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;
UNITED STATES OF AMERICA,

Respondents.

T-MOBILE USA, INC.

Petitioner,

v.

FEDERAL COMMUNICATIONS COMMISSION;
UNITED STATES OF AMERICA,

Respondents.

On Petition 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

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER, THE CENTER FOR DEMOCRACY & TECHNOLOGY, THE ELECTRONIC FRONTIER FOUNDATION, PRIVACY RIGHTS CLEARINGHOUSE, AND PUBLIC KNOWLEDGE AS *AMICI CURIAE* IN SUPPORT OF THE FCC'S FORFEITURE ORDERS

[Counsel listed inside front cover]

January 17, 2025

Alan Butler
Christopher Frascella
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

Aaron Mackey
Adam Schwartz
Mario Trujillo
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Samir Jain
Eric Null
CENTER FOR DEMOCRACY &
TECHNOLOGY
1401 K St NW, Suite 200
Washington, DC 20005
(202) 637-9800

Attorneys for Amici Curiae

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), *amici curiae* certify that:

A. Parties, Intervenors, and Amici

Except for the following, all parties, intervenors, and *amici* appearing in this Court are listed in the Brief for the Respondents: the Center for Democracy & Technology, the Electronic Frontier Foundation, Privacy Rights Clearinghouse, and Public Knowledge.

B. Ruling Under Review

References to the rulings at issue appear in the Brief for the Respondent.

C. Related Cases

This case has not previously been before this Court or any other court. The following cases deal with similar FCC forfeiture orders, but do not involve the same Petitioners as this case: *AT&T, Inc. v. FCC*, No. 24-60223 (5th Cir.) and *Verizon Communications Inc. v. FCC*, No. 24-1733 (2d Cir.).

/s/ Alan Butler
ALAN BUTLER

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amici curiae* the Electronic Privacy Information Center, the Electronic Frontier Foundation, the Center for Democracy and Technology, Privacy Rights Clearinghouse, and Public Knowledge state that they have no parent corporations and that no publicly held corporation owns 10% or more of either of their stock.

/s/ Alan Butler
ALAN BUTLER

CIRCUIT RULE 29(d) STATEMENT REGARDING SEPARATE BRIEFING, CONSENT TO FILE, AUTHORSHIP, AND MONETARY CONTRIBUTIONS

All parties have consented to the filing of this brief. *Amici curiae* the Electronic Privacy Information Center, the Center for Democracy & Technology, the Electronic Frontier Foundation, Privacy Rights Clearinghouse, and Public Knowledge certify that a separate amicus brief is necessary. This brief provides the views of multiple organizations that regularly advocate for the privacy and consumer protection interests of phone subscribers, such as those whose location data was exposed in this case.

No party's counsel authored this brief in whole or in part, and no party or party's counsel contributed money intended to fund the preparation or submission of this brief. No person—other than the *amici* or their counsel—contributed money intended to fund the preparation or submission of this brief. *See* Fed. R. App. P. 29(a)(4)(E).

/s/ Alan Butler
ALAN BUTLER

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative Material

Other Authorities

GLOSSARY

1998 Order	*Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (Rel. Feb. 26, 1998)
1999 Act	Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286
1999 Order	*Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409 (Rel. Sept. 3, 1999)
2007 Order	*Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (Rel. Apr. 2, 2007)
Comm'r Starks Stm't	Statement of Commissioner Geoffrey Starks, Approving in Part and Dissenting in Part, *In Re: T-Mobile USA, Inc.*, File No.: EB-TCD-18-00027702, FCC 20-27 (Rel. Feb. 28, 2020)
Communications Act	Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, codified at 47 U.S.C. §§ 151 *et seq*. amending the Communications Act of 1934
CPNI	Customer Proprietary Network Information

CSLI	Cell Site Location Information
CTIA	CTIA – The Wireless Association®
"FCC" or "Commission"	Federal Communications Commission
FOs	The Forfeiture Orders (FOs) issued in *In re Sprint Corp.*, File No. EB-TCD-18-00027700, FCC 24-42 (Rel. Apr. 29, 2024), *In re T-Mobile USA, Inc.*, File No. EB-TCD-18-00027702, FCC 24-43 (Rel. Apr. 29, 2024)
GPS	Global Positioning System
LGBTQ+	Lesbian, Gay, Bisexual, Transgender, Queer, Questioning, Intersex, Asexual, Two-Spirit, and others
SIM	Subscriber Identity Module
T-Mobile	T-Mobile USA, Inc. and Sprint Corp.

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center ("EPIC") is a non-profit public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely participates as amicus curiae before federal courts in cases concerning the privacy and security of consumer data.[1]

The Electronic Frontier Foundation ("EFF") is a San Francisco-based, member-supported, nonprofit civil liberties organization that has worked for more than 30 years to protect free speech, privacy, security, and innovation in the digital world. With more than 30,000 members, EFF represents the interests of technology users in court cases and policy debates regarding the application of law to the internet and other technologies.

The Center for Democracy and Technology ("CDT") is a non-profit advocacy organization established in 1994 working to promote democratic values online and in new, existing, and emerging technologies.

