all device-location information is CPNI thus contradicts the Act, as statutory context, history, and regulatory guidance confirm.

*Third*, the Orders violate fundamental principles of fair notice. The FCC adopted its broad view of CPNI for the first time in these enforcement proceedings, after the conduct had already occurred. The FCC's previous discussions of CPNI had addressed only *call*-related location information, and the FCC even denied a request for rulemaking to clarify the scope of carriers' CPNI obligations regarding location information. The FCC cannot impose massive penalties on past conduct based on a newly announced interpretation of CPNI.

*Fourth*, the FCC's hindsight-based liability findings are arbitrary and capricious. The FCC's rules require only that carriers "take reasonable measures" to guard against "unauthorized access to CPNI." 47 C.F.R. § 64.2010(a). The Companies' LBS programs satisfied that standard. Among other safeguards, the Companies limited the number of entities with direct access to device-location information, ensured that LBS providers were vetted before allowing them to participate in the LBS programs, and required express customer consent before sharing device-location information. The Companies also responded promptly to the *New York Times* article and acted well within the bounds of reason in winding down their LBS programs over time, rather than immediately

shutting down valuable and even life-saving services. The FCC fails to adequately explain why the Companies' responses to the *New York Times* article were purportedly unreasonable when the FCC itself knew about the incident reported in the article for months before it was published, yet never informed the Companies. Viewed objectively and as a whole, the Companies' actions were reasonable.

*Fifth*, the penalties imposed are unlawful, arbitrary, and capricious. The FCC faulted each Company for failing to immediately shut down its LBS program after the *New York Times* article was published—a single, continuing failure to act subject to an inflation-adjusted statutory maximum penalty of just over $2 million. 47 U.S.C. § 503(b)(2)(B). To avoid that cap, the FCC artificially subdivided each Company's single purported failure to terminate its LBS program into many individual violations—resulting in fines exponentially higher than the statute allows. In addition, the FCC did not adequately justify the large forfeitures here in light of its past practice, which has saved massive penalties for cases involving fraud or significant, proven harm.

This Court should grant the petition, vacate the FCC's Orders, and order that the penalty amounts be refunded to the Companies.

## JURISDICTIONAL STATEMENT

This Court has subject-matter jurisdiction under 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1). The petitions for review challenge final Orders released by the FCC on April 29, 2024. The Companies paid the penalties under protest, securing jurisdiction in this Court under § 402(a). *AT&T Corp. v. FCC*, 323 F.3d 1081, 1083-85 (D.C. Cir. 2003). The Companies timely petitioned for review on June 27, 2024. 28 U.S.C. § 2344.

## STATUTES AND REGULATIONS

Pertinent statutes and regulations are set forth in the addendum filed with this brief.

## STATEMENT OF ISSUES

1. Whether the FCC violated the Seventh Amendment, Article III, and/or due process by directly imposing civil penalties through administrative proceedings.

2. Whether the Orders exceed the FCC's statutory authority because the location information at issue is not CPNI as defined in 47 U.S.C. § 222(h)(1).

3. Whether the FCC failed to provide fair notice of the novel interpretation of CPNI on which the Orders are based.

4. Whether the FCC acted arbitrarily and capriciously in concluding that the Companies failed to take reasonable measures to safeguard the location information at issue, and were thus liable under 47 C.F.R. § 64.2010(a).

5. Whether penalties of more than $80 million and $12 million unlawfully exceed the inflation-adjusted statutory maximum of approximately $2 million for a single continuing violation, 47 U.S.C. § 503(b)(2)(B), and/or are arbitrarily and capriciously excessive and disproportionate.

## STATEMENT OF THE CASE

### A. Legal Framework

At all relevant times, T-Mobile and Sprint both offered wireless voice and data services. JA4 ¶ 8; JA289 ¶ 8. Those two distinct types of wireless service—voice and data—were subject to dramatically different regulatory requirements under the Act.

Wireless *voice* services are "'telecommunications services' under Title II of the Act." *Mozilla Corp. v. FCC*, 940 F.3d 1, 17 (D.C. Cir. 2019)

(per curiam); *see* JA2 ¶ 2 n.7 (citing 47 U.S.C. § 153(53)).[2] Telecommunications services are heavily regulated under the Act—they receive "common carrier status" and are subject to "an array of statutory restrictions and requirements" set forth in Title II. *Mozilla*, 940 F.3d at 17.

By contrast, wireless *data* services—such as Internet access and texting—were not telecommunications services during the time period relevant to this case. Rather, wireless data services were classified as "'information services' under Title I" of the Act that were "exempted from common carriage status and, hence, Title II regulation." *Mozilla*, 940 F.3d at 17; *see Restoring Internet Freedom*, 33 FCC Rcd 311 (2018); *Petitions for Declaratory Ruling on Regul. Status of Wireless Messaging Serv.*, 33 FCC Rcd 12075 (2018).[3] Where, as here, the same company

[2] Because both Orders at issue here contain substantially similar reasoning, this brief typically cites only the T-Mobile forfeiture order, except where context warrants otherwise.

[3] The FCC recently issued an order classifying broadband Internet access service as a "telecommunications service." *Safeguarding and Securing the Open Internet*, 89 Fed. Reg. 45,404 (May 22, 2024). That order, however, postdated the events at issue in this case, and it has, in any case, been stayed pending review. *See In re MCP No. 185*, 2024 WL 3650468 (6th Cir. Aug. 1, 2024) (per curiam).

offers both a Title II telecommunications service and a Title I information service, it is treated as a Title II common carrier "only to the extent that it is engaged in providing telecommunications services." 47 U.S.C. § 153(51); *see Cellco P'ship v. FCC*, 700 F.3d 534, 538 (D.C. Cir. 2012).

This case involves an FCC regulation adopted under Title II. Section 222 of the Act requires telecommunications carriers to protect the confidentiality of "customer proprietary network information," or CPNI. 47 U.S.C. § 222(a). The FCC has read that provision to require carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a).

As relevant here, CPNI refers only to information that satisfies two statutory requirements, both of which require a close link to a Title II "telecommunications service" (*i.e.*, a voice service). 47 U.S.C. § 222(h)(1)(A). First, the information must "relat[e] to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier." *Id.* Second, the information must have been "made available to the carrier by the customer solely by virtue of the carrier-customer relationship." *Id.*

The original CPNI definition did not mention "location" information. "Location" was added in 1999, when Congress amended § 222 to protect "call location information," while ensuring that it could still be used in emergencies. 47 U.S.C. § 222(d)(4), (f)(1); *see* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, sec. 5, 113 Stat. 1286, 1288-89.

Prior to this enforcement action, the FCC had never claimed that CPNI includes location information beyond the "call location information" referenced in § 222. The 2007 FCC order adopting 47 C.F.R. § 64.2010, for example, listed only call-related information when describing CPNI, including "the phone numbers called by a consumer" and "the frequency, duration, and timing of such calls." 22 FCC Rcd 6927, at ¶ 5 (2007) ("*2007 CPNI Order*").[4] And in 2013, the FCC specifically linked the CPNI definition's reference to "location" information to voice calls, stating that CPNI includes "the location of the device *at the time of the calls*" and the "location of a *customer's use of a telecommunications service*," while also acknowledging that CPNI does not include information that "pertains to the device's *access of the carrier's data*

[4] https://docs.fcc.gov/public/attachments/FCC-07-22A1.pdf.

*network*." 28 FCC Rcd 9609, at ¶¶ 22, 28 & n.66 (2013) ("*2013 CPNI Ruling*") (emphasis added).[5]

If a carrier violates its CPNI obligations, the FCC may seek a "forfeiture penalty," either by proceeding before an FCC administrative law judge, 47 U.S.C. § 503(b)(3), or by imposing a penalty itself, *id.* § 503(b)(4). In either case, Congress capped the forfeiture amount for continuing violations at roughly $2 million "for any single act or failure to act." *Id.* § 503(b)(2)(B); *see Amend. of Section 1.80(b) of the Commission's Rules*, 34 FCC Rcd 12824, 12828 (2019) (setting 2020 inflation-adjusted cap at $2,048,915).

### B. Factual Background

#### 1. Location-Based Services

This case involves the LBS programs that the Companies made available to their customers until 2019, when each Company wound down its program.

A location-based service, or LBS, refers to a mobile app or other service that "combine[s] information about a user's physical location with online connectivity." FCC, *Location-Based Services: An Overview of*

[5] https://docs.fcc.gov/public/attachments/FCC-13-89A1_Rcd.pdf.

*Opportunities and Other Considerations* 1 (May 2012).[6] Today, many LBS offerings—such as maps and rideshare apps—interface directly with on-device GPS data. JA127 ¶ 12 n.48. But when the Companies initiated their LBS programs more than a decade ago, not all wireless customers owned handsets with on-device GPS functionality, and not all those who did wanted to use GPS data to access LBS offerings. JA210. The Companies' LBS programs—like those of other major wireless carriers—served those customers by enabling them to share network-based location information with LBS providers. JA210.

