Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Location-Based Routing for Wireless 911 Calls	)	PS Docket No. 18–64

COMMENTS ON NOTICE OF PROPOSED RULEMAKING

by

Electronic Privacy Information Center (EPIC)

Submitted February 16, 2023

Megan Iorio
Senior Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

Summary

The Commission should clarify the privacy and security rules for device-based location data—and routing data more generally—before it sets a deadline for carriers to begin collecting and disclosing this data. The type of device-based location data the Commission proposes that carriers collect and disclose is very precise and, therefore, very sensitive data. Carriers have misused location data in the past, selling the data to data brokers who have, in turn, made the data available to any willing buyer, from bounty hunters to the government. The surveillance that location data enables disproportionately impacts vulnerable groups. To ensure equity, the Commission should set strong, clear privacy and security rules for device-based location data from the outset.

Specifically, we recommend that the Commission:

1. Clarify how the Customer Proprietary Network Information (CPNI) rules apply to device-based location data;
2. Apply the NEAD rules to all device-based location data, not just dispatch data;
3. Clarify what constitutes "911 purposes;"
4. Clarify carriers' responsibilities for third-party vendors; and
5. Adopt additional data minimization rules, such as a deletion rule to ensure that carriers do not store precise location data for longer than necessary.

Table of Contents

Comments

I. Introduction

The **Electronic Privacy Information Center (EPIC)** files these comments to urge the Federal Communications Commission ("Commission" or "FCC") to clarify the privacy and security rules for device-based location data before setting a deadline for carriers to begin collecting and disclosing this data. We appreciate the Commission's desire to improve emergency response times. However, the Commission's proposal would require carriers to collect and disclose more precise—and thus, more sensitive—location data than ever before. Given the recent, high-profile, and widespread failure of carriers to safeguard location data, we urge the Commission to adopt clear rules that ensure the privacy and security of device-based location data from the outset.

We also urge the Commission to consider how the lack of clear privacy and security safeguards would have a disproportionately negative impact on certain vulnerable groups. Government entities have used location data to target immigrants, Muslims, and protesters. Bounty hunters and abusers have used carrier location data to track down individuals. Some states have moved to criminalize almost all abortion and location data may become a useful tool for enforcing these laws. To ensure equity, the Commission must adopt rules that prevent carrier location data from being used to surveil, harass, and oppress those with marginalized identities.

We urge the Commission to:

1. Clarify how the CPNI rules apply to device-based location data;
2. Apply the NEAD rules to all device-based location data, not just dispatch data;
3. Clarify what constitutes "911 purposes;"
4. Clarify carriers' responsibilities for third-party vendors; and

5. Adopt additional data minimization rules, such as a deletion rule to ensure that carriers do not store precise location data for longer than necessary.

Microsoft raised concerns about the privacy and security of device-based location data in its recent Reply Comments in this docket.[1] The Commission also has an established record of addressing privacy and security concerns when they are raised, even if the Commission did not incorporate those concerns initially.[2] We hope the Commission will do the same here.

II. Carriers Have Misused Emergency Location Data Before.

The Commission is aware that carriers have misused location data in the past.[3] Device-based location information at the level of precision the Commission will require carriers to collect (within a 165-foot radius) is highly sensitive information—even more sensitive than the cell-site location information carriers previously collected and sold.[4] The Commission's proposal requires carriers that do not currently collect this highly sensitive data to start to collect it within six to eighteen months.[5] To ensure that this new trove of sensitive data is not misused, the Commission must be clear about the applicable privacy and security rules before setting a deadline for implementation.[6]

---

[1] *See In re* Location-Based Routing for Wireless 911 Calls*,* Comments of Microsoft Corporation, PS Docket No. 18-64, at 5 (filed Jul. 25, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/10725399907952 ("We believe that device users' privacy and security interests can and should be preserved when enabling necessary and proportionate uses of location information for emergency calling. For example, to address some privacy concerns, access to location information by responders could be limited to when an emergency call or text is made and any subsequent use of the information could be restricted to emergency call/text routing and emergency services dispatch.").

[2] *See, e.g.*, Jon Brodkin, Ajit Pai's plan for phone location data never mentions the word "privacy", Ars Technica (Mar. 14, 2019), https://arstechnica.com/tech-policy/2019/03/despite-carriers-selling-911-location-data-fcc-ignores-privacy-in-new-rules/.

[3] *See* FCC Proposes Over $200M in Fines for Wireless Location Data Violations (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations.