Privacy Rights Clearinghouse ("PRC") is a nonprofit organization based in San Diego, California, established in 1992 to advance privacy for all by empowering individuals and advocating for positive change.

[1] EPIC Fall Law Clerk Matt Contursi contributed to research for this brief; EPIC Spring Law Clerk Madeline Rosenstein contributed to editing.

Public Knowledge ("PK") is non-profit consumer rights organization that advocates for technology policy that serves the public interest. PK advocates before Congress, the courts, the FCC, and other agencies to support consumer rights, including the right of consumers to have their confidential personal information protected.

INTRODUCTION AND SUMMARY

The Court should affirm the Forfeiture Orders in this case because Congress entrusted the Federal Communications Commission ("FCC" or "Commission"), through the Telecommunications Act of 1996 ("Communications Act") as codified under 47 U.S.C. § 222, with the responsibility of holding the nation's largest telecommunications providers accountable when those carriers violate the privacy of their subscribers. Congress intended for Section 222 to ensure that telecommunications providers would protect personal data collected from their customers, and intentionally included broad definitions and gave the Commission clear authority to interpret them as technologies evolved. Decades later, it has become clear that one of the most sensitive categories of data that telecommunications providers collect about their customers is mobile location data. The unique sensitivity of this data has been recognized by the Supreme Court in its constitutional privacy rulings. A holding here that the majority of subscribers' mobile location data collected by carriers is not protected under the subscriber privacy provisions in Section 222 would go against the purpose of the statute. Furthermore, the FCC is the best-positioned regulator to enforce privacy violations committed by carriers against their subscribers.

In 2020, the FCC charged then-four[2] of the largest mobile voice and data services providers with violating their privacy obligations under Section 222 of the Communications Act for inappropriately disclosing and for failing to safeguard the sensitive location information of their subscribers. The Supreme Court has emphasized that this data "provides an intimate window into a person's life, revealing not only [their] particular movements, but through them [their] familial, political, processional, religious, and sexual associations." *Carpenter v. United States*, 585 U.S. 296, 311 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). The vast majority of American consumers use mobile devices, and nearly three-quarters keep them nearby or on their person wherever they go, *Carpenter*, 585 U.S. at 311 (quoting *Riley v. California*, 573 U.S. 373, 395 (2014)); those subscribers deserve the privacy protections that the law promises, which can only be secured through broad coverage of the sensitive data about them and robust enforcement.

The Commission has issued Forfeiture Orders ("FOs") to hold AT&T, T-Mobile/Sprint ("T-Mobile"), and Verizon accountable for giving third party data brokers access to subscribers' sensitive location data, in violation of the

[2] Sprint and T-Mobile merged in 2020. *See, e.g.*, Eli Blumenthal, *T-Mobile closes Sprint merger after two-year battle*, CNET (Apr. 1, 2020), https://www.cnet.com/tech/mobile/t-mobile-closes-sprint-merger-after-two-year-battle/.

Communications Act and the FCC's Customer Privacy Network Information ("CPNI") regulations. T-Mobile, and the other companies through separate actions, are now attempting to invalidate those FOs by arguing that subscribers have no privacy rights with respect to their mobile location data under the Communications Act, or that companies transferring this sensitive data to third parties without subscriber consent did not violate the FCC's regulations.

The Court should reject T-Mobile's arguments and hold that the text and purpose of Section 222 clearly authorize the FCC orders under review. If the carriers were to prevail in setting aside the FOs, they will have successfully evaded virtually all means of legal accountability for violating their customers' privacy, including data sold to bounty hunters. Allowing the carriers to avoid the FCC's authority will mean that there is essentially no backstop to enforcing the privacy rights Congress guaranteed consumers under the Communications Act. The Court should not allow the carriers to evade liability for these significant privacy harms.

ARGUMENT

I. Both the text and purpose of Section 222 support the Commission's conclusion that mobile location data is protected as CPNI.

Congress tasked the FCC with enforcing rules that require telecommunications carriers to safeguard their customers' data. The Court should affirm the FCC's interpretation that CPNI includes all customer location data collected by a carrier, and not just data collected during an active voice service

call. The statute makes clear that CPNI includes all "information that relates to the…location…of a telecommunications service." 47 U.S.C. § 222(h)(1)(A). This broad definition serves an important purpose of ensuring that consumers do not lose control of their data when it is collected by their carrier. The narrow interpretation of the statutory CPNI protections proposed by T-Mobile in this case would undercut this purpose by exposing extremely sensitive location data to misuse and abuse.

Under T-Mobile's interpretation of Section 222, carriers would have no obligation under the statute to protect mobile location data unless it was collected during an active call. This Court should affirm the FCC's FOs and find that all customer cell site location information ("CSLI") collected by carriers fits within the CPNI definition for at least three reasons: (1) the statute's explicit reference to "location" in the CPNI definition cannot be reasonably read as "location of an active phone call," (2) Congress intended from the outset that Section 222 would confer a general duty on carriers to protect subscriber data, and a narrower interpretation of CPNI would be inconsistent with that purpose, and (3) the FCC has put carriers on notice that permitting this type of subscriber data to be sold to data brokers without consumer consent would violate Section 222 as well as the Commission's regulations.