The Companies' LBS programs generated location information by approximating the location of the customer's mobile device based on its registration with network-signal towers. JA126-27 ¶ 12 & n.48; JA165; JA215; JA407; JA427; JA10 ¶ 23. Customers could then choose to share that network-based device-location data with approved LBS providers to access their services. JA210; *see* JA423. Dozens of LBS providers participated in the Companies' LBS programs, including well-known companies like Life Alert, AAA, and Allstate. JA210; JA424-27. The services available were varied and valuable, including emergency-

[6] https://docs.fcc.gov/public/attachments/DOC-314283A1.pdf.

response services, roadside assistance, workforce applications, concierge services, bank-fraud-prevention services, and shipment tracking. JA424-27; *see* JA210.

Importantly, the device-location information used in the LBS programs was *not* tied to call-location information. Mobile devices periodically register with nearby signal towers when they are powered on, "even when the customer does not have an active established connection, such as a voice call or data usage." JA126 ¶ 12; *see* JA165; JA215; JA407-08; JA427; JA10 ¶ 23; JA296 ¶ 24. The Companies used that registration data to approximate the location of a mobile device. JA126 ¶ 12; *see also*, *e.g.*, JA165.

The Companies used two location aggregators, LocationSmart and Zumigo, to facilitate their LBS programs. JA214-15; JA424. Those aggregators, in turn, contracted with LBS providers (sometimes via a sub-aggregator), which offered and provided services directly to customers. JA215; JA409. For example, if a T-Mobile customer needed roadside assistance, she would contact an LBS provider (*e.g.*, AAA), which—after obtaining her consent—would contact a location aggregator (LocationSmart or Zumigo) to request her device's approximate location.

The aggregator, upon verifying the customer's consent, would then obtain network-based location information from the relevant carrier (T-Mobile) and provide it to the LBS provider (AAA). Because LocationSmart and Zumigo each contracted with all major carriers, the LBS provider did not need to know to which carrier the customer subscribed. And because the aggregators also contracted with many LBS providers, the Companies were able to include many LBS providers in their programs.

The Companies structured their LBS programs with numerous safeguards to protect the security and privacy of their customers' device-location information. Only LocationSmart and Zumigo had direct access to customers' location data, and the Companies required both aggregators—and through them, all LBS providers with which they contracted—to comply with industrywide standards set forth in CTIA's Best Practices and Guidelines for Location Based Services ("CTIA Guidelines").[7] JA215-16; JA413. Consistent with CTIA Guidelines, the Companies required that LBS providers give customers clear notice

[7] The CTIA Guidelines are available at: https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services. CTIA is a trade association representing the U.S. wireless communications industry.

regarding how their location information would be used, disclosed, and protected, and they further required aggregators to obtain a customer's express consent before disclosing the customer's location information to an LBS provider. JA247; JA290 ¶ 9. Both Companies also required maintenance of customer-consent records. JA247; JA561-62. And the Companies required that users be allowed to revoke consent and report abuse. JA246-47; JA558-62.

The Companies also implemented processes to verify how LBS providers planned to use and protect customers' location data. T-Mobile required aggregators to seek preapproval for each distinct service (or "campaign") an LBS provider might offer, and it assigned each campaign a unique identifier that allowed T-Mobile to monitor specific requests for location information. JA247; JA215-16; JA86. As part of its preapproval process for each campaign, T-Mobile evaluated the LBS provider's business, proposed service, opt-in procedures, opt-in messages, and privacy language, among other things. JA215-16; JA261. T-Mobile also commissioned external risk assessments of its LBS program in 2016 and 2018. JA226-27. Both assessments concluded that the aggregators were

properly obtaining customer consent prior to collecting, using, and disclosing location information. JA226-27.

Sprint likewise had a "Certification" process that required the aggregators to test LBS providers' applications "to ensure they met Sprint's notice, privacy, and data security requirements" before granting LBS providers access to customer location information. JA290-91 ¶ 10; *see* JA544, 551. Sprint also had the right to audit compliance with that certification requirement. JA291 ¶ 12; JA556-57; JA410. Both Companies could also terminate or suspend an aggregator's or LBS provider's access immediately for non-compliance. JA248; JA551, 554.

T-Mobile in particular had evidence indicating that its established safeguards worked. In 2017, T-Mobile learned through an investigation that an LBS provider, LocateUrCell, may have been misusing its approved campaign (a phone-finding service) for unapproved purposes. T-Mobile reached out to LocationSmart about the issue in September, and it learned that LocationSmart had already investigated LocateUrCell and disabled its access effective August 22. JA225-26.

### 2. The Securus Incident And The Companies' Responses

In May 2018, the *New York Times* reported that LBS provider Securus Technologies, which offers prison telecommunications services, may have been misusing its access to carriers' LBS programs.[8] The Companies—along with the other major wireless carriers—had authorized Securus to access location information to operate a consent-based "[g]eofencing" service designed to ensure that the recipient of an inmate call was not within a certain distance of the detention facility. JA217. Securus obtained that information through sub-aggregator 3CInteractive. JA217.

According to the article, however, Securus also operated a separate, unauthorized service allowing law enforcement to track a suspect's wireless device, purportedly based on a valid warrant or other legal process. JA217. Securus masked that unauthorized use behind its geofencing campaign, JA218, and apparently did not review the legal documents that were used to justify the unauthorized tracking requests.

---

[8] *See* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.

Between 2014 and 2017, a Missouri sheriff, Cory Hutcheson, exploited Securus's unauthorized service to access location information without uploading valid legal process. JA7-8 ¶¶ 14-15; JA184. Hutcheson was criminally charged and pleaded guilty to federal crimes. JA7 ¶ 15.

The FCC knew of Sheriff Hutcheson's unauthorized location tracking long before the *New York Times* article was published. In August 2017, a consumer-advocacy group specifically raised the issue in letters to the FCC when opposing an application to transfer control of Securus. *See Joint Application of Securus Investment Holdings, LLC et al.*, Letters from Wright Pet'rs, WC Dkt. No. 17-126 (Aug. 4 & 5, 2017).[9] But while the FCC acknowledged the concerns, it nevertheless approved the applications. *Joint Application of Securus Inv. Holdings, LLC*, 32 FCC Rcd 9564, at ¶ 28 (2017).[10] The FCC did not notify the Companies of any concerns with their LBS programs at that time. Rather, the Companies did not learn of that misuse until the *New York Times* article was published nine months later.

---

[9] https://www.fcc.gov/ecfs/document/10804689721322/1; https://www.fcc.gov/ecfs/document/10805871110099/1.

[10] https://www.fcc.gov/ecfs/document/1030133504695/1.

Both Companies responded quickly. On May 11, 2018—the day after the article was published—T-Mobile terminated Securus's and 3CInteractive's access to location information for any purpose, and T-Mobile directed LocationSmart to do the same. JA218. T-Mobile also investigated the incident, JA91, and in July 2018, it notified the aggregators that it would terminate its LBS program effective December 9, 2018, JA233 (LocationSmart); JA234 (Zumigo). In November 2018, T-Mobile agreed to extend the termination date by three months to "ensure a smooth wind down of the program without the added pressure of terminating the program during the holidays." JA231-32.

On January 8, 2019, however, *Motherboard* published an article claiming to have paid a "bounty hunter" to obtain a phone's approximate location through LBS provider Microbilt. Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8, 2019).[11] Although the phone owner (who happened to be a T-Mobile customer) "gave their consent to Motherboard to be tracked," the article suggested that unscrupulous users of Microbilt's verification service could, for a fee,

[11] https://www.vice.com/en/article/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile/.

obtain location information about customers on "all mobile networks" by submitting requests under false pretenses. *Id.*

T-Mobile terminated Microbilt's access on January 4, 2019, the day after it learned of the Microbilt allegations (before the article was published), JA175; JA92, 117, and it also then accelerated the shutdown of its LBS program. It terminated services for many LBS providers on January 14, and continued to phase them out through February 8, when it terminated the final, most important campaigns (such as emergency services and roadside assistance). JA169; *see* JA208; JA195.

Sprint likewise responded promptly to news of the Securus incident. It immediately began an investigation, terminated Securus's access on May 17, 2018, and suspended LocationSmart from its LBS program on May 25. JA293 ¶ 15; JA429. On June 20, Sprint terminated the entire LocationSmart contract effective immediately and triggered the 90-day notice to terminate Zumigo's contract. JA293 ¶ 15; JA429. In August 2018, Sprint signed two new, short-term agreements with LocationSmart that allowed only AAA and a second LBS provider (offering state-lottery-related services) to access location information. JA429-30; JA437; JA468. Those enhanced contracts required an

independent third-party audit of LocationSmart's practices. JA449; JA480. Around that same time, Sprint also adopted a requirement that the aggregators submit detailed reports to Sprint about aggregators' and LBS providers' use of location information. JA293-94 ¶ 16.

In late October 2018, Sprint temporarily reinstated Zumigo's contract to provide location services "to particular anti-fraud and anti-identity theft services." JA430; JA435-36. But Sprint terminated that contract on January 9, 2019, the day after the Microbilt article ran, JA406-07, 413, and it terminated services for the final two LBS providers by May 31, 2019, JA407.