[4] *See* Fed. Commc'ns Comm'n, *In re* Location-Based Routing for Wireless 911 Calls, Notice of Proposed Rulemaking in PS Docket No. 18-64, 88 Fed. Reg. 2565, 2573 (Jan. 17, 2023), *available at* https://www.federalregister.gov/d/2023-00519/p-102 [hereinafter "NPRM"].

[5] *See* id. at 2566, *available at* https://www.federalregister.gov/d/2023-00519/p-23.

[6] *See* id. at 2570, *available at* https://www.federalregister.gov/d/2023-00519/p-74.

The Commission is aware of the risks inherent in collecting and disclosing subscriber location data. Commissioner Starks has noted the harm that misuse of emergency location data can cause: "While precise location information is critical to an effective emergency response, it can also be dangerous in the wrong hands."[7] Chairwoman Rosenworcel recently observed that "the highly sensitive nature of [geolocation] data—especially when location data is combined with other types of data—and the ways in which this data is stored and shared with third parties is of utmost importance to consumer safety and privacy."[8]

The location data market is a multi-billion-dollar industry.[9] Like many other companies that collect location data, carriers have sold their customers' information to data brokers who have then sold access to anyone willing to buy—from bounty hunters[10] to the government. The disclosure and sale of location data has serious implications for equity because vulnerable people are most likely to be the targets of surveillance.[11] For example, ICE has sought location data to target immigrants.[12] Several government entities have used location data of Muslim phone subscribers to surveil Muslim communities.[13] In states that have criminalized abortion, law

---

[7] *See, e.g.*, *In re* Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Statement of Commissioner Geoffrey Starks, FCC 20-98 (July 17, 2020), https://www.fcc.gov/ecfs/document/071729921305/4 [hereinafter "Comm'r Starks E911 Statement"].
[8] Press Release, Chairwoman Rosenworcel Probes Top Mobile Carriers on Data Privacy Practices (Jul. 19, 2022), https://docs.fcc.gov/public/attachments/DOC-385446A1.pdf.
[9] *See* Joe Keegan & Alfred Ng, There's a Multibillion-Dollar Market for Your Phone's Location Data, The Markup (Sep. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.
[10] *See* Joseph Cox, "I Gave a Bounty Hunter $300. Then He Located Our Phone." Motherboard (Jan. 8, 2019), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.
[11] *See* NPRM at 2576, https://www.federalregister.gov/d/2023-00519/p-141.
[12] *See, e.g.*, Dana Khabbaz, EPIC, DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information 36 (2022), https://epic.org/wp-content/uploads/2022/08/DHS-Data-Reservoir-Report-Aug2022.pdf.
[13] *See, e.g.*, Joseph Cox, Leaked Location Data Shows Another Muslim Prayer App Tracking Users, Motherboard (Jan. 11, 2021), https://www.vice.com/en/article/xgz4n3/muslim-app-location-data-salaat-first; Glenn Blain, Court of Appeals Allows NYPD to Hide Records of Possible Islamic Surveillance,

enforcement or anti-abortion extremists could use location data to target individuals seeking reproductive care.[14] Location data can be used to infer intimate details about a person's life, such as their sexual orientation,[15] which could then be used to blackmail, harass, or otherwise threaten a person's life or livelihood. Companies have touted the ability to track protesters' cellphones and identify protesters' age, gender, and race.[16] Stalkers and abusers (including those who work for law enforcement organizations) may use this information to track, harass, and/or otherwise attempt to exert control over their intended victims.[17]

In light of carriers' historical misuse of location data, the increased sensitivity of the location data to be collected, and the disproportionate impact on vulnerable individuals, we strongly urge the Commission to revise its proposals to ensure that the privacy and security of emergency location data is properly safeguarded.

III. The Commission Should Articulate Clear, Strong Privacy Rules for Emergency Location Data.

In previous proceedings, the Commission established privacy and security rules for

---

Daily News (Mar. 29, 2018), https://www.nydailynews.com/news/politics/court-nypd-hide-records-islamic-surveillance-article-1.3903652.

[14] *See, e.g.*, Sara Geoghegan and Dana Khabbaz, Reproductive Privacy in the Age of Surveillance Capitalism, Electronic Privacy Information Center (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/; Joseph Cox, Data Broker Is Selling Location Data of People Who Visit Abortion Clinics, Motherboard (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

[15] *See, e.g.*, Molly Olmstead, A Prominent Priest Was Outed for Using Grindr. Experts Say It's a Warning Sign, Slate (July 21, 2021), https://slate.com/technology/2021/07/catholic-priest-grindr-data-privacy.html.

