FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the National	)	WC Docket No. 18-336
Suicide Hotline Act of 2018	)	

Relating to the
Notice of Proposed Rulemaking
Issued February 9, 2025

Comments of

Electronic Privacy Information Center and
Wildflower Alliance

April 3, 2025

By:
Chris Frascella
Counsel
frascella@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

Table of Contents

Comments

I. Introduction and Summary

The **Electronic Privacy Information Center (EPIC)**[1] and **Wildflower Alliance**[2] file these comments regarding the Wireline Competition Bureau's (Bureau's) request for further comment on privacy issues related to text-to-988 georouting released on February 19, 2025[3] and published in the Federal Register on March 4, 2025.[4] We thank the Bureau for its attention to and thoughtfulness about this critical issue, as individuals in crisis are unlikely to make use of valuable supportive resources if they are afraid that their anonymity, privacy, or autonomy may be at enhanced risk as a direct result of utilizing those resources. Moreover, we applaud the Commission for its attentiveness to the risks both of monetization and of misuse of help-seeker data. Our recommendations below reflect the explicit goals of the 988 program and are offered with the hope that, if adopted, they will help reassure would-be texters that the 988-affiliated service is safe to use.

---

[1] Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC has filed numerous comments with the Federal Communications Commission regarding the privacy and safety of individuals contacting emergency services, as well as regarding phone subscribers suffering heightened risks from violations of their privacy. *See, e.g.*, Comment of EPIC, *In re* Location-Based Routing for Wireless 911 Calls, PS Dkt. No. 18-64 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10216148603009; Comment of EPIC, *In re* Facilitating Implementation of Next Generation 911 Services (NG911), PS Dkt. No. 21-479 (Aug. 9, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108091404918126; Reply Comments of EPIC, et al., *In re* Supporting Survivors of Domestic and Sexual Violence, Affordable Connectivity Program, Lifeline and Link Up Reform and Modernization, WC Dkt. Nos. 22-238, 21-450, 11-42 (May 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10512158610690.

[2] The Wildflower Alliance supports healing and empowerment for broader communities and people who have been impacted by psychiatric diagnosis, trauma, extreme states, homelessness, problems with substances and other life-interrupting challenges. The Wildflower Alliance is currently one of five Recovery Learning Communities in Massachusetts. It focuses on community supports and development and regularly holds events and workshops in a variety of settings such as housing units, hospitals, jails, churches, and more.

[3] Wireline Competition Bureau Seeks Further Comment on Privacy Issues Related to Text-to-988 Georouting, WC Dkt. No. 18-336 (Feb. 19, 2025), https://docs.fcc.gov/public/attachments/DA-25-148A1.pdf.

[4] Proposed Rule, Implementation of the National Suicide Hotline Act of 2018, 90 FR 11142 (Mar. 4, 2025), https://www.federalregister.gov/documents/2025/03/04/2025-03399/implementation-of-the-national-suicide-hotline-act-of-2018 [hereinafter "988 Georouting NPRM"].

We emphasize four points in the comments below:

1) Text georouting must not lead to non-consensual geolocation of persons in distress;
2) Best practice involves meaningful consent before using georouting;
3) Enhanced privacy and cybersecurity measures are needed to ensure secure storage, retention and rightful access to 988 texter data because of the unique sensitivity of that data; and
4) Carriers regularly argue that Section 222 of the Communications Act doesn't apply to texts, which while incorrect in this context suggests that the Bureau should articulate additional legal authorities to prevent providers evading enforcement for privacy violations.