The core purpose of Section 222 is to ensure that carriers are properly limiting the collection, use, and disclosure of the personal data they collect from their customers. The title for the section is aptly broad: "Privacy of customer information." And the general duties imposed by the law are similarly scoped to be all inclusive within the context of the carrier-customer relationship: "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of . . . customers." 47 U.S.C. § 222(a).

The amendments that Congress made in 1999, *see* Wireless Communications and Public Safety Act of 1999 ("1999 Act"), Pub. L. 106-81, in response to the increased rollout of commercial mobile (wireless) phone services, also support the FCC's broad interpretation. In the 1999 Act, Congress added "location" to the list of example data categories within the CPNI definition, 47 U.S.C. § 222 (h)(1).[3] The express purpose of this amendment was to "encourag[e] the provision and use of wireless services by providing protection to users' location information by specifying the conditions under which such information may be disclosed to third parties." H.R. Rep. No. 106-25 at 5 (1999). The narrower term, "call location" was added to other specific provisions within the statute including the set of transfer exceptions in Section 222(d)(4), but Congress used the

[3] Originally Section 222(h)(1) was labeled as Section 222(f)(1). *See* Communications Act, PL 104-104 § 222 (Feb. 8, 1996). Section 222(f)(1) was re-assigned to Section 222(h)(1) and "location" was added by the 1999 Act.

broader term in the CPNI definition. The narrower reference to "call location" in the exception and other subparts is consistent with the specific purpose of those provisions to ensure that customers making calls to a "public safety answering point" like 911 can be located. But the addition of "location" to the CPNI definition in Section 222(h)(1) served the broader purpose of protecting the privacy of wireless subscribers generally. The argument put forth by T-Mobile would require the Court to read the qualifier "call" into Congress's term "location" in Section 222(h)(1), but that would be inconsistent with both the intent of the 1999 amendment and with the decision by Congress to leave that term out of the definition.

Indeed, the only argument that T-Mobile and its amicus CTIA offer against the clearly broad inclusion of location information in the definition of CPNI is a cramped interpretation of the phrase "use of a telecommunications service" in Section 222(h)(1). That argument misses the key point of the FCC's interpretation, which is that the telecommunications service provided by mobile carriers is not limited to active calls. The ability to receive a call or text message wherever you are located is a core part of cell phone service—and the "non-call-location information" (as T-Mobile styles it) collected in the course of providing that service therefore meets the definition of CPNI. As the Supreme Court has

observed, cell phones produce location data several times a minute, "even if the owner is not using one of the phone's features." *Carpenter* 585 U.S. at 300–01.

The legislative histories of both acts of Congress also support a broad interpretation of Section 222 grounded in consumer protection. Although the term "location" was not explicitly added to the CPNI definition until 1999, the 1995 Senate Report for the 1996 Communications Act noted that "[t]he bill will not have any adverse impact on the personal privacy of individuals affected and will give greater control over such information to the consumer." S. Rep. No. 104-23 at 16 (1995).[4] Thus, even before Congress explicitly named location data as CPNI, it authorized the FCC to hold carriers accountable for protecting subscriber data under the general duties imposed by Section 222(a). When Congress updated Section 222 in the 1999 Act, they understood that location data fell within CPNI. The original co-sponsor in the House, Rep. Billy Tauzin, stated unambiguously that:

> If a carrier seeks to use location information for marketing purposes, it must obtain the customer's prior express authorization. In short, the location of someone's travels is not going to be commercialized for purposes without their permission.

[4] https://www.congress.gov/congressional-report/104th-congress/senate-report/23.

145 Cong. Rec. 2887 (1999).[5] Congress, in making location data available for emergency purposes, rightly feared how phone subscriber location data might be misused, and explicitly amended Section 222 to require its protection rather than leaving it to the existing general carrier obligations under 222(a).

The FCC's regulatory and enforcement actions in the thirty years since Congress enacted Section 222 also reflect that the purpose and scope of the statute is broad and intended to protect consumers. In its 2007 Order, the FCC identified documented examples of misuse of subscriber information that resulted in harm, citing to a record containing Congressional testimony and reports and news articles. *See Implementation of the Telecommunications Act of 1996*, Report and Order, 22 FCC Rcd 6927 at n. 31 (2007) ("2007 Order"). Because the collection of sensitive personal data, including mobile location information, is necessary to provide these telecommunications services, the carriers must act as a quasi-fiduciary with respect to their customers' data. The fundamental purpose of Section 222 is to impose those obligations on carriers in order to protect consumers. *Implementation of the Telecommunications Act of 1996,* Order on Reconsideration, 14 FCC Rcd 14409, ¶ 4 (1999) ("1999 Order") (citing 1998 Order). As the FCC has noted, the enactment of Section 222 "reflects Congress'

[5] https://www.congress.gov/congressional-record/volume-145/issue-29/house-section/article/H728-3.