[16] *See, e.g.*, Zak Doffman, Black Lives Matter: US Protesters Tracked By Secretive Phone Location Technology, Forbes (Jun. 26, 2020), https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=5e8ac2424a1e; Sara Morrison, *The Hidden Trackers in Your Phone, Explained*, VOX (July 8, 2020), https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location.

[17] *See, e.g.*, Joseph Cox, U.S. Marshal Charged for Using Cop Phone Location Tool to Track People He Knew, Motherboard (June 14, 2022), https://www.vice.com/en/article/k7bqew/us-marshal-securus-phone-location-tracked; Conor Friedersdorf, Police Have a Much Bigger Domestic-Abuse Problem Than the NFL Does, The Atlantic (Sept. 2014), https://www.theatlantic.com/national/archive/2014/09/police-officers-who-hit-their-wives-or-girlfriends/380329/.

certain types of location data,[18] but it is unclear how those rules will apply to device-based location data. The Commission should clearly articulate what privacy and security rules apply to device-based location data before requiring carriers to collect and disclose this data. We urge the Commission to:

1. Clarify how the CPNI rules apply to device-based location data;
2. Apply the NEAD rules to all device-based location data, not just dispatch data;
3. Clarify what constitutes "911 purposes;"
4. Clarify carriers' responsibilities for the actions of third-party vendors; and
5. Adopt additional data minimization rules, such as a deletion rule to ensure that carriers do not store precise location data for longer than necessary.

Section 222 defines CPNI as "information that relates to the…destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and … [available] solely by virtue of the carrier-customer relationship."[19] CPNI explicitly includes location data, even while the phone subscriber is not

[18] *See, e.g.*, *In re* Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Memorandum Opinion and Order, 32 FCC Rcd 9699 (Nov. 14, 2017) (approving privacy and security plan for NEAD), *available at* https://digital.library.unt.edu/ark:/67531/metadc1225670/m1/603/ [hereinafter "2017 Order"]; id. at 9703 ¶ 13 ("[NEAD Privacy and Security Plan] also provides that '[e]xcept as may be required by applicable law, information contained in the NEAD Platform will not be disclosed to third parties, including government entities, other than for 911 purposes'"); *In re* Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Sixth Report and Order and Order on Reconsideration, FCC 20-98 at ¶ 56 (July 17, 2020), https://www.fcc.gov/ecfs/search/search-filings/filing/071729921305 ("We adopt our proposal to require CMRS providers to implement privacy and security safeguards to non-National Emergency Address Database dispatchable location technologies equivalent to those that applied to the National Emergency Address Database….CMRS providers must certify that neither they nor any third party they rely on to obtain dispatchable location information for 911 purposes will use such information for any non-911 purpose, except with prior express consent or as required by law") [hereinafter "6th R&O Recon."]; id. at 26 ¶ 57 ("Similarly, CMRS providers who work with third-party vendors are responsible for ensuring that those vendors take appropriate measures to address privacy and security concerns."). *See also*, *In re* Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Fifth Report and Order and Fifth Further Notice of Proposed Rulemaking, 34 FCC Rcd 11592, 11615-16 at ¶ 51 (Nov. 25, 2019), *available at* https://digital.library.unt.edu/ark:/67531/metadc1637223/m1/593/ [hereinafter "5RO5FNPRM"].

[19] 47 U.S.C. § 222(h)(1)(A).

actively using their phone to make a call.[20] The Commission has found that CPNI is a subset of proprietary information subject to greater restrictions.[21] These restrictions include only using, disclosing or permitting access to individually identifiable CPNI in its provision of the service from which such information is derived, or in services necessary to or used in the provision of such service.[22] They also include exceptions for providing call location information to a public safety answering point (PSAP) or to specific services solely for the purpose of assisting the delivery of emergency services in response to an emergency.[23] The Commission has articulated how CPNI rules apply to other types of location data used for 911 call routing and dispatch.[24] The Commission should clarify how its CPNI rules and restrictions apply to device-based location data.

Second, the Commission should state that the privacy and security rules that apply to dispatchable location data also apply to routing data. In its 2017 Order, the Commission stated that "information contained in the NEAD Platform will not be disclosed to third parties, including government entities, other than for 911 purposes."[25] The Commission previously stated that, following the demise of NEAD, the NEAD rules would apply to non-NEAD dispatchable

---

[20] *See In re* Data Breach Reporting Requirements, WC Docket No. 22-21, Notice of Proposed Rulemaking, FCC 22-120 at ¶ 2 (Jan. 6, 2023), https://docs.fcc.gov/public/attachments/FCC-22-102A1.pdf (citing to Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 FCC Rcd 6927, 6930 at ¶ 5 [hereinafter "2007 CPNI Order"]; also citing to AT&T, Inc., File No.: EB-TCD-18-00027704, Notice of Apparently Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1757, paras. 33-35 (2020) [hereinafter "2020 NAL"]).