### C. The FCC's Forfeiture Orders

On February 28, 2020, the FCC issued separate Notices of Apparent Liability ("NALs") against all four major wireless carriers. JA121; JA362. In the NALs, the FCC claimed—for the first time—that device-location information is CPNI even if not linked to a voice call. JA135-36 ¶ 43. On that basis, the FCC concluded that all four carriers had apparently violated § 222 and 47 C.F.R. § 64.2010(a) by purportedly failing to take reasonable measures to protect their customers' location data. The FCC proposed more than $200 million in total penalties,

including a $91.6 million penalty against T-Mobile and a $12.2 million penalty against Sprint. Commissioner O'Rielly wrote separately to raise serious concerns with the NALs' factual and legal bases. JA155.

The NALs did not identify a single T-Mobile or Sprint customer whose location information was accessed without authorization after Hutcheson's criminal conduct (which, the NALs acknowledged, fell outside the statute of limitations, JA148 ¶ 85). Instead, the FCC's theory was that Hutcheson's criminal misuse of a single, unauthorized service (Securus) suggested that each carrier's then-existing LBS program *as a whole* lacked "reasonable measures" to protect CPNI. 47 C.F.R. § 64.2010(a). The only feasible way for any carrier to avoid liability under that theory would have been to shut down its entire LBS program immediately. JA148 ¶ 84.

To generate the headline-grabbing penalty amounts and avoid the statutory maximum, the NALs posited that the Companies committed "separate continuing violations" as to each aggregator and LBS provider that was allowed to access location data 30 days after the *New York Times* article. JA148 ¶ 84. The NALs piled on by proposing upward adjustments of 75% (T-Mobile) and 100% (Sprint) because of the

purported severity of the violations, JA150; JA391, which produced, in T-Mobile's case, what was then the third-largest proposed penalty in the FCC's history, JA122.

The Companies filed written responses to the NALs, explaining that the device-location information used in the LBS programs was not CPNI, that the FCC's application of a new CPNI definition violated fair-notice principles, that the Companies took reasonable measures to protect device-location information, and that the proposed penalties exceeded the statutory cap and were factually unsupported. *See* JA58; JA330. The Companies also argued that imposing the proposed penalties would violate the Seventh Amendment and Article III, among other constitutional provisions. *See* JA54.

On April 29, 2024—more than four years after the NALs—the FCC issued the Orders against the Companies. The majority adopted each of the positions set forth in the NALs, except that it reduced the penalty against T-Mobile due to a counting error. JA39-40 ¶¶ 93-95. The FCC thus imposed an $80,080,000 penalty against T-Mobile and a $12,240,000 penalty against Sprint. JA1-2 ¶ 1; JA286-87 ¶ 1.

Two Commissioners dissented. Commissioner Carr explained that while he originally supported the NALs, "[n]ow that the investigations are complete," he could not support the Orders. JA50. He concluded that the Companies' LBS programs "plainly fall outside the scope of the FCC's section 222 authority," that the Orders' "newfound" and expansive definition of CPNI "finds no support in the Communications Act or FCC precedent," and that the "eye-popping," "retroactiv[e]" forfeitures were thus "inconsistent with the law and basic fairness." JA50. Commissioner Simington focused specifically on the penalty amounts, explaining that they "exceed[ed] [the] statutory maximum" and that there was no basis for finding that a carrier's "single, systemic failure" to shut down the LBS program could be subdivided into many separate violations. JA53.

## SUMMARY OF ARGUMENT

The FCC's Orders are unlawful for at least five reasons:

I. By imposing civil penalties on the Companies outside the context of a jury trial in a federal court, the Orders violate the Seventh Amendment and Article III. *Jarkesy*, 144 S. Ct. 2117. Civil penalties are a prototypical common-law remedy, which "effectively decides" that the Seventh Amendment applies. *Id.* at 2130. And the FCC's claim that the

Companies failed to take "reasonable measures" to protect location information is analogous to a common-law negligence claim historically decided by juries. The public-rights exception, which is narrowly limited to historic categories of cases, does not apply. Accordingly, the FCC must pursue its claims before a jury in federal court. The Seventh Amendment's protections are especially important in the context of FCC enforcement actions because they prevent the FCC from improperly acting as rule-maker, investigator, prosecutor, judge, and jury, in violation of due process and separation-of-power principles.

II. The Orders also exceed the FCC's statutory authority. Under the Act, information is not CPNI unless it (1) relates to the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service," *and* (2) "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). Regarding the first prong, information about the "location … of use of a telecommunications service" can refer only to "call location information"—the phrase Congress contemporaneously used when it amended § 222 to cover location information, *see id.* § 222(d)(4), (f)(1). The LBS program, by contrast, used device-location information

derived from cell-tower registrations. That information does not relate to the location at which a "telecommunications service" is "use[d]." As to the second prong, network-based device-location information is not made available to the carrier "solely" because of the carrier-customer relationship—that is, solely because of voice services. The location information at issue supported *both* data and voice services; indeed, both Companies had data-only customers who did not subscribe to any voice services. The location information at issue therefore is not CPNI.

III. Further, the FCC did not give the Companies fair notice that it considered non-call-location information CPNI. In fact, the FCC's prior statements all indicated that *only* call-location information would count. At the very least, then, the Companies' view of the statute was reasonable and consistent with existing guidance, and the FCC failed to provide ascertainable certainty of what § 222 purportedly required. *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995).

IV. The Orders should also be set aside because they are arbitrary and capricious in concluding that the Companies failed to take "reasonable measures" to protect location information. 47 C.F.R. § 64.2010(a). Both before and after the Securus incident (which is not

itself the basis for the penalties), the Companies implemented numerous safeguards to protect device-location information. They restricted direct access to only two aggregators, they required express customer consent, and they utilized only LBS providers whose processes had been vetted. The Companies also responded reasonably to the Securus incident, promptly cutting off Securus's access and then, after further investigation, moving to terminate their entire LBS programs on timelines that would not unduly disrupt customers. All major carriers took a similar approach. The FCC's hindsight-based standard—that each Company needed to immediately terminate its *entire* LBS program following the *New York Times* article—would have created a disorderly wind-down and harmed customers by too quickly cutting off valuable, even life-saving services. Particularly given the lack of any guidance or fair notice of that draconian rule, the Companies' phased response was reasonable. The Orders are arbitrary and capricious in holding otherwise.

V. Finally, the FCC's penalties are in all cases unlawful. The FCC far exceeds the statutory maximum by counting one continuing failure to act as dozens of individual violations, based on a limitless view

of the FCC's statutory authority. 47 U.S.C. § 503(b)(2)(B). The FCC also failed to explain adequately why the facts here warranted imposing on T-Mobile a forfeiture amount equivalent to those imposed only on the worst offenders.

## STANDARD OF REVIEW

A petition for review should be granted if agency action 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)). Legal questions are reviewed de novo. *Lake Region Healthcare Corp. v. Becerra*, 113 F.4th 1002, 1007 (D.C. Cir. 2024); *Nat'l Lifeline Ass'n v. FCC*, 983 F.3d 498, 507 (D.C. Cir. 2020). An agency's action is arbitrary and capricious if it is not "'reasonable and reasonably explained,'" which requires "'a rational connection between the facts found and the choice made.'" *Ohio v. EPA*, 144 S. Ct. 2040, 2053 (2024).

## ARGUMENT

### I. The Orders Violate The Seventh Amendment And Article III

The Orders should be vacated because the Seventh Amendment and Article III bar the FCC from directly imposing civil penalties. As the

Supreme Court recently held in *Jarkesy*, agency claims seeking civil penalties must be tried by a jury before a constitutionally independent Article III judge.

### A. Civil Penalties Under Federal Law Require A Jury Trial In An Article III Court

The Seventh Amendment guarantees "the right of trial by jury" in "Suits at common law." U.S. Const. amend. VII. As *Jarkesy* confirms, that right to a jury trial in an Article III court "extends to" all federal suits not within equity or admiralty jurisdiction, including statutory claims that are "legal in nature." 144 S. Ct. at 2128. Courts consider both the nature of "the cause of action and the remedy it provides" in determining whether a suit is legal; the remedy is the "more important" factor. *Id.* at 2129.

The remedy ordered here—civil penalties—"is all but dispositive" of the Seventh Amendment's applicability. *Jarkesy*, 144 S. Ct. at 2129; *see* 47 U.S.C. § 503(b)(1) (authorizing "forfeiture penalt[ies]"). Civil penalties are "a type of remedy at common law that could only be enforced in courts of law." *Jarkesy*, 144 S. Ct. at 2129. They are intended to "punish or deter," not, as with equitable relief, to "restore the status quo." *Id.* In *Jarkesy*, for example, the civil penalties the government sought

under the securities laws were punitive (and thus implicated the Seventh Amendment) because the statute focused on culpability and deterrence, rather than the victim's loss, and because the government itself could retain any recovery secured. *Id.* at 2129-30. The same was true in *Tull v. United States*, where the government sought civil penalties under the Clean Water Act. 481 U.S. 412, 418-25 (1987).