II. Text Georouting Must Not Lead to Non-consensual Geolocation Collection.

As EPIC noted in its reply comments in the Second Further Notice of Proposed Rulemaking (2FNPRM) last year,[5] if the Bureau wants help-seekers to feel comfortable contacting 988 while in distress,[6] it should explicitly prohibit the use of geolocation data in the context of 988.[7] Only an entity like the Federal Communications Commission could implement such a safeguard, and more importantly once implemented only an entity like the FCC could remove it. This proposed prohibition should not apply to 911 providers if a 988 call is transferred

[5] *See* Reply Comment of EPIC, Second Further Notice of Proposed Rulemaking (2NPRM), WC Dkt. No. 18-336 (July 29, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10729418918342 [hereinafter "EPIC 2FNPRM Reply Comment"].
[6] Note that some help-seekers may be calling on behalf of others, and note that this could be weaponized. *See, e.g.*, Ad Council Research Institute, *988 Suicide & Crisis Lifeline Messaging and Communications to Trusted Messengers of People Disproportionately Impacted by Suicide* at 34, 38, 39-40 (May 2024), https://suicidepreventionmessaging.org/sites/default/files/2024-05/988%20FR_Trusted%20Messengers_Report_Final-508.pdf; Tara Blackwell, *How to Punish Your Least Favorite Online Influencer: Wellness Checks as Swatting and their Disproportionate Impact on Marginalized Creators*, 30 Wash. & Lee J. Civ. Rts. & Soc. Just. 291 (Fall 2023), https://scholarlycommons.law.wlu.edu/crsj/vol30/iss1/10.
[7] *See* 988 Georouting NPRM at 11145-46, https://www.federalregister.gov/d/2025-03399/p-37 (speaking to preventing chilling effects).

to 911; it should be loudly and clearly explicit to text-based help-seekers when this transfer process is about to occur and its implications for use of the help-seeker's geolocation data, with the option for the help-seeker to cancel the transfer.

While the Commission has been diligent in communicating the difference between geolocation and georouting, we believe that those most in need of 988's support would be more likely to utilize the program if there were an explicit prohibition on the use of geolocation by 988 providers, with a clear explanation of what the process for obtaining the texter's precise location entails—for example, the point at which a text is transferred to 911. This level of transparency would reassure persons in crisis that their privacy and autonomy will be respected when they contact 988. Failing to provide this transparency risks the help-seeker experiencing a "gotcha" feeling, harming the help-seeker both in the short-term and the long-term due to a non-consensual intervention, and more broadly chilling participation in the 988 program.

III. Obtaining Informed Consent Prior to Initiating Georouting is Best Practice.

We applaud the Bureau for placing an emphasis on meaningful consent[8] and suggest that CPAC's proposal of inviting but not requiring the texter to manually provide their location may be the most cost-efficient and generally efficient method for georouting.[9] Most importantly, it centers the decision about what information to provide with the help-seeker, which emphasizes

[8] *See id.* (speaking to meaningful and informed consent). *See also* Sasha Zabelski, et. al., *Crisis Lines: Current Status and Recommendations for Research and Policy*, Psychiatric Services, 74(5) at 505–512 (2022), https://doi.org/10.1176/appi.ps.20220294 ("Ethical data practice should clearly inform users, before a conversation is begun, on the ways in which their data will be handled…In addition, auditing procedures by a third party (e.g., an accrediting nonprofit body or government organization) could be established to ensure responsible handling of caller data.") (internal citations omitted).

[9] *See* Comment of CPAC Foundation Center for Regulatory Freedom, WC Dkt. No. 18-336 at 6-7 (Jan. 9, 2025), https://www.fcc.gov/ecfs/search/search-filings/filing/1010931442619 [hereinafter "CPAC Comment"].

their autonomy. Additionally, attempting to engineer a tech-based solution introduces unnecessary privacy and cybersecurity risks.[10]

Informed consent is vital to the success of 988, both in terms of help-seeker utilization and in terms of help-seeker outcomes. Early crisis hotlines were created to be a community-based model of support that gave help-seekers a space to talk openly about their reality without the fear of being institutionalized and without the threat of social or legal punishment.[11] Today, however, this has been turned on its head, with several hotlines employing policies that trigger involuntary emergency interventions resulting in unwanted and deleterious contact with law enforcement or psychiatric institutions.[12] 988 advocates and policymakers have defended this practice and as a result advocated for increased surveillance to facilitate non-consensual interventions.[13] We suspect that 988 operators are themselves aware that help-seekers want complete anonymity; secretly obtaining location data or other data that could be used to identify or interact with the help-seeker without their consent undermines this help-seeker expectation and this foundational principle of crisis hotlines. Instead, placing the choice in the help-seeker's hands—for example, by asking something like "would you like to provide your location so that we can better recommend resources and supports in your area?"—instead of automatically collecting that data preserves this key principle of meaningful, informed consent.