view that as competition increases, it brings with it the potential that customer privacy interests will not be adequately protected by the marketplace." *Id.*

Petitioners and their amicus contort the language of Section 222 in an effort to evade responsibility for protecting the sensitive data of T-Mobile customers. They invite this Court to imagine that the offering of telecommunication services is only a point of sale service, and beyond that a one-time retail event. *See* Amicus Br. of CTIA at 13. They also attempt to distract the court from Section 222's plain text, which explicitly contemplates CPNI generated by automated notification systems, rendering incoherent any claim that a subscriber needs to actively "use" or "initiate" a transmission before Section 222's data protection obligations apply. *See id.* at 14. In the same 1999 Act that explicitly added "location" to Section 222's list of CPNI, Congress repeatedly discussed the need for privacy in automated crash notification systems—notwithstanding that these automated systems are not subscriber-initiated phone calls. The absurdity of these arguments are further underscored by the Supreme Court in *Carpenter*:

> [c]ell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site," and "tap into" the vast cell-site network "several times a minute whenever their signal is on, *even if the owner is not using one of the phone's features*.

585 U.S. at 300–01 (emphasis added).

Congress tasked the FCC with holding each carrier accountable for protecting the data of its subscribers through Section 222; here, subscriber data was

exposed in violation of the statute and ultimately and predictably that data was abused. Against this backdrop, it is implausible to argue that Congress did not intend for the FCC to regulate precisely this type of misconduct by telecom companies.

II. Excluding mobile location data from Section 222 would undermine the purpose of the statute.

A. Location information and other data generated by mobile phones is uniquely sensitive and created within the scope of the carrier-subscriber relationship, as the Supreme Court recognized in *Carpenter*.

Congress gave the FCC clear authority to protect subscriber data when it enacted Section 222 in 1996, and then explicitly included location information in the scope of those provisions in 1999 given the emerging use of wireless services. The evolution in wireless networks since then have only increased the need for these privacy protections. The Supreme Court has found that cell phone location data is of unique quantity, quality, and pervasiveness, thereby meriting heightened privacy protections. In *Riley*, a unanimous court noted that cell phones are so prevalent in "daily life that the proverbial visitor from Mars might conclude they were an important feature of the human anatomy." *Riley*, 573 U.S. at 385. In *Carpenter*, the court described cell phone location records as uniquely comprehensive, capable of retrospective collection and of sensitive inferences, exposed to carriers in a manner that is not meaningfully voluntary by subscribers,

and at that time, more than five years ago, "rapidly approaching GPS-level precision." *Carpenter*, 585 U.S. at 297–98, 312–13, 315.

Today, mobile location data can be more precise than GPS. *See* subsection II.B, *infra*. The *Carpenter* court starkly distinguished CSLI from other types of commercial information that consumers entrust to service providers: "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." *Carpenter*, 585 U.S. at 297. Without FCC protection of location data related to telecommunications services, subscribers are likely to experience significant harm.

Mobile location data can expose "familial, political, professional, religious, and sexual associations", *id.*at 311 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)), and reveal other profoundly sensitive information such as medical information.[6] This is in part because unlike traditional GPS, phone subscribers carry their device with them on their person everywhere they go, including inside

[6] A cell phone "faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 585 U.S. at 311 (describing mobile location data in contrast to GPS data). *See also United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd in part sub nom. Jones*, 565 U.S. (2012) (noting that the sequence of a person's movements can reveal "whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.").

buildings. *Carpenter*, 585 U.S. at 311 (quoting *Riley*, 573 U.S. at 395 in noting that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower"); *id.* at 311–12, 315 (carrying a cell phone is essentially a prerequisite to participation in modern society, and users "compulsively carry cell phones with them all the time").

This creates an exhaustive record of the subscriber's activities, which can reveal patterns over time, *see, e.g.*, *United States v. Rhine*, 652 F. Supp. 3d 38, 82 (D.D.C. 2023) (citing *Carpenter*, 585 U.S. at 305–313 and describing an " 'all-encompassing record' of a person's whereabouts, including the ability to 'reconstruct a person's movements' retrospectively"), and facilitate identification of specific individuals. *See, e.g.*, Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Sci. Rep. 3 (Mar. 2013)[7] (four points of location data enough to uniquely identify 95% of cellphone users, 50% can be individually categorized with two random datapoints); Manilo De Domenico, et al., *Interdependence and Predictability of Human Mobility and Social Interactions*, Pervasive and Mobile Computing 18 (July 2013)[8] (given a large enough data set, analysts can predict an individual's location months or years

[7] https://pubmed.ncbi.nlm.nih.gov/23524645/.
[8] https://arxiv.org/pdf/1210.2376.

ahead of time); *see also Carpenter*, 585 U.S. at 314–15 (noting that a detailed chronicle of someone's location itself reveals identifying information). The Supreme Court has found that cell phones are indispensable aspects of everyday life that produce location data continuously without any action required by the user—in fact, the technology was designed to function that way. *See id.* at 315 ("[v]irtually any activity on the phone generates CSLI" and so there is "no way to avoid leaving behind a trail of location data" without disconnecting from the network entirely).