Those decisions control here because, like the SEC in *Jarkesy*, the FCC imposed civil penalties meant to punish or deter. The FCC imposed civil penalties on T-Mobile and Sprint exceeding $80 million and $12 million, respectively. As required by statute, *see* 47 U.S.C. § 503(b)(2)(E), the FCC purported to base those penalties on, among other factors, the "gravity of the violation," the "degree of culpability," and "any history of prior offenses," along with the penalties' potential to "act as a powerful deterrent." JA9-10 ¶ 21; JA35-38 ¶¶ 81, 85, 91. The consideration of "culpability, deterrence, and recidivism" reflects an intent to punish. *Jarkesy*, 144 S. Ct. at 2129. The penalties also accrue to the FCC, not any purportedly harmed consumer. *See id.* at 2129-30. The penalties are

thus legal remedies, which "effectively decides" that the Seventh Amendment applies. *Id.* at 2130.[12]

The "close relationship" between the charges against the Companies and common-law claims "confirms that conclusion." *Jarkesy*, 144 S. Ct. at 2130. An action to recover a civil monetary penalty is a suit at common law, analogous to an action in debt. *Tull*, 481 U.S. at 418-20. And substantively, the FCC's claim is analogous to a common-law negligence claim. Both the FCC's claim under 47 C.F.R. § 64.2010(a) and common-law negligence "target the same basic conduct," *Jarkesy*, 144 S. Ct. at 2130, by imposing a duty of care to refrain from unreasonable actions that might harm others. *Compare* 47 U.S.C. § 222(a) (imposing a "duty to protect the confidentiality of" CPNI), *and* 47 C.F.R. § 64.2010(a) ("carriers must take reasonable measures"), *with Air & Liquid Sys. Corp. v. DeVries*, 586 U.S. 446, 452 (2019) (negligence imposes a "'duty to exercise reasonable care' on those whose conduct

[12] The *Jarkesy* dissent correctly recognized that the FCC's civil penalty framework would be affected by the decision. *See* 144 S. Ct. at 2174-75 (Sotomayor, J., dissenting).

presents a risk of harm to others"); *see also* JA46 ¶ 108 (relying on 47 U.S.C. § 222 and 47 C.F.R. § 64.2010(a) to impose the penalties).[13]

### B. The FCC's Counterarguments Are Unpersuasive

The FCC has attempted to justify the imposition of a civil penalty without a jury on two grounds. Neither is persuasive.

#### 1. The Public-Rights Exception Is Inapplicable

In the Orders, the FCC first argued that the forfeitures fall within the "public rights" exception, which allows agencies to adjudicate certain matters without violating Article III or the Seventh Amendment. JA43-45 ¶¶ 104-05. That limited exception is inapplicable here.

Article III vests "[t]he judicial Power of the United States" in the federal courts. U.S. Const. art. III, § 1. Congress therefore may not assign to an agency "'any matter which, from its nature, is the subject of a suit at the common law, or in equity, or admiralty.'" *Jarkesy*, 144 S. Ct. at 2134 (quoting *Murray's Lessee v. Hoboken Land & Improvement Co.*,

[13] The actions of third parties who misused private location data would likewise implicate common-law claims, including fraud, intrusion upon seclusion, eavesdropping, and principles of bailment and conversion—further confirmation of the close relationship between this case and the common law.

59 U.S. (18 How.) 272, 284 (1856)). Suits "concerning private rights" therefore "may not be removed from Article III courts." *Id.* at 2132.

By contrast, cases involving only public rights "historically could have been determined exclusively by the executive and legislative branches." *Jarkesy*, 144 S. Ct. at 2132 (quoting *Stern v. Marshall*, 564 U.S. 462, 493 (2011)) (brackets omitted). But that limited, specific "class of cases" is "an *exception*" to the normal rule of Article III adjudication and is restricted to "historic categories." *Id.* at 2132-34; *see id.* at 2146 (Gorsuch, J., concurring) ("public rights are a narrow class defined and limited by history"). Public-rights cases include those involving the collection of government revenue, immigration, tribal relations, public-land administration, and the granting of public benefits, pensions, and patent rights. *Id.* at 2132-33 (majority). The "presumption is in favor of Article III courts." *Id.* at 2134.

The FCC's claim does not fit any recognized category of public rights. In the Orders, the FCC argued that the public-rights exception applies because the enactment of § 222 "'created new statutory obligations'" beyond those recognized at common law. *E.g.*, JA44 ¶ 104. *Jarkesy* rejected that reasoning, however, holding that a claim does not

involve public rights simply because it has "statutory origins" or is brought by the government. 144 S. Ct. at 2136. What matters is whether the claim resembles a common-law cause of action and whether the agency has imposed civil penalties, which "could only be enforced in courts of law." *Id.* As explained above, both factors are present here.

The public-rights exception therefore does not apply, and any penalties can be imposed only by a jury before a constitutionally independent federal judge.

### 2. Section 504(A) Collection Actions Are No Substitute For A Jury Trial

In the AT&T LBS appeal, the FCC has raised another novel argument: that by seeking judicial review of a forfeiture order under 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1), a regulated entity *waives* the right to a jury trial. That strained argument fails at every step.

The Companies raised the Seventh Amendment before the FCC, arguing that a jury trial is necessary for civil penalties. *See* JA55. The FCC rejected that argument and imposed millions of dollars in penalties without a jury trial. JA40-46 ¶¶ 97, 104-05, 108-09. The Companies are now appealing the FCC's rejection of the Seventh Amendment argument and imposition of penalties. By paying the penalties (under protest) and

then challenging the Orders in this Court—including on the ground that they are unconstitutional—the Companies followed the judicial-review process this Court laid out in *AT&T*, 323 F.3d at 1083-85. Invoking that judicial-review process did not waive the Companies' respective rights to a jury trial.

The FCC's contrary view rests on misapplying 47 U.S.C. § 504(a). That provision allows the Department of Justice to bring a *collection action* against entities who *refuse to pay* FCC forfeiture orders, providing that "any suit for the recovery of a forfeiture … shall be a trial de novo." 47 U.S.C. § 504(a). The FCC assumes that in a § 504(a) action, all legal and factual defenses are reviewable de novo. But that assumption is not necessarily correct. At least some courts have held that in a § 504(a) suit, review is limited—*e.g.*, defendants may raise only "a factual defense" to a forfeiture order, not a "challenge" to the order's "legal validity." *United States v. Stevens*, 691 F.3d 620, 622-23 (5th Cir. 2012); *see United States v. Hodson Broad.*, 666 F. App'x 624, 627-28 (9th Cir. 2016); *United States v. Olenick*, 2019 WL 2565280, at *3 (W.D. Tex. Apr. 2, 2019). And while this Court has stated that all issues would be subject to de novo review, *AT&T*, 323 F.3d at 1083-85 (discussing *Pleasant Broad. Co. v. FCC*, 564

F.2d 496 (D.C. Cir. 1977)), the government could assure more limited review by bringing its § 504(a) collection suit in a different jurisdiction, *see* 47 U.S.C. § 504(a) (permitting suit "in any district through which the line or system of the carrier runs"). The only mechanism for *the Companies* to seek judicial review is the one they have invoked under 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1).

Even assuming the Companies could raise all legal and factual defenses to the Orders in a government-initiated collection action, it would not follow that they waive their Seventh Amendment arguments by instead pursuing those defenses directly. Congress provided the Companies a mechanism for challenging FCC forfeiture orders without requiring the Companies to play the part of a scofflaw. *See* 47 U.S.C. § 402(a); 28 U.S.C. § 2342(1). Seeking review of the FCC's erroneous rulings under those provisions cannot constitutionally deprive the Companies of their rights to a jury trial.

The FCC's position would impermissibly condition the Companies' jury-trial rights on disclaiming the statutory right to seek prompt § 402(a) review of the Orders. A government-initiated collection action under § 504(a) may be years away, if it happens at all—the government

has five years to file one. *See* 28 U.S.C. § 2462. In the interim, the FCC's public finding of liability would remain in force, carrying the potential for "reputational injury." *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 255-56 (2012). And the FCC has even said it could use the facts underlying its determination against the Companies in a later license renewal or transfer proceeding, or as a basis to enhance future penalties. *See Commission's Forfeiture Pol'y Statement & Amend. of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, 12 FCC Rcd 17087, at ¶¶ 34-35 (1997). If the government never filed a collection action, the Companies would still be stuck with unchallenged adverse orders (and their consequences)—the 60-day filing window for § 402(a) appeals will have long-since expired. 28 U.S.C. § 2344.

The § 504(a) recovery-action procedure is thus no substitute for a jury trial in an Article III court in the first instance. The Companies did not waive those rights.

### C. Separation-Of-Powers Principles And Due Process Confirm The Need For A Jury Trial

The need for a jury trial is especially pronounced in FCC enforcement actions because the FCC itself otherwise unfairly and improperly acts as rule-maker, investigator, prosecutor, judge, and jury.