[21] *See, e.g.*, In re TerraCom Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175, at ¶ 14-16 (Oct. 24, 2014), https://docs.fcc.gov/public/attachments/FCC-14-173A1.pdf (discussing the Commission's authority to protect privacy under Section 222 and citing to 2007 CPNI Order at 6946) [hereinafter "2014 NAL"].

[22] 47 U.S.C. § 222(c)(1).

[23] 47 U.S.C. § 222(d)(4).

[24] *See e.g.*, 5RO5FNPRM, 34 FCC Rcd 11592, 11615-16 at ¶ 51 (Nov. 25, 2019), *available at* https://digital.library.unt.edu/ark:/67531/metadc1637223/m1/593/.

[25] 2017 Order at ¶ 13.

location data.[26] We urge the Commission to clarify that these privacy and security requirements also apply to location-based routing data.

Third, we urge the Commission to clarify the data use cases within the scope of "for 911 purposes" and urge the Commission to limit the only to uses necessary to route calls and dispatch assistance. In particular, we urge the Commission to clarify that law enforcement cannot use 911 location data for investigative leads or for enforcement unrelated to the purpose of the 911 call.

Fourth, we urge the Commission to clarify that carriers are responsible for their third-party vendors' collection, use, and disclosure of device-based location data. In its July 2020 Order, the Commission was said that "CMRS providers who work with third-party vendors are responsible for ensuring that those vendors take appropriate measures to address privacy and security concerns."[27] Clarifying third-party liability in this context is especially important given the limits of the Commission's enforcement authority over downstream entities who receive location data from carriers, a concern which Commission Starks has previous articulated.[28]

Finally, we urge the Commission to adopt additional data minimization rules for emergency location data. This is consistent with our prior comments to the Commission in

[26] *See* id. at ¶ 56. This mirrored the March 2019 NEAD requirements. *See In re* Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Fourth Further Notice of Proposed Rulemaking, FCC 19-20 at ¶ 29 (Mar. 18, 2019), https://www.fcc.gov/ecfs/document/031804287561/4 ("CMRS providers must certify that they will not use the NEAD or associated data for any purpose other than for the purpose of responding to 911 calls, except as required by law.")(internal citations omitted).
[27] 6th R&O Recon. at 26 ¶ 57.
[28] *See* 2020 NAL, Statement of Commissioner Geoffrey Starks, at 41-42 https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf ("Though Securus holds multiple FCC authorizations, I recognize that, there may be legal limitations on the Commission's ability to take enforcement against the company for its misuse of customer location data").

related dockets,[29] with Microsoft's recent Reply Comments in this docket,[30] with proposed best practice by other federal agencies and with Commissioner Starks' statements in other contexts.[31] The Commission has the authority to enforce privacy and data security protections, such as data minimization, under Sections 222 and 201(b) of the Communications Act.[32]

In particular, the Commission should require that carriers delete location data after the information is no longer necessary to provide 911 services. Routine deletion of 911 location data would prevent the creation of large location datasets that have been proven to be valuable commodities and targets for hackers. Data that is securely deleted cannot be sold or misused. It also cannot be breached. Each of the major carriers has been subject to data breaches in the last

[29] *See In re* Wireless E911 Location Accuracy Requirements; E911 Requirements for IP-Enabled Service Providers, Comments of EPIC, PS Docket No. 07-114; WC Docket No. 05-196 at 6 (Aug. 10, 2007), https://www.fcc.gov/ecfs/document/5514762968/1 ("Privacy protections should increase in response to increasing accuracy of location technology. The goal of increasing accuracy standards is public safety and better emergency response… The appropriate response to public safety accuracy increases is to increase privacy protection accordingly.").

[30] *See* Comments of Microsoft Corporation, *supra* note 1 at 5.

[31] *See, e.g.*, Fed. Trade Comm'n, In re Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FR 51273, 51277 (Aug. 22, 2022), *available at* https://www.federalregister.gov/d/2022-17752/p-88 ("The term "data security" in this ANPR refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices.") [hereinafter "FTC ANPR"]; id. at ¶¶ 43, 46, *available at* https://www.federalregister.gov/d/2022-17752/p-227; *see also* Consumer Financial Protection Bureau, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights: Outlines of Proposals and Alternatives Under Consideration 41 at Q88 (Oct. 27, 2022), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf; Speech, Starks Remarks on the Future of Broadcast Television 6 (Oct. 19, 2022), https://www.fcc.gov/document/starks-remarks-future-broadcast-television ("What data will broadcasters be able to collect from users, and how do they intend to use it? How can they follow the important principle of data minimization, and work to achieve their goals with a minimum of data collected, stored, and shared?").