Beyond the immediate privacy harms caused by the unauthorized distribution of mobile location data, as described in *Carpenter* and *Riley*, there are additional downstream harms that can flow from misuse of this kind of exhaustive record of location data. As was revealed during the FCC's investigation preceding this challenged enforcement action, CSLI data has been abused by law enforcement and bounty hunters, including collecting data on other law enforcement officers and on a judge. *See* Statement of Commissioner Geoffrey Starks, Approving in Part and Dissenting in Part, *In Re: T-Mobile USA, Inc.*, File No.: EB-TCD-18-00027702, FCC 20-27 at 3–4 (Rel. Feb. 28, 2020) [hereinafter *Comm'r Starks Stm't*].[9] Members of Congress have cited to other sources of location data that put historically marginalized groups at heightened risk, for

[9] https://docs.fcc.gov/public/attachments/FCC-20-27A5.pdf.

examples survivors of domestic violence or LGBTQ+ clergy—*see, e.g.*, Letter from Reps. Katie Porter and Jamie Raskin, et al., to FTC and FCC Chairwomen at 1–2 (Dec. 9, 2021)[10]—or women seeking reproductive health services, *see, e.g.*, Press Release, *Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics* (Feb. 13, 2024).[11] Even non-marginalized groups can be subject to financial consequences based on location information gathered about them without their knowledge, *see, e.g.*, Letter from Sen. Ron Wyden to FTC Chairwoman (July 26, 2024),[12] or can expose public officials to lethal harm, *see, e.g.*, "Daniel's Law."[13] Similar risks

---

[10] https://raskin.house.gov/_cache/files/b/b/bba089eb-7b97-4b74-a7ad-f44cef5fd1bc/EA1DAC0E56C44CC379A28B713093351B.porter-raskin-location-data-privacy-letter-to-ftc-fcc.pdf.

[11] https://www.wyden.senate.gov/news/press-releases/wyden-reveals-phone-data-used-to-target-abortion-misinformation-at-visitors-to-hundreds-of-reproductive-health-clinics; *see also The Location Data Market, Data Brokers, and Threats to Americans' Freedoms, Privacy and Safety*, *Hearing before Joint Comm. on Consumer Prot. and Pro. Licensure* (Mass. June 26, 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/07/Sherman-Justin_WrittenTestimony_MA_Legislature.pdf (written testimony of Justin Sherman).

[12] https://www.wyden.senate.gov/imo/media/doc/wyden-markey_auto_privacy_letter_to_ftc.pdf.

[13] https://danielslaw.nj.gov/ (District Judge Esther Salas describing the motivation for Daniel's Law as "protecting the lives of public servants from retaliatory threats and violence") (0:50). Daniel's Law pertains to residential address only, whereas mobile location goes beyond where a user's phone spends the night. *See* Stuart Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-

apply to the unregulated use of mobile location data here; given the unique harms associated with location data, it is crucial the FCC has authority to protect that data against misuse.

B. Mobile location data has become even more sensitive as wireless infrastructure and data analysis technologies have become more advanced.

This Court should consider the sensitivity, pervasiveness, and involuntariness of mobile location data collection in light of its prevalence and precision today, as well as the historical context within which the technology has continued to develop, because of the consumer-focused purpose of Section 222 and the broad scope of its CPNI definition.

The precision and accuracy of mobile location data has predictably increased as wireless infrastructure has advanced and network density has increased. Even at the time *Carpenter* was decided, the Supreme Court observed that CSLI can "pinpoint a phone's location within 50 meters," *Carpenter*, 585 U.S. at 313. Locating a mobile device based on cell site data becomes more precise as site density increases. *Id.* ("[a]s the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk"). The increased density of cell sites can result in location accuracy more precise than 10 feet in some areas. *See, e.g.*,

---

phone.html (NY Times obtained large geolocation dataset and could identify and track celebrities, law enforcement officers, "high-powered lawyers (and their guests)," and even a Secret Service agent assigned to President Trump).

Robert M. Bloom and William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information & the Need for Fourth Amendment Protections*, 106 J. Crim. L. & Criminology 167, 176 (2016).

Subscribers can be identified by what cell sector they connect to the network through, or even more precisely by triangulating their location relative to multiple sites. Consequently, as wireless infrastructure relies upon increasingly granular sectors, mobile location data becomes more precise. *See, e.g.*, Statement for the Record, Prof. Matt Blaze, H. Subcomm. Crime, Terrorism, and Homeland Sec., Hearing on the Geolocation Privacy and Surveillance (GPS) Act at 10 (May 17, 2012) ("in urban areas and other environments that use microcells, a sector's coverage area can…effectively identif[y] individual floors and rooms within buildings"). Similarly, as the density of cell sites increases, the accuracy of location data derived by triangulation becomes more precise. *See* Congressional Research Service, *Legal Standard for Disclosure of Cell-Site Information and Geolocation Information* 3 (June 29, 2010).[14] Industry estimates that the total number of cell sites in the United States increased from 913 in 1986, *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 832 (S.D. Tex. 2010), *subsequently vacated*, 724 F.3d 600 (5th Cir. 2013) (citing CTIA survey), to more than 256,000 in 2011, *U.S. Wireless Quick Facts*, CTIA: The Wireless Ass'n (visited Feb. 28,

[14] https://sgp.fas.org/crs/intel/crs-csi.pdf.