That combination of functions offends separation-of-powers principles and due process, which "requires a 'neutral and detached judge'" to adjudicate claims. *Concrete Pipe & Prods. of Cal., Inc. v. Constr. Laborers Pension Tr. for S. Cal.*, 508 U.S. 602, 617 (1993). While older precedent suggests that not every union of "investigative and adjudicative functions" violates due process, *Withrow v. Larkin*, 421 U.S. 35, 58 (1975), that precedent is ripe for reconsideration in light of more recent case law, *e.g.*, *Williams v. Pennsylvania*, 579 U.S. 1, 8 (2016). And in any event, "special facts and circumstances" are present here that make "the risk of unfairness … intolerably high" even under *Withrow*. 421 U.S. at 58.

Some of the Commissioners who ultimately voted to approve the Order made statements suggesting that they had prejudged the issues. *Cinderella Career & Finishing Schs., Inc. v. FTC*, 425 F.2d 583, 590-91 (D.C. Cir. 1970). Nearly a year before the NALs issued, one Commissioner took to the *New York Times* to pressure the agency to "act swiftly and decisively to stop" what he deemed to be "illegal and dangerous pay-to-track practices." Geoffrey Starks, *Why It's So Easy for*

*a Bounty Hunter to Find You*, N.Y. Times (Apr. 2, 2019).[14] And two Commissioners issued statements alongside the NALs showing that they had made up their minds before even receiving the carriers' responses, arguing that the Companies should be punished even more severely than the NALs proposed.[15] Not surprisingly, those Commissioners voted to approve the ultimate Orders. Statements like those would not be acceptable in an Article III court, and the result should not change where an agency's combination of powers poses even *greater* risks. A jury trial is necessary to protect the Companies' constitutional rights to a neutral arbiter and vindicate separation-of-powers concerns.[16]

---

[14] https://www.nytimes.com/2019/04/02/opinion/fcc-wireless-regulation.html.

[15] *See* JA156-57 (stating that the carriers' actions were "a violation of the law," chronicling public efforts to "t[ake] on this issue on my own," and criticizing the "impose[d] fines" as "too small"); JA158-63 ("there should be no dispute" about the statutory question, the carriers committed "serious violations," and "[s]ignificant penalties are more than justified").

[16] The Communications Act also improperly delegates to the FCC policymaking authority over the mechanism for seeking a forfeiture. While the statute identifies two paths for forfeiture orders—an administrative-law-judge proceeding, 47 U.S.C. § 503(b)(3), or direct imposition of a penalty through the NAL process, *id.* § 503(b)(4)—Congress did not specify which process applies. Instead, it delegated that legislative decision to "the discretion of the Commission," without any intelligible principle. *Id.* § 503(b)(3)(A). That is unlawful: "[A] total absence of guidance" as to where an agency should bring a particular

## II. The Orders Exceed The FCC's Statutory Authority

In addition to being unconstitutional, the Orders exceed the FCC's statutory authority because the device-location information on which the Orders are based is not CPNI. Under § 222, information is CPNI only if it both (1) "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 (2) "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). Neither requirement is satisfied.

### A. The "Location" Component Of CPNI Covers Only Call-Location Information

As Commissioner Carr explained, the "location" component of CPNI "covers a particular type of data known as 'call location information'—namely, the customer's location *while making or receiving a voice call*."

---

action "is impermissible under the Constitution." *Jarkesy v. SEC*, 34 F.4th 446, 462 (5th Cir. 2022). While this Court recently took a different view of a similar question in denying an injunction pending appeal, *Meta Platforms, Inc. v. FTC*, 2024 WL 1549732, at *3 (D.C. Cir. Mar. 29, 2024) (per curiam), that non-precedential decision should not control here, especially given the express delegation to the FCC's discretion.

JA51. It does not, as the Orders contend, extend to "all location information collected by a carrier, irrespective of particular calls." JA51.

### 1. Section 222 Does Not Cover Device-Location Information Unrelated To Voice Calls

There is no dispute that the device-location information used in the LBS programs (and that forms the basis for the penalties) is not call-location information. JA12 ¶ 27. As the NALs explained, the location information used in the LBS programs was "generated from [the] registration activity" created when mobile phones "periodically register with nearby network signal towers." JA126 ¶ 12; *see* JA10 ¶ 22 (incorporating NAL discussion by reference). The FCC concedes that "[t]his type of location information … is created even when the customer does not have an active established connection, such as a voice call or data usage." JA126 ¶ 12. It can be generated from idle devices or when a user is engaged in a data-only session. JA135-36 ¶ 43.

The Orders' theory of liability thus hinges on the FCC's view that non-call-location information is CPNI. That position cannot be reconciled with the statutory text. Device-location information that is not linked to a voice call is not information relating to the "quantity, technical configuration, type, destination, location, and amount *of use* of a

*telecommunications service*." 47 U.S.C. § 222(h)(1)(A) (emphasis added). The FCC agrees that the phrase "telecommunications service" refers to the customer's "mobile voice services." JA2 ¶ 2 n.7; *supra*, at 7-9.[17] And more specifically, a "telecommunications service" is a service that offers the actual "transmission" of a voice between "points specified by the user." 47 U.S.C. § 153(50), (53). Information about the location of a *device* that is not engaged in telecommunications is not information about the location of use of a *telecommunications service*.

That conclusion is buttressed by the statutory term "use." CPNI encompasses information relating to the "destination, location, and amount *of use* of a telecommunications service." 47 U.S.C. § 222(h)(1)(A) (emphasis added). The term "use" "'impl[ies] action and implementation,'" not something "'passive,' 'passing,'" or employed in an "ancillary" way. *Dubin v. United States*, 599 U.S. 110, 118-19 (2023); *see Black's Law Dictionary* (7th ed. 1999) ("use" is "[t]he application or employment of something"). Information relating to a device's passive registration with a network tower when it is not being used for a call is

[17] The question whether a "telecommunications service" can also include an Internet access service is not implicated here. *Supra*, at 8 n.3.

not information relating to the "location … of use of a telecommunications service." 47 U.S.C. § 222(h)(1)(A). By contrast, as the FCC previously acknowledged, "[t]he location of a customer's *use* of a telecommunications service" is CPNI. *2013 CPNI Ruling* ¶ 22 (emphasis added).

Statutory context and history also confirm the Companies' reading. Section 222 twice refers to the "location" component of CPNI as "call location information." 47 U.S.C. § 222(d)(4), (f)(1). Originally, § 222 did not include any references to "location" information. In 1999, however, Congress amended § 222 to facilitate the use of wireless call-location information for emergency services, while otherwise protecting the privacy of that location information. *See* 113 Stat. 1286, 1288-89.[18] To achieve that result, Congress amended the CPNI definition to add information about the "location" at which a telecommunications service is used, 47 U.S.C. § 222(h)(1)(A), and enacted two substantive provisions

[18] The Committee Reports confirm that the amendment was understood to "provid[e] privacy protection for *the call location information* of users of wireless phones, including such information provided by an automatic crash notification system." S. Rep. No. 106-138, at 2 (1999) (emphasis added); *see* H.R. Rep. No. 105-768, at 32 (1998). An "automatic crash notification system" was a system designed to trigger a car phone to place a call to first responders in the event of a crash. *See* 145 Cong. Rec. 2886-87 (1999) (statement of Rep. Tauzin).

governing "call location information"—one requiring the customer's express consent before disclosing the information, *id.* § 222(f)(1), and the other creating an exception for emergency services, *id.* § 222(d)(4). The fact that Congress simultaneously added "location" information to the definition of CPNI while adopting rules governing "call location information" shows that CPNI location information refers specifically to call-location information.

Longstanding FCC guidance is in accord. The *2007 CPNI Order*, which adopted the regulation at issue here, 47 C.F.R. § 64.2010(a), described CPNI as including various types of call information, "such as the phone numbers called by a consumer" and "the frequency, duration, and timing of such calls." *2007 CPNI Order* ¶ 5. If, as the FCC now claims, CPNI encompasses device-location information unrelated to voice calls, one would expect the FCC to have raised that important point when adopting 47 C.F.R. § 64.2010(a). Yet the *2007 CPNI Order* never suggested that CPNI included non-call-related information.

The *2013 CPNI Ruling* further shows that device-location information unrelated to voice calls is not CPNI. It repeatedly and exclusively refers to CPNI location information as information relating

to voice calls. It states, for example, that CPNI incudes: the "telephone numbers of calls dialed and received and *the location of the device at the time of the calls*," "[t]he location of a customer's *use of a telecommunications service*," and "'the *location*, date, and time a handset experiences a network event, *such as a dialed or received telephone call [or] a dropped call*.'" *2013 CPNI Ruling* ¶¶ 22, 25 (emphases added). The FCC never suggested that CPNI includes device-location information created when a handset is idle or engaged in a data session. In fact, the *2013 CPNI Ruling* recognized that "not all of the information collected on mobile wireless devices is CPNI," and it expressly *excluded* "information that pertains to the device's *access of the carrier's data network*." *Id.* ¶ 28 & n.66 (emphasis added).