Inviting the help-seeker to provide their zip code also mitigates the problems of the help-seeker feeling deceived (the aforementioned "gotcha") and of scope creep inherent in automated data collection. Whereas a help-seeker may be unlikely to contact 988 again if their outreach

[10] *See id.* at 6.
[11] *See, e.g.*, TransLifeline, *The Problem with 988: How America's Largest Hotline Violates Consent, Compromises Safety, and Fails the People* at 7 (Oct. 2024), *available at* https://translifeline.org/safe-hotlines/the-problem-with-988-report/.
[12] *See id.*
[13] *See id.* at 9.

results in unwanted interventions (for example, as a result of collecting their location information and dispatching "assistance" without the help-seeker's consent), letting the help-seeker decide whether they want to provide their location information reassures the help-seeker that their autonomy is being respected. It is conceivable that this zip code information could be used for a purpose other than georouting the texter's outreach, and the Commission should implement enforceable guardrails to prevent that. But such a process would be less invasive and less costly than automated collection of location information. Additionally, while automated data collection can create living datasets that can fuel program improvement, such datasets present too great a temptation to be used for other purposes (e.g., training AI). The risk of scope creep is reduced when the texter is invited to provide their zip code data each time, as opposed to a system that automatically collects the help-seeker's location data.

Health data can be particularly attractive to malicious actors and to businesses alike.[14] The content of communications from a person in crisis can be especially valuable to bad actors due to financial incentives as in blackmail[15] or for non-financial but personally-motivated conduct akin to doxxing.[16] For example, while employers should not discriminate on the basis of

[14] *See, e.g.*, Elisa Jillson, *The DNA of privacy and the privacy of DNA*, Fed. Trade Comm'n: Bus. Blog (Jan. 5, 2024), *available at* https://web.archive.org/web/20250202104758/https://www.ftc.gov/business-guidance/blog/2024/01/dna-privacy-privacy-dna ("The more sensitive the data, the more valuable it may be to bad actors"); Shaun Callaghan et al., *Feeling good: The future of the $1.5 trillion wellness market*, McKinsey Insights (Apr. 8, 2021), https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/feeling-good-the-future-of-the-1-5-trillion-wellness-market.

[15] *See, e.g.*, Statement of Chair Lina M. Khan joined by Commissioner Alvaro M. Bedoya & Commissioner Rebecca Kelly Slaughter, *In re Mobilewalla, Inc.*, Fed. Trade Comm'n (Dec. 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/statement-khan-bedoya-slaughter-mobilewalla.pdf (noting that foreign adversaries could identify whether someone has a substance abuse problem, a gambling addiction, or major financial problems—a "torrent of blackmail data" ripe for abuse). Blackmail based on sensitive information has also occurred in the context of non-consensual intimate images. *See, e.g.*, Danielle K. Citron, *Sexual Privacy*, 128 Yale L. J. 1870, 1874–81, 1915-21 (2019), https://www.yalelawjournal.org/pdf/Citron_q8ew5jjf.pdf.

[16] *See, e.g.*, Amelia Hansford, *Mother explains how nine-year-old trans kid was 'doxxed' by vile hate forum Kiwi Farms*, PinkNews (Sept. 7, 2022), https://www.thepinknews.com/2022/09/07/kiwi-farms-harassed-nine-year-old/ ("She explained she received a Google alert notification about the information leak and described her fear of watching several cars stop in front of her house during an ice storm when her city 'was essentially shut down'.");

a person's mental health condition or even just the fact that they once utilized a crisis line, employers have conducted mental health assessments under the guise of personality assessments prior to making hiring decisions.[17] It is easy to imagine a malicious actor targeting a help-seeker for ideological reasons and exposing extremely sensitive information to their employer or social circle. Introducing a tech-based solution for georouting risks creating new vectors by which a help-seeker could be identified.[18]

As a final point, as CPAC observed, many providers who would be responsible for implementing a georouting process for texts for 988 have indicated that they are not ready and that it is premature to require it.[19] The technological infeasibility is an independent reason for the FCC to conclude that automated georouting is inadvisable at this time.