2012),[15] to more than 432,000 in 2024, CTIA, *2024 Annual Survey Highlights* at 6 (Sept. 2024).[16] In 2023, there were more than 202,000 outdoor small cells supporting more than 466,000 small cell nodes, Fed. Commc'ns Comm'n, *2024 Communications Marketplace Report* at ¶ 76 (Rel. Dec. 31, 2024),[17] and more than 775,000 indoor small cell nodes, *id*.[18] Small cells are radio equipment and antennae that can be placed on smaller structures like streetlights rather than their own towers, installed every few blocks rather than miles apart. *See* CTIA, *What is a Small Cell? A Brief Explainer*.[19]

As of 2022, small cells represented more than 34% of all cell sites. *See* CTIA, *U.S. Wireless Consumer Data Use, Industry Investment Again Hits Record Highs, CTIA Annual Survey Finds* (July 25, 2023).[20] Simultaneously, the commercial demand for location data, such as CSLI, has nearly tripled over the last eight years, from approximately $8 billion in 2016, *see* Grand View Research, *Location Intelligence Market Size, Share & Trends Analysis Report By Application*

---

[15] Archived by the Wayback Machine at http://web.archive.org/web/20120228052232/http://ctia.org/media/industry_info/index.cfm/aid/10323.
[16] https://api.ctia.org/wp-content/uploads/2024/09/2024-Annual-Survey.pdf. CTIA notes this is a 24% increase in number of cell sites since 2018.
[17] https://docs.fcc.gov/public/attachments/FCC-24-136A1.pdf (citing WIA 2023 Wireless Infrastructure Report at 8; WIA Comments at 1).
[18] *Id.* (citing WIA 2023 Wireless Infrastructure Report at 9; WIA Comments at 1).
[19] https://www.ctia.org/news/what-is-a-small-cell.
[20] https://www.ctia.org/news/u-s-wireless-consumer-data-use-industry-investment-again-hit-record-highs-ctia-annual-survey-finds.

(July 2018),[21] to $12 billion in 2021, *see* Jon Keegan and Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (updated Sept. 30, 2021),[22] to more than $21 billion in 2024, *see* Grand View Research (last visited Jan. 9, 2025).[23] Members of Congress have expressed concern about this industry. *See, e.g.*, Letter from Rep. Carolyn Maloney, et al. to SafeGraph CEO (July 7, 2022).[24]

Congress enacted Section 222 to ensure that carriers would safeguard the data of their subscribers, and that customers would not have to forfeit their privacy in order to access modern telecommunications networks. Much has changed since the law was passed, but the basic principle remains. Telephones used to be tethered to the wall, or to a public booth—the location of an active call was static, and it was futuristic to imagine a consumer phone that could be carried everywhere you go continuously creating location data in its attempts to stay reachable by the

[21] Archived by the Wayback Machine at http://web.archive.org/web/20181127035048/https:/www.grandviewresearch.com/industry-analysis/location-intelligence-market.
[22] https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.
[23] Archived by the Wayback Machine at http://web.archive.org/web/20250102184549/https://www.grandviewresearch.com/industry-analysis/location-intelligence-market.
[24] https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/2022-07-07.CBM%20RK%20Jacobs%20to%20Hoffman-SafeGraph%20re%20Abortion%20Location%20Tracking.pdf.

network even while not actively on a phone call. Moreover, multiple individuals might have shared use of a landline phone, whereas today even many children and young adults use their own cell phone for everyday tasks. *See, e.g.*, Statista, *Share of Children Owning a Smartphone in the United States in 2015, 2019, 2021, by age*;[25] Anya Kamenetz, *It's A Smartphone Life: More Than Half Of U.S. Children Now Have One*, NPR (Oct. 31, 2019).[26] Unlike the rotary phones of old, phone location data is now pervasive and unavoidable, with the ability to identify individuals and facilitate financial, physical, and other downstream harms resulting from misuse of that data.

It is not reasonable to expose wireless customers to the risks of these downstream harms, and there is no clear reason why carriers should be giving any third-party direct access to mobile location data absent a subscriber's affirmative direction. Indeed, there are other and better ways if a subscriber wants to disclose their location data for a specific purpose. Numerous software applications (apps) can facilitate consumer-initiated transactions or services that rely on location data—for example a consumer might want to use their location to identify the fastest route based on current traffic patterns or to search for the closest open

[25] https://www.statista.com/statistics/1324262/children-owning-a-smartphone-by-age-us/.
[26] https://www.npr.org/2019/10/31/774838891/its-a-smartphone-life-more-than-half-of-u-s-children-now-have-one (this percentage exceeds 80% for teenagers).

restaurant. As the FCC's investigation uncovered, misuse of the mobile location data that subscribers cannot help but continuously produce and entrust to carriers' custody has come to represent an extreme risk, not a mere hypothetical risk, exposing the underlying problem with location-based services programs like T-Mobile's. *See* Comm'r Starks Stm't at 4, 6.