This Court, too, has linked CPNI with call information. In 2009, it described CPNI as "encompass[ing] customers' particular calling plans and special features, the pricing and terms of their contracts for those services, and details about who they call and when." *Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 997 (D.C. Cir. 2009).

In short, because the location information at issue is not "call location information," it is not CPNI. 47 U.S.C. § 222(h)(1).

### 2. The Orders' Contrary Reasoning Is Unpersuasive

In the Orders, the FCC departed from its prior guidance and concluded that CPNI includes *any* network-based device-location information, not just call-location information. JA10-12 ¶¶ 23-27. That argument is unpersuasive.

***"Of use" modifies "location."*** The Orders take the position that the phrase "of use" in § 222's definition of CPNI modifies only the word "amount," not the word "location," such that CPNI includes any information relating to "the location … of a telecommunications service." JA10-11 ¶ 24. That argument is incorrect and, in any event, cannot support the Orders.

Read naturally and sensibly, the phrase "of use" modifies each noun listed in the CPNI definition: "the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service." Linking each term to the customer's *use* of the service ensures that each term applies to "*customer* proprietary network information," 47 U.S.C. § 222(h)(1) (emphasis added), rather than network information in

the abstract. And it gives each term a discernible, voice-call-related meaning.[19]

The FCC's reading also makes hash of the statutory definition. For example, the phrase "destination … of a telecommunications service" has no readily discernable meaning, whereas the phrase "destination … *of use* of a telecommunications service" does. Similarly, one does not ordinarily speak of the "location … of a telecommunications service" that a customer subscribes to, at least when referring to protecting the *customer*'s information—that phrase calls to mind generic information about the carrier itself. Perhaps for that reason, the FCC itself previously said that CPNI "includes information about a customer's *use* of the service." *2013 CPNI Ruling* ¶ 9 (emphasis added).

In the Orders, the FCC invoked the "rule of the last antecedent" to argue that "of use" modifies only "amount." JA10 ¶ 24. But that "context

[19] While the Court need not precisely define each term—and the Companies do not purport to offer comprehensive definitions—under the Companies' "of use" reading, CPNI would encompass a wide variety of information relating to customers' use of telecommunications services, including the number and frequency of calls ("quantity"); technical details about the calls ("technical configuration"); whether the call involved a landline or mobile phone ("type"); and who was called ("destination"), from where ("location"), and for how long ("amount"). 47 U.S.C. § 222(h)(1)(A).

dependent" canon does not apply where, as here, "the modifying clause appears after an integrated list" to which the modifier equally applies. *Facebook, Inc. v. Duguid*, 592 U.S. 395, 404 (2021). In that scenario, the series-qualifier canon directs that the modifier "applies to the entire series." Scalia & Garner, *Reading Law: The Interpretation of Legal Texts* 147 (2012); *see Paroline v. United States*, 572 U.S. 434, 447 (2014).

The FCC also claimed that the *Companies'* reading produces anomalous results, asserting that the meaning of "technical configuration … of use" is "not clear." JA11 ¶ 24. That argument falls flat. The "technical configuration of use" of the subscriber's telecommunications service refers to any technical aspects of the voice service being used and would encompass, for example, information about radio frequencies, the network connection, the mobile device, call quality, or other relevant technical details. 47 U.S.C. § 153(50).

Lastly, the FCC asserted that the CPNI definition's reference to "location" information should be read to cover more than "call location information" because § 222(d)(4) and (f)(1) reference "call location information" specifically. But as explained, those provisions were added to the statute at the same time (in 1999), and thus are best read as cross-

references to each other, meaning the same thing. That Congress used a different phrase in the definitional provision ("information that relates to the … location … of use of a telecommunications service") than it did in the substantive provisions ("call location information") simply reflects the differing grammatical structures of the provisions and the fact that, unlike the definitional provision (which must cover *all* types of CPNI, including non-location information), the substantive provisions focus specifically on location-based CPNI.

Ultimately, even if "of use" did not modify "location," the phrase "location … of a telecommunications service" still is best read to refer to call-location information, rather than device-location information. That reading makes the most sense of the fact that the CPNI definition is located in Title II (which governs only voice services), the statutory and historical context, and the FCC's and industry's longstanding interpretation of CPNI. *Supra*, at 41-45. It also avoids the strange results that flow from the FCC's novel position. *Supra*, at 47. The FCC itself has equated the phrase "location … of a telecommunications service" with "[t]he location of a customer's *use* of a telecommunications service," confirming that the reading is permissible. *2013 CPNI Ruling*

¶ 22 & n.48 (emphasis added). Properly interpreted, however, the phrase "of use" modifies "location" and provides additional confirmation that the Companies' reading is correct.

***The "location … of use of a telecommunications service" refers only to call-location information.*** As a fallback, the FCC asserted in the Orders that even if "of use" modifies "location," non-call-location information would still be CPNI because the information is necessary to allow the device to send and receive calls. JA11-12 ¶ 26. That view is incorrect for multiple reasons.

The argument misconstrues the term "use" to encompass the passive, background registration of a mobile device with a cell tower to secure a signal connection. That automatic activity—which occurs any time a mobile device is powered on—is not the "use" of a mobile device. As the Supreme Court has said, mobile devices scan for cell sites "even if the owner is *not using* one of the phone's features." *Carpenter v. United States*, 585 U.S. 296, 300-01 (2018) (emphasis added). Further, network-based device-location information is not inherently associated with voice calls (*i.e.*, "telecommunications services"). As explained below, the same device-location information is necessary to engage in a data session,

which the FCC agrees is "a non-telecommunications service." JA13-14 ¶ 31; *infra*, at 52-53. That information therefore does not relate to the "use *of a telecommunications service*." 47 U.S.C. § 222(h)(1)(A) (emphasis added).

For all these reasons, CPNI encompasses only call-location information, not other types of location information.

### B. The Location Information Was Not Made Available "Solely By Virtue Of The Carrier-Customer Relationship"

The FCC's expansive view of CPNI fails for a second, independent reason: The location information at issue here 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)(A).

The phrase "the carrier" in § 222(h)(1) refers back to the phrase "telecommunications carrier," which in turn is a "provider of telecommunications services." 47 U.S.C. § 153(51); *see also id.* § 153(11) (defining "carrier"). As explained, a telecommunications service is a Title II telephone voice service, not a Title I "information service" such as Internet-access service. *Supra*, at 7-9 & n.3. Thus, location information is not CPNI under the statute unless the customer made it available to

the Companies "solely by virtue of" the Companies' provision of voice services. 47 U.S.C. § 222(h)(1)(A).

The ordinary meaning of "solely" is "to the exclusion of all else." *Merriam-Webster's Collegiate Dictionary* 1118 (10th ed. 1997). Yet the FCC does not contend that the device-location information at issue was provided *only* because of a Title II telecommunications service, "to the exclusion of all else"—and the record forecloses any such claim. Both Companies collected device-location information by recording the network-signal stations to which a mobile device registered when it was powered on; that information supported *both* data and voice services, and was not exclusively associated with voice. JA165; JA215; JA407-08; JA427; *see* JA10 ¶ 23.

For any customer with both voice and data services, then, location information was not generated "solely" because of the voice subscription—the only service for which the Companies are Title II "telecommunications carrier[s]." *See Cellco P'ship*, 700 F.3d at 538; *supra*, at 7-9. Indeed, data-only customers who used the LBS programs—*e.g.*, for many tablets or wearables, JA190-94—lacked *any* Title II "carrier-customer" relationship. 47 U.S.C. § 222(h)(1)(A). Thus, as

Commissioner Carr correctly explained, "the location information was unrelated to a [telecommunications] service. The customer did not need to make a call to convey his or her location. In fact, the carrier could have obtained the customer's location even if the customer had a data-only plan for tablets." JA50. The FCC cannot maintain that device-location information "depend[s] exclusively on the carrier-customer relationship" (JA13 ¶ 29) when it undeniably supports customers who receive *both* data and voice services and customers who subscribe *only* to data services.

* * *

Because the Orders purport to regulate location information that is not CPNI under § 222, they exceed the FCC's authority and should be set aside as unlawful.

## III. The Orders Violate Principles Of Fair Notice

Even if the definition of CPNI could be stretched to cover the device-location information used in the LBS programs, principles of fair notice preclude the agency from basing millions of dollars in liability on a novel view of the statute at odds with its own prior views.

Due process requires that "laws which regulate persons or entities … give fair notice of conduct that is forbidden" so that businesses know "what is required of them." *Fox Television*, 567 U.S. at 253. A regulated party must therefore "be able to identify, with 'ascertainable certainty,' the standards with which the agency expects parties to conform." *Gen. Elec.*, 53 F.3d at 1329. If the FCC failed to provide "fair warning of its interpretation," then the Orders violate due process. *Id.* at 1333.