IV. The Unique Sensitivity of Texter Data Demands Enhanced Privacy and Cybersecurity Measures.

If the Commission is going to move forward with requiring georouting for texts to 988, it must establish heightened protocols to safeguard the data that will be collected. This is especially important as there are likely to be jurisdictional gaps that would frustrate attempts by federal

---

Ahmar Khan and Amy Simon, *Twitch streamer and transgender activist doxed in Northern Ireland after leaving Canada*, Global News (updated Aug. 31, 2022), https://globalnews.ca/news/9097654/twitch-streamer-and-transgender-activist-doxxed-in-northern-ireland/ ("Earlier this month, Sorrenti was at the centre of a previous swatting attack after being doxxed by harassers who sent false death threats with her name and address to London city councillors, leading to her being arrested at gunpoint.").

[17] *See, e.g.*, ACLU Rhode Island, *ACLU and CVS/pharmacy Resolve Discrimination Complaint* (July 19, 2011), https://www.riaclu.org/en/news/aclu-and-cvspharmacy-resolve-discrimination-complaint; Ifeoma Ajunwa, *The Quantified Worker* (Apr. 2023) at 129-137 (describing mental health screening tool used by employer to wrongfully deny employment); Kelly Timmons, *Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act*, Penn State Law Review: Vol. 125: 2 at 419-22 (2021), https://elibrary.law.psu.edu/pslr/vol125/iss2/2 (same).

[18] *See, e.g.*, Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The privacy bounds of human mobility*, Scientific Reports 3, 1376 (2013), https://doi.org/10.1038/srep01376 (only four points of location data needed to uniquely identify 95% of individuals); Latanya Sweeney, *k-anonymity: a model for protecting privacy*, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 557-570 (2002) (identifying the Massachusetts Governor's hospital records using only public data); Paul Ohm, *Broken promises of privacy: Responding to the surprising failure of anonymization*, UCLA L. Rev. 57, 1701 (2009).

[19] *See* CPAC Comment at 3.

regulators to correct a mishandling of help-seeker data when such a mishandling occurs.[20] These obstacles are further complicated in the context of text messaging, see Section V *infra*.

a. The Bureau Should Maintain Its Focus on the Risks of Monetization and Malicious Actors.

We are encouraged by the Bureau's thoughtfulness about the misuse of 988 data for monetization purposes or by malicious actors.[21] Setting aside the extremely sensitive contents of a communication with a crisis service, the mere fact that an individual reached out to 988 at all is likely something that person would prefer to keep private—or at least to decide when and to whom that information is disclosed.

As EPIC noted in its 2FNPRM reply comments, providers should be prohibited from sharing 988-related data even if the subscriber opted in to sharing their CPNI, and ensure providers and their vendors meet basic cybersecurity requirements.[22] Given the enhanced risks involved in written communications like text messages (which can be easily copied or forwarded, parsed by reader software, fed into an algorithm, etc.), we urge the Bureau to consider what even further elevated precautions might be appropriate. The Bureau should recommend that providers direct help-seekers to encrypted communication channels where possible, see subsection IV.c *infra*.

At a minimum, the FCC should require providers to include proper oversight of their vendors with regards to the provider's privacy and cybersecurity obligations. We also urge the

[20] *See* EPIC 2FNPRM Reply Comment at 2, 8, 11-13 (noting that not all hotlines are covered under HIPAA, that the FTC is unlikely to have jurisdiction over nonprofit entities or non-VoIP providers, and that the 988 program's affiliation with a government initiative likely further complicates accountability).
[21] *See* 988 Georouting NPRM at 11145, https://www.federalregister.gov/d/2025-03399/p-36.
[22] *See* EPIC 2FNPRM Reply Comment at 11-14. In these comments, EPIC also analogized to the explicit prohibition the FCC employed in its Safe Connections Act proceeding that protected calls to DV hotlines from being used to inform marketing programs. *See id.* (citing to *in re Supporting Survivors of Domestic and Sexual Violence, Affordable Connectivity Program, Lifeline and Link Up Reform and Modernization*, Report and Order, WC Dkt. Nos. 22-238, 21-450, 11-42, FCC 23-96 at ¶¶ 39, 46 (Rel. Nov. 16, 2023), https://www.fcc.gov/document/fcc-approves-rules-safeguard-domestic-violence-survivors-0).