[32] *See, e.g.*, 2014 NAL, at ¶ 12 ("By failing to employ reasonable data security practices to protect consumers' [proprietary information], the Companies also engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) of the Act. They failed to use even the most basic and readily available technologies and security features and thus created an unreasonable risk of unauthorized access."); id. at ¶ 14 ("The Commission has consistently interpreted Section 222(a) as requiring telecommunications carriers to protect sensitive private information, and we affirm that view here.") (internal citations omitted); Fed. Commc'ns Comm'n, Privacy/Data Security/Cybersecurity: Customer Proprietary Network Information, https://www.fcc.gov/enforcement/areas/privacy (last visited Feb. 14, 2023).

five years, further underscoring the need to minimize the amount of sensitive data the carriers store.[33]

The privacy and security risk of retaining more information than necessary is why the Federal Trade Commission included data minimization under the umbrella of "data security" in its recent ANPR,[34] and why it has brought several enforcement actions against companies that retained data longer than was necessary to provide the service requested by the consumer.[35] The Commission should articulate its authority to impose data minimization requirements for precise location data under Sections 222 and 201(b).[36]

The Commission must consider how new troves of precise location data could facilitate government surveillance. The many examples of government use of location data to facilitate surveillance and deportation of marginalized groups,[37] and relatedly of confusion as to whether it is safe for undocumented individuals to seek emergency medical care,[38] may give vulnerable

---

[33] *See*, *e.g.*, Lily Hay Newman, T-Mobile's $150 Million Security Plan Isn't Cutting It, Wired (Jan. 20, 2023), https://www.wired.com/story/tmobile-data-breach-again/; Brian Krebs, It Might Be Our Data, But It's Not Our Breach, KrebsOnSecurity (Aug. 11, 2022), https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/; Sergiu Gatlan, Verizon notifies prepaid customers their accounts were breached, Bleeping Computer (Oct. 18, 2022), https://www.bleepingcomputer.com/news/security/verizon-notifies-prepaid-customers-their-accounts-were-breached/ (as relates to data minimization specifically: "attackers couldn't access the full credit card number or the customers' banking information, financial information, passwords, Social Security numbers, tax IDs, or other personal details since user accounts don't contain this info.").

[34] *See* FTC ANPR *supra* note 31.

[35] *See, e.g.*, Complaint, *In re* Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 11(g) (Jun. 23, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter; Complaint, *In re* Drizly, LLC, FTC File No. 2023185 at ¶ 13(f) (Oct. 24, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf; Complaint, *In re* SkyMed International, Inc., FTC File No. 192-3140 at ¶ 12(e) (Feb. 5, 2021), https://www.ftc.gov/system/files/documents/cases/skymed_-_complaint.pdf.

[36] *See, e.g.*, 2014 NAL, *supra* note 21.

[37] *See, e.g.*, Khabbaz *supra* note 12; Corin Faife, ICE Uses Data Brokers to Bypass Surveillance Restrictions, Report Finds, Verge (May 10, 2022), https://www.theverge.com/2022/5/10/23065080/ice-surveillance-dragnet-data-brokers-georgetown-law.

[38] *See, e.g.*, Noah Lanard, The Right and Wrong Lessons to Take From That Viral Photo of an ICE Arrest at a Hospital, MotherJones (Mar. 13, 2020), https://www.motherjones.com/politics/2020/03/the-right-and-wrong-lessons-to-take-from-that-viral-photo-of-an-ice-arrest-at-a-hospital/.

phone subscribers pause before calling 911 and put them at risk afterward. This could undermine the Commission's important equity goals in this proceeding.

We urge the Commission to clarify the privacy and security rules for device-based location data before requiring carriers to collect and disclose this new and highly sensitive information.

IV. Conclusion

History shows that industry will not take privacy and security of location data seriously unless regulators force them to take it seriously. It is thus of the utmost importance that the Commission establish clear privacy and security rules for device-based location data before it requires carriers to collect and disclose this data.

We thank the Commission for the opportunity to comment on this important matter, and for its historical responsiveness to this important issue.

Respectfully submitted, this the 16th day of February 2023, by:

Megan Iorio
Senior Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036