The FCC failed to provide fair warning here. The Companies' view—that the "location" component of CPNI encompasses only call-location information—was not just reasonable on its face, but also affirmatively supported by the FCC's own guidance. Before it moved to impose these staggering penalties, the FCC's only relevant statements tied CPNI to call-related information. As explained, the *2007 CPNI Order* consistently described CPNI in terms of call information. *E.g.*, *2007 CPNI Order* ¶¶ 5, 13-14. And the *2013 CPNI Ruling* specifically described CPNI as including *call*-location information and even said that information related to a data session is not CPNI. *See supra*, at 44-45.

The FCC tries to wave away the 2013 ruling, pointing to a footnote to argue that it did not exhaustively define CPNI. JA16 ¶ 37 & n.128

(citing *2013 CPNI Ruling* ¶ 24 n.54) (declining to "set out a comprehensive list"). That misses the point. The FCC clearly signaled that it read § 222 to cover only call-location information, stating, *e.g.*, that "where the customer was located when he or she made a call" is "sensitive information." *2013 CPNI Ruling* ¶ 1. Without further guidance, the Companies could not have predicted with "ascertainable certainty" that the FCC would subsequently take the view that *all* location information is CPNI. *Gen. Elec.*, 53 F.3d at 1329.

Notably, the wireless industry petitioned the FCC to adopt privacy rules implementing Congress's 1999 location-related amendments "by establishing a clear framework for industry to design the services and consumers to predict how their location information will be handled." *Request by CTIA to Commence Rulemaking to Establish Fair Location Info. Pracs.*, 17 FCC Rcd 14832, at ¶ 6 (2002).[20] The FCC denied that request, however, over a dissent by Commissioner Copps expressing concern that "[e]ven the definition of 'location information' is debated by commenters." *Id.* at 14839. He presciently warned that "without Commission action, consumers and carriers will not know what is

[20] https://docs.fcc.gov/public/attachments/FCC-02-208A1.pdf.

contained in this opaque term until the question is subject to court action that follows a potential privacy violation." *Id.*

The fair-notice problems are especially pronounced here because the FCC knew of the industry's interpretation that CPNI refers only to voice services. In 2016, for example, comments filed by carriers focused on the use of voice services.[21]

The FCC cannot now "impose potentially massive liability on [the Companies] for conduct that occurred well before" the FCC announced its new interpretation of CPNI. *Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 155-56 (2012). Particularly "where, as here, an agency's announcement of its interpretation is preceded by a very lengthy period of conspicuous inaction" relevant to an "entire industry," the "potential for unfair surprise is acute." *Id.* at 158. Because the Companies were unable to determine with "ascertainable certainty" the standards with which the FCC expected them to conform, *Gen. Elec.*, 53 F.3d at 1329, the

[21] *E.g.*, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Comments of T-Mobile USA, Inc. at 24, WC Dkt. No. 16-106 (May 27, 2016), https://www.fcc.gov/ecfs/document/60001974410/1; *id.*, Comments of the Competitive Carriers Ass'n at 13 (May 27, 2016), https://www.fcc.gov/ecfs/document/60001973474/1.

Orders violate due process and should be set aside, *see* JA51 (Carr dissent).

## IV. The Orders Are Arbitrary And Capricious Because The Companies Employed Reasonable Protective Measures

The Orders are not just legally improper but also factually unsupportable. On any fair reading of the record, the Companies took "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a). The FCC's hindsight-based arguments to the contrary are arbitrary and capricious.

### A. The Companies' Safeguards Were Reasonable

Section 64.2010(a) does not require perfection, only "reasonable measures." 47 C.F.R. § 64.2010(a). The Companies easily cleared that bar.

At the time of the *New York Times* article reporting on Securus, both Companies had robust measures in place to protect customer location information. The Companies structured their LBS programs to limit direct access to customers' location information to only two aggregators. JA214-15; JA424. That "common sense" measure reflects the fact that "the risk of unauthorized disclosure of customer information

increases with the number of entities possessing it." *Nat'l Cable*, 555 F.3d at 1001-02.

The Companies also imposed strict conditions on accessing location information. The Companies required both aggregators and LBS providers to comply with industry-standard CTIA Guidelines—including clear notice, express consent, and the right to revoke consent. JA246-47; JA558-61. The aggregators also had to maintain clear records of customer consent. JA247; JA561-62. Both Companies had the right to terminate access immediately. JA248, 250; JA554.

The Companies also had established processes for vetting LBS providers. T-Mobile itself preapproved each LBS campaign after reviewing detailed information about the LBS provider, including clear depictions of the process by which it secured customers' consent. JA246; JA215-16. T-Mobile also assigned each campaign a unique identifier for tracking purposes. JA215-16. And T-Mobile tested its safeguards by conducting risk assessments in 2016 and 2018 through outside consultants, both of which determined that the aggregators were properly obtaining pre-disclosure customer consent. JA226-27; *see also supra*, at 16 (explaining that T-Mobile's established processes shut off

access for LocateUrCell). Sprint likewise implemented a certification process, subject to Sprint's own auditing, through which aggregators tested sub-aggregators' and LBS providers' applications to ensure they met Sprint's notice, privacy, and data security requirements. JA290-91 ¶ 10; JA409; *see* JA544, 551.

Both Companies also responded reasonably and prudently to the May 10, 2018, *New York Times* article about Securus's misuse of access to device-location data. The day after the article, T-Mobile terminated Securus's access to location information and directed LocationSmart to do the same. JA218. T-Mobile also began an investigation, completed review of its 2018 risk assessment, and considered whether it could bring the LBS program in-house. JA91. By July 2018—within roughly two months—T-Mobile had advised LocationSmart and Zumigo that it would terminate the entire LBS program on December 9, 2018, JA233; JA234, which would give time for customers to transition.

T-Mobile extended the termination deadline to March 2019 to avoid added pressure over the holidays. JA231-32. After it learned of the issue with Microbilt, however, *supra*, at 19-20, T-Mobile immediately terminated that LBS provider's access and expedited its shutdown of the

broader LBS program, phasing out many services by January 14 and terminating the final, most important campaigns by February 8. JA169, 175-76; JA93; JA205-07 (schedule of shutdown).

Sprint's response to the May 10 article was also reasonable. It immediately investigated the incident, suspended Securus's access by May 17, and then suspended *all* location sharing with LocationSmart (and LocationSmart's LBS providers) on May 25. JA293 ¶ 15; JA429. On June 20, Sprint terminated the LocationSmart contract effective immediately and triggered a 90-day notice to terminate Zumigo's contract. JA293 ¶ 15; JA429. To mitigate the negative effects of the shutdown on customers, however, Sprint allowed AAA and a state-lottery provider to sign new short-term contracts through LocationSmart, requiring the additional safeguard of an independent third-party audit. JA429-30; JA480. In late October 2018, Sprint also reinstated Zumigo's contract for a short time for certain LBS providers. JA430; JA435-36. But when Sprint learned of the Microbilt incident in January 2019, Sprint terminated its contract with Zumigo on January 9. JA406-07, 413. Sprint shut down access for the AAA and state-lottery services by May 31, 2019. JA407.

Those actions reflected reasonable efforts to protect location information, balancing customer privacy with a graduated shutdown to avoid cutting off customer access to important services.

### B. The FCC's Hindsight-Based Reasoning Fails

The FCC reached the contrary conclusion by applying hindsight-based reasoning rather than a reasonableness standard.

The FCC was aware of the Securus incident months before the Companies and took no action, and it identifies no T-Mobile or Sprint customer whose location information was disclosed without consent during the relevant time period. *See* JA115; JA338 n.3; JA148 ¶ 85. Despite all that, the FCC determined in the Orders that the Companies acted unreasonably by not terminating their entire LBS programs immediately following a single newspaper article. *E.g.*, JA33 ¶ 74.

The Supreme Court has warned against this kind of error: deeming past actions "unreasonable in the harsh light of hindsight." *Bell v. Cone*, 535 U.S. 685, 702 (2002). As explained, both Companies responded to reporting on Securus quickly and reasonably, with measures tailored to the problem reported. It bears emphasizing that Securus was authorized to provide a prison-geofencing service, and that its unauthorized service

was limited to the specialized context of allowing law-enforcement officers to obtain the location information of suspects based on legal process. That use was unauthorized, to be sure, but it did not suggest a widespread problem. The fact that a rogue sheriff exploited Securus's failure to verify the validity of legal process shows only that criminal conduct occurred and that Securus's access needed to be promptly shut off—which, of course, is what happened.

The FCC offers no reason why reporting on Securus's and Sheriff Hutcheson's misdeeds should have led the Companies to cut off LBS providers like AAA, Life Alert, banks, state lotteries, or others as to which there was no reason to suspect wrongdoing. The reasonableness of the Companies' response is confirmed by the fact that none of the other carriers acted as the FCC suggests they should have. And of course, the FCC itself took no action on the same information when the FCC learned about it months before the *New York Times* report.

The FCC also concluded that the Companies' safeguards did not do enough to distinguish between permissible and impermissible (fraudulent) uses of approved LBS campaigns. JA21 ¶ 48. But, of course, T-Mobile's process *did* ferret out LocateUrCell, *supra*, at 16, and the

Companies *did* conduct certifications and risk assessments, *supra*, at 15-16. Further, after the Securus incident, the Companies decided to safely phase out their LBS programs. *Supra*, at 19-21. The FCC's insistence on more drastic measures more quickly is inconsistent with the reasonableness standard.