Bureau to consider requiring providers to delete their records after 90 days. Crisis service providers have similar protocols, using the data for quality assurance in the short-term and then deleting it[23] to reduce the severity of harm should a data breach occur. There is no reason a service provider at any other point in the process needs to store help-seeker data longer than that.

If the Bureau decides to move forward with georouting, it should not use a system that could surreptitiously erode a help-seeker's privacy now or in the future.[24] The dither option for obscuring location data, for example,[25] runs the risk of the stripping not occurring. Longitude and latitude measurements can be quite precise depending on the number of decimal points involved.[26] County-level codes may provide adequate anonymity,[27] unless there are additional methods by which texter data might be sorted—e.g., a texter in a small county contacting a hotline focused on LGBTQ+-specific needs— in which case help-seekers might be at greater risk of being identified.[28]

b. Increasing the Number of Entities Involved Increases the Risk of Data Being Mishandled.

We note that the more entities that have access to data, the greater the risk of that data being misused. Third-party vendors are increasingly attractive targets for cyber criminals seeking unauthorized access to Americans' data.[29] As the Bureau notes, text-to-988 georouting would

[23] *See, e.g.*, TransLifeline, *Terms of Service and Privacy Policy* (updated Jan. 2025), https://translifeline.org/terms-of-service-and-privacy-policy/.
[24] *See, e.g.*, EPIC 2FNPRM Reply Comment at 14-16 (Section III).
[25] *See* 988 Georouting NPRM at 11145, https://www.federalregister.gov/d/2025-03399/p-35.
[26] *See, e.g.*, Garmin Support Center, *Accuracy of Decimal Places in Latitude and Longitude Degrees*, https://support.garmin.com/en-US/?faq=hRMBoCTy5a7HqVkxukhHd8 (last visited Apr. 3, 2025).
[27] *See* 988 Georouting NPRM at 11145, https://www.federalregister.gov/d/2025-03399/p-34.
[28] Third Report and Order and Third Further Notice of Proposed Rulemaking, WC Dkt. No. 18-336 at ¶ 35 (Rel. Oct. 18, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/101898760723 (recognizing privacy concerns); *see also* Shelby Rowe, Director, Suicide Prevention Resource Center, University of Oklahoma Health Sciences Center, 988 Geolocation Forum, https://www.youtube.com/watch?v=HjHXXPGEuus&t=11070s.
[29] *See, e.g.*, *Disrupting Data Abuse*: *Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, Comments of EPIC, FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security at 204-05 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-

likely require the involvement of more entities than voice-to-988 georouting.[30] We agree with CX360: the attractiveness of the data and the opportunities to obtain unauthorized access to that data[31] are significantly reduced by the extent to which data collection and sharing can be restricted and aggregated earlier in the process.[32] In addition to regulatory action, this should be bolstered by contractual obligations to ensure proper data processing, retention, and deletion practices by all parties that could have access to help-seeker data, including the mere fact that the help-seeker contacted 988.

c. Texters Should Be Directed to Encrypted Applications, as SMS is Notoriously Insecure.

The content of communications is one of the most sensitive types of data; this is even more salient when those communications are between a person in severe distress and crisis support services. Unfortunately, there have been numerous reasons to distrust the privacy and security of SMS (text messaging),[33] exacerbated significantly as of 2024.[34] As a result, we urge the Bureau to recommend that providers direct help-seekers to communications platforms that can reliably provide end-to-end encrypted (E2EE) communications. However, as not every help-seeker may have consistent access to data services necessary to maintain an E2EE conversation, the Bureau should implement adequate privacy safeguards for SMS-based conversations as well.