As telecommunications services continue to evolve, it is important for the FCC to evaluate and update its interpretation of Section 222 to keep pace with technological change.

III. The FCC is the best-positioned regulator to address carrier misuse of subscriber data.

Consumers need privacy protections now. Cell phones are personal devices, containing records of personal communications, not merely voice calls but text messages, including with essential and confidential services such as crisis hotlines. In creating consumer protection agencies such as the FTC and the FCC, Congress entrusted and empowered those regulators to address evolving technology issues such as these, because advances in technology and its use by bad actors occur at a more rapid pace than legislators can keep up with. Of these two, the FCC is in the best position to regulate carrier misuse of subscriber data. Other checks against corporate misconduct have proven incapable of reining in these abuses. Because the relationship between a carrier and their subscriber is so akin to that of a fiduciary, especially as it relates to the sensitive and non-voluntary nature of

mobile location information, this court should not read Section 222 as a narrow directive from Congress that shields companies but rather as a broad privacy safeguard that protects consumers.

The FCC has been regulating carriers for roughly a century; it has more experience and familiarity with the practices of carriers than any other regulator. Clear authority and enforcement capacity are necessary to ensure that companies have a strong incentive to safeguard the uniquely sensitive mobile location data; the FCC possesses both. Indeed, even beyond the CPNI provisions of Section 222, Congress empowered the agency with broader privacy authorities in Sections 222(a) and 201(b), in addition to the general ancillary jurisdiction under the Communications Act. If the Court held that the FCC lacks jurisdiction here, there would be a critical gap in regulatory authority that would mean cell phone subscribers have essentially no location privacy protections. Carriers are aware of this and argue jurisdiction as suits their convenience, in a decades-long shell game inviting consumers and courts to try to guess which authority actually applies to their privacy and cybersecurity practices. We urge this Court to resolve this swiftly: Congress has always placed the authority with the FCC.

In Section 222, Congress tasked the FCC with ensuring that every telecommunications carrier protects the confidentiality of proprietary information of and relating to its customers. 47 U.S.C. § 222(a). This protection is vital because

as the FCC has recently noted in a breach reporting case, carriers are exempt in many cases from authority under Section 5 of the FTC Act when they are acting in their capacity as common carriers. *See, e.g.*, Resp'ts Br., *Ohio Telecom Association, et al., v. Federal Communications Commission and United States of America*, 6th Cir. Nos. 24-3133, 24-3206, 24-3252 at 26 (filed July 29, 2024). It would be absurd to draw an imaginary line between CSLI generated by active voice calls and CSLI generated by continuous passive network registration, saying the former is the purview of the FCC and the latter is the responsibility of the FTC—it is the same data, collected by the same technological infrastructure, controlled by the same entities. Other federal agencies are simply not as well positioned to enforce privacy regulations against the large carriers.

Other traditional methods for incentivizing good corporate conduct have proven ineffective here. Carrier self-regulation has not worked and will not work. Even with Section 222 in force and with clear indications that privacy was a priority for the FCC, these carriers still chose to increase their revenue over following the law and protecting user privacy. Having no privacy authority will only exacerbate that problem. Beginning in 2008, the FCC required carriers to complete annual reporting about misuse of CPNI, including any litigation brought by carriers against data brokers. *See, e.g.*, Fed. Commc'ns Comm'n, *Customer*

Proprietary Network Information (CPNI) Certification Home.[27] With the exception of the very first year the FCC imposed this requirement, neither T-Mobile nor Sprint has again reported bringing litigation against a data broker on behalf of injured consumers, *see* Sprint Nextel Corp., *in re Annual CPNI Compliance Certification*, EB Dkt. No. 06-36 (Mar. 3, 2008),[28] not even resulting from the egregious conduct Securus facilitated. *See, e.g.*, Comm'r Starks Stm't at 3–5. Carriers like T-Mobile have demonstrated that they are not only unlikely to police misuse of mobile location data by their partners, but also that they will evade liability at every opportunity.

The telecom giants have avoided civil enforcement by their own subscribers seeking to vindicate their privacy rights, persuading courts that their arbitration clauses require dismissal of private lawsuits. *See, e.g.*, *Baron v. Sprint Corp.*, 2019 WL 5456796 (D. Md. Oct. 24, 2019) (resolving four class action suits filed against the major carriers). The companies avoided class action liability by arguing that the dense and largely unread terms of service required customers to use arbitration to resolve any legal disputes. *See id.* at *1–4. Thus, although the alleged conduct of the providers was "indeed troubling," *id.* at *3, carriers like T-Mobile were able to effectively foreclose their own customers' efforts to hold them accountable for the

[27] https://apps.fcc.gov/eb/CPNI/.
[28] https://www.fcc.gov/ecfs/search/search-filings/filing/5515012959; annual filings in EB Dkt. No. 06-36 as of March 1, 2024.

alleged CPNI violations. *See* Aaron Mackey, *Forced Arbitration Thwarts Legal Challenge to AT&T's Disclosure of Customer Location Data*, EFF Deeplinks (April 14, 2021).[29] Should T-Mobile prevail in its challenge here, it would effectively result in the providers facing no legal consequences for violations of a federal privacy law that protects their customers.