The Companies' efforts are especially reasonable given the FCC's failure to provide any guidance on the meaning of the "reasonable measures" standard, even in the face of an industry request for guidance. *Supra*, at 55-56. The Companies were thus left to guess at what "reasonable measures" might mean. And no one could have anticipated (or in fact did) what the FCC eventually required: shutting down the entire program immediately following a single *news report*. JA33 ¶ 74; JA140 ¶ 58. That requirement is irreconcilable with the *2007 CPNI Order*'s description of the "reasonableness" standard—that it would "allow carriers to implement whatever security measures are warranted in light of their technological choices" and "enable market forces to improve carriers' security measures *over time*." *2007 CPNI Order* ¶ 65 (emphasis added). Section 64.2010(a) was "'unclear,'" the Companies' interpretations were "'reasonable,'" and the FCC provided no guidance,

let alone a "'definitive reading.'" *Trinity Broad. of Fla., Inc. v. FCC*, 211 F.3d 618, 632 (D.C. Cir. 2000). The Companies therefore were not on notice and "'may not be punished.'" *Id.*

## V. The FCC's Penalties Are Unlawful And Arbitrary

The FCC compounded all those mistakes by imposing penalties that exceed the statutory maximum and are arbitrary and capricious.

### A. The Penalties Exceed The Statutory Maximum

Congress capped civil penalties by providing that "the amount assessed for any continuing violation shall not exceed a total of $1,000,000 for any single act or failure to act." 47 U.S.C. § 503(b)(2)(B). Adjusted for inflation, the maximum penalty in 2020 (when the NALs issued) was $2,048,915. JA34 ¶ 77. The FCC flagrantly exceeded that cap by imposing penalties of $80,080,000 on T-Mobile and $12,240,000 on Sprint. JA1-2 ¶ 1; JA286-87 ¶ 1.

Under the FCC's theory of the case, each Company purportedly committed a single, continuing failure to act by purportedly failing to terminate its LBS program or otherwise properly secure the confidentiality of location information. *See* JA53 (Simington dissent). The FCC's own framing of the purported violations confirms as much.

According to the Orders, each Company supposedly violated § 222 and the FCC's rules because it "placed its customers' location information at *continuing risk* of unauthorized access *through its failure to terminate its program or impose reasonable safeguards* to protect its customers' location information." JA33 ¶ 73 (emphasis added); JA311 ¶ 61. Indeed, according to the FCC, each Company's LBS program "suffered from *the same fundamental vulnerabilities*" across all aggregators and LBS providers. JA35 ¶ 79 (emphasis added); JA313 ¶ 66. The Orders could hardly be clearer that each Company committed, at most, a single, continuing failure to act that is subject to the statutory maximum. Each penalty should have been capped at $2,048,915.

The FCC attempted to circumvent that mandatory limit by claiming that "each unique relationship between [the Companies] and an LBS provider or aggregator represented a distinct failure to reasonably protect customer CPNI," and thus that T-Mobile committed 73 continuing violations and Sprint committed 11. JA35 ¶ 79; JA312-13 ¶¶ 64-66. But that results-oriented justification is entirely made up and untethered to the statutory text, as the FCC's reasoning confirms. The FCC claimed that it could have picked different numbers; for example, it

"could well have chosen to look to the total number of … subscribers when determining the number of violations," and that, "taking into account the tens of millions of consumers" at issue, the penalties would have been "significantly higher." JA35 ¶ 80.[22] It also cited another in-house forfeiture order in which it "elected to ground its forfeiture calculation in the number of unprotected documents," which exceeded 300,000. JA35 ¶ 79 (citing *TerraCom, Inc. & YourTel Am., Inc.*, 29 FCC Rcd 13325, at ¶ 50 (2014)).[23] The FCC therefore lauded its approach here as "not only reasonable," but "eminently *conservative*." JA35 ¶ 80.

To explain the FCC's position is to refute it. Section 503(b)(2) speaks in terms of an "act," and as Commissioner Simington explained, it is "simply not plausible" to interpret that language as authorizing the FCC to "arrive at forfeitures of any size simply by disaggregating an 'act' into its individual constituent parts, counting the members of whatever class of objects may be related to the alleged violation to arrive at

[22] The FCC thus claimed authority to impose *hundreds of trillions* of dollars in penalties on T-Mobile and Sprint, who reported 79.7 million and 54.4 million subscribers, respectively. *See* T-Mobile, 2018 Form 10-K, https://tinyurl.com/ybmh43bd; Sprint, 2018 Form 10-K, https://tinyurl.com/ycxdvd4p.

[23] https://docs.fcc.gov/public/attachments/FCC-14-173A1_Rcd.pdf.

whatever forfeiture amount suits a preordained outcome." JA53. That is not reasoned statutory interpretation, but "the whole-cloth creation of a novel legal ontology." JA53

For these reasons, the FCC's penalties should be set aside as unlawful and arbitrary and capricious.

### B. The Penalties Are Arbitrarily Disproportionate

The FCC's penalties are also arbitrary and capricious because they are disproportionate—*i.e.*, they are "out of line with the agency's decisions in other cases." *Collins v. SEC*, 736 F.3d 521, 526 (D.C. Cir. 2013).

The FCC imposed a combined total of more than $92 million in penalties on T-Mobile and Sprint, with more than $80 million attributable to T-Mobile alone. At the time, the penalty proposed for T-Mobile in the NAL would have been the third largest in the FCC's history. JA122.

In the rare instances when the FCC has issued penalties of this size, it has been for intentional efforts to defraud or to harm or mislead consumers. For instance, in *Best Insurance Contracts, Inc.*, the FCC imposed an $82.1 million forfeiture, finding the defendants had

orchestrated "a massive spoofing scheme" that "misled" "millions of people," with the "intent to financially profit … from unlawful conduct." 2018 WL 4678487, at ¶¶ 17, 22, 28 (FCC Sept. 26, 2018) (capitalization altered).[24] In *Sandwich Isles Communications, Inc.*, the FCC imposed a $49 million forfeiture based on the "extraordinary gravity" of the actors' "willful and fraudulent" scheme to obtain $27 million in FCC funds to which they were "not entitled." 35 FCC Rcd 10831, at ¶¶ 2-3 (2020).[25] And in *American Broadband & Telecom Co.*, the FCC proposed a $63.5 million forfeiture for "apparent mass fraud." 33 FCC Rcd 10308, at ¶ 175 (2018).[26]

Here, the Companies did not commit fraud, and even assuming they misunderstood their statutory or regulatory duties, there is no evidence that they violated the law willfully. *See supra*, at 11-21. Further, the FCC points to no instance of a customer's location information being disclosed without their consent during the relevant time period.

---

[24] https://docs.fcc.gov/public/attachments/FCC-18-134A1_Rcd.pdf.

[25] https://docs.fcc.gov/public/attachments/FCC-20-131A1_Rcd.pdf.

[26] https://docs.fcc.gov/public/attachments/FCC-18-144A1_Rcd.pdf.

The FCC dismissed those distinctions with the *ipse dixit* that even though the Companies "may not have engaged in fraud or otherwise sought to mislead or harm consumers," their conduct was still "egregious" and "worthy of a significant monetary penalty." JA36 ¶ 84. But the Orders never explain why "*potential* exposure" to harm, JA36 ¶ 84 (emphasis added), warrants penalties equal to or higher than those cases involving fraud and serious *actual* harms.

In short, the FCC's scant reasons offer no "satisfactory explanation for its action," and the penalty amounts are therefore arbitrary and capricious. *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

## CONCLUSION

The Court should grant the petition; hold unlawful, vacate, enjoin, and set aside the FCC's Orders; and order the FCC to refund the penalties the Companies paid pursuant to the Orders.

Dated: November 25, 2024

Respectfully submitted,

/s/ *Helgi C. Walker*

Helgi C. Walker
Russell B. Balikian
Zachary E. Tyree
Nathaniel J. Tisa
GIBSON, DUNN & CRUTCHER LLP
1700 M Street, N.W.
Washington, D.C. 20036-4504
hwalker@gibsondunn.com
rbalikian@gibsondunn.com
(202) 955-8500

*Counsel for Petitioners*

## CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because this brief contains 12,985 words, as determined by the word-count function of Microsoft Word, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the typestyle requirements of Federal Rule of Appellate Procedure 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2019 in 14-point New Century Schoolbook font.

Dated: November 25, 2024

/s/ *Helgi C. Walker*

Helgi C. Walker
GIBSON, DUNN & CRUTCHER LLP
1700 M Street, N.W.
Washington, D.C. 20036-4504

*Counsel for Petitioners*

## CERTIFICATE OF SERVICE

I hereby certify that on November 25, 2024, I electronically filed the foregoing document with the Clerk of Court for the United States Court of Appeals for the D.C. Circuit and accomplished service by using the appellate CM/ECF system.

Dated: November 25, 2024

/s/ *Helgi C. Walker*
Helgi C. Walker