Nov2022.pdf (citing to numerous FTC enforcement actions as well as ABA Cybersecurity Legal Task Force, *Vendor Contracting Project: Cybersecurity Checklist Second Edition* 1 (2021), https://www.potteranderson.com/media/publication/941_Vendor%20Contracting%20Project%20-%20Cybersecurity%20Checklist.pdf; *Target Hackers Broke in Via HVAC Company*, Krebs on Security (Feb. 5, 2014), https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/).

[30] *See* 988 Georouting NPRM at 11145, https://www.federalregister.gov/d/2025-03399/p-31.

[31] *See* Section III *supra*.

[32] *See* 988 Georouting NPRM at 11144, https://www.federalregister.gov/d/2025-03399/p-29.

[33] *See, e.g.*, Brian Krebs, *Can We Stop Pretending SMS is Secure Now?*, KrebsonSecurity (Mar. 16, 2021), https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/.

[34] *See, e.g.*, Kevin Collier, U.S. officials urge Americans to use encrypted apps amid unprecedented cyberattack, NBC News (Dec. 3, 2024 4:01pm ET), https://www.nbcnews.com/tech/security/us-officials-urge-americans-use-encrypted-apps-cyberattack-rcna182694 (noting that officials from the FBI and CISA both recommended Americans using encrypted messaging apps to minimize the chances of China's intercepting their communications during ongoing Salt Typhoon hacking campaign).

V. The Bureau Should Anticipate Arguments That Section 222 Does Not Apply to Text Messages.

The Bureau will likely need to identify other legal authorities, and as necessary other regulators and enforcement entities, to ensure that the protections it puts in place for 988 are adhered to; service providers repeatedly argue, in different contexts, that text messages do not fall within the FCC's authority under Section 222.[35] EPIC maintains that the Commission's Section 222 authority applies beyond the scope of voice service,[36] however the stakes are too high to rely on this authority alone. We further note that this trend of challenging the agency's privacy authorities is likely to be even more aggressive in the context of encrypted messaging applications.

VI. Conclusion

We appreciate the Commission's efforts to improve our nation's emergency response system, but we urge greater emphasis on protecting the new forms of data that will power that system. We want 988 to be successful both in terms of utilization rates and in terms of actual outcomes for callers.

[35] *See, e.g.*, Br. for CTIA as Amicus Curiae Supporting Petitioner, *Verizon Communications Inc. v. FCC, et al.*, No. 24-1733 at 16-17 (2nd Cir filed Nov. 4, 2024), available at https://epic.org/wp-content/uploads/2025/01/Verizon-Br-ca2-2024-01733-00036.pdf; Defendant-Appellee's Answering Brief, *Michael Terpin v. AT&T Mobility, LLC*, No. 23-55275 at 23-24 fn.4 (9th Cir. filed Sept. 25, 2023), available at https://epic.org/wp-content/uploads/2025/01/Terpin-ATT-Reply-23-09-25-ca9-2023-55375-009034191683.pdf; Br. for CTIA as Amicus Curiae Supporting Petitioner, *Michael Terpin v. AT&T Mobility, LLC*, No. 23-55275 at 24-26 (9th Cir. filed Oct. 2, 2023), available at https://epic.org/wp-content/uploads/2025/01/Terpin-CTIA-Amicus-23-10-02.pdf.

[36] *See, e.g.*, Fed. Commc'ns Comm'n, *In re Data Breach Reporting Requirements*, Report & Order, WC Docket No. 22-21 at ¶ 15-20 (Rel. Dec. 21, 2023), https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf; Reply Comments of EPIC, et. al., *In re Data Breach Reporting Requirements*, WC Docket No. 22-21 at 11-12 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814; Reply Comments of EPIC, National Consumer Law Center, et. al., *In re Protecting Consumers from SIM-Swap and Port-Out Fraud*, WC Dkt. No. 21-341 at 6, 19-22 (Feb. 12, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10213160552872.

Respectfully submitted, April 3, 2025.

Chris Frascella
Counsel
frascella@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036