In multiple contexts implicating subscriber data privacy and cybersecurity, carriers repeatedly assert that the data at issue is not CPNI and therefore beyond the FCC's reach. Fortunately, courts have not fallen for this argument in cases involving SIM swap attacks. *See, e.g., Terpin v. AT&T Mobility LLC,* 118 F.4th 1102, 1117 (9th Cir. 2024) (rejecting industry arguments that a SIM swap necessarily does not entail CPNI, finding triable fact as to whether AT&T gave hackers access to plaintiff's CPNI). This court should not narrowly construe the definition of CPNI.

In Section 222, Congress created a clear prohibition against disclosure of subscriber data in the exact manner that happened in this case: carriers disclosed CSLI to location aggregators without the affirmative request of the subscriber and beyond what was necessary for the provision of the carrier's services to the subscriber. A system by which third-party brokers are provided direct access to

[29] https://www.eff.org/deeplinks/2021/04/forced-arbitration-thwarts-legal-challenge-atts-disclosure-customer-location-data.

precise location data obtained as a result of the carrier-customer relationship inherently violates Section 222—as opposed to downstream applications or services that obtain data from the user or device itself. Misuse is not a prerequisite for a violation, although actual misuse did occur here. *See* Comm'r Starks Stm't at 1–2, 4. Carriers did not need to share this extremely sensitive data absent a clear, applicable statutory exception; carriers chose to share it. It does not matter that T-Mobile thought its system was adequate, especially where it did not adequately investigate. *See, e.g.*, Resp'ts Br. at 19, 22, 55 n.10.

Carriers act in a fiduciary capacity when it comes to mobile location data, due to the unique sensitivity and pervasiveness of the data, as well as the unavoidability with which subscribers must surrender it, by virtue of the nature of the carrier-customer relationship. In the instant case, T-Mobile chose to give access to uniquely sensitive mobile location data to location aggregators; it cannot thereby offload its own liability for falling short of its obligations under Section 222. Although in his dissent in *Carpenter* Justice Gorsuch went awry in characterizing personal data as property, his description of a fiduciary-type relationship between carriers and their subscribers is illustrative:

> At least some of this Court's decisions have already suggested that use of technology is functionally compelled by the demands of modern life…Plainly, customers have substantial legal interests in this information [data protected under Section 222], including at least some right to include, exclude, and control its use.

Carpenter v. United States, 585 U.S. 296, 402, 406 (2018) (Gorsuch, J., dissenting). Gorsuch describes Section 222 as imposing broad restrictions on a carrier's ability to use sensitive data about their customers by virtue of the legal interest Congress clearly conferred upon subscribers in the information collected about them by their carriers.

The requirements of Section 222 are clear. Whether a carrier adequately secured the location data they chose to warehouse is of no moment as to whether that carrier is statutorily liable for misuse of data it chose to disclose to a location aggregator, especially when that carrier is acting in essence as a fiduciary of uniquely sensitive, unavoidably-shared location data. There is no leeway for reasonableness. Moreover, it is well-established and commonsense that a deficient practice need not actually cause harm to violate a rule establishing minimum adequate safeguards. Although in the context of private litigation a plaintiff may struggle to demonstrate standing for bare procedural violations, a regulator must be able to enforce its rules.

If this Court lets carriers escape liability here, it would send a clear message that the industry's pattern of negligence and evasion is permissible under law, despite Congress's directive to the FCC to protect consumer privacy by regulating carriers.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to affirm the FCC's Forfeiture Orders.

Date: January 17, 2025

/s/ Alan Butler
Alan Butler
Christopher Frascella
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

/s/ Samir Jain
Samir Jain
Eric Null
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K St NW, Suite 200
Washington, DC 20005
(202) 637-9800

/s/ Aaron Mackey
Aaron Mackey
Adam Schwartz
Mario Trujillo
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Attorneys for Amici Curiae Electronic Privacy Information Center, the Center for Democracy & Technology, Electronic Frontier Foundation, Privacy Rights Clearinghouse, Public Knowledge

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(4) because this brief contains 6,491 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point font in Times New Roman font.

Signature: *<u>/s/ Alan Butler</u>* **Date:** January 17, 2025

CERTIFICATE OF SERVICE

I certify that on January 17, 2025, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the D.C. Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: January 17, 2025

/s/ Alan Butler
Alan Butler
Christopher Frascella
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

/s/ Samir Jain
Samir Jain
Eric Null
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K St NW, Suite 200
Washington, DC 20005
(202) 637-9800

/s/ Aaron Mackey
Aaron Mackey
Adam Schwartz
Mario Trujillo
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Attorneys for Amici Curiae Electronic Privacy Information Center, the Center for Democracy & Technology, Electronic Frontier Foundation, Privacy Rights Clearinghouse, Public Knowledge