Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Advancing Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION AND THE AMERICAN CIVIL LIBERTIES UNION

Cooper Quintin
Senior Staff Technologist
Electronic Frontier Foundation
815 Eddy Street, San Francisco, CA 94109
cooperq@eff.org

Chao Jun Liu
Senior Legislative Associate
Electronic Frontier Foundation
815 Eddy Street, San Francisco, CA 94109
chao@eff.org

June 25, 2026

Comments of the Electronic Frontier Foundation and the American Civil Liberties Union on Further Notice of Proposed Rulemaking

June 25, 2026

I. Overview

The Electronic Frontier Foundation and the American Civil Liberties Union (Joint Commenters) submits these comments in response to the Federal Communications Commission's May 26, 2026, Further Notice of Proposed Rulemaking.

Joint Commenters urge the Commission to abandon its proposal to collect the personal information of every person who uses a phone service.

The Federal Trade Commission found that a significant portion of illegal robocalls stem from overseas sources.[1] The Commission itself found that "the most effective way to prevent illegal calls from reaching American consumers is by ensuring they never enter the network." [2] Collecting the identifying information of every consumer in the entire country does not address the problem.

Collecting such information will create a database of personal information of every American that would be too lucrative for cybercriminals to ignore. This is especially concerning given the telecommunication industry's proven inability to be good stewards of data, both in their proven susceptibility to cyberattacks and violation of their own privacy practices.

The Commission's approach will lead to a loss of privacy that directly harms and silences consumers, while also creating an exclusionary impact that disproportionately harms those the Commission should be serving. Anonymity in calls provides people the safety they may require to organize with others, speak freely, and seek services. Additionally, requiring data collection to have a phone number could prevent citizens from communicating with loved ones, getting a job, and feeding their families.

II. Joint Commenters Interest in This Rulemaking

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 32,000 individual dues-paying members and well over 1 million followers on social networks, we focus on promoting policies that benefit users of technology.

---

[1] *Data Show That a Significant Proportion, If Not the Majority, of Illegal Robocalls Originate From Overseas*, Federal Trade Commission (April 11, 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters.

[2] *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls and Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 17-59 and CG Docket No. 02-278, Further Notice of Proposed Rulemaking (2026), at ¶ 2, available at https://docs.fcc.gov/public/attachments/FCC-26-27A1.pdf

EFF defends freedom of speech, freedom of association, personal privacy, and personal control over privacy against threats arising from governments and the private sector.

For more than 100 years, the American Civil Liberties Union (ACLU) has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. The ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

III. Collecting Every Consumer's Information Will Not Address Unwanted or High-Volume Calls

Joint Commenters advise the Commission to abandon its proposal to collect the personal information of every person who uses a phone service.

The dubious logic of this approach is that by eliminating anonymity in phone calls and texts, it will be easier to find bad actors.

The Commission seeks to eliminate unwanted calls by requiring private entities to, "at a minimum, obtain and retain the name, physical address, government issued identification number, and alternative telephone number of any new and renewing consumer before granting access to [phone service]." [3] The Commission also expresses interest in limiting high-volume callers.[4] The Commission also seeks comments on how physical address should be defined, whether and how private entities would verify identity, data retention, scope of collection, and what concerns might arise from this collection of information.[5]

However, by the Commission's own admission, "[t]he most effective way to prevent illegal calls from reaching American consumers is by ensuring they never enter the network."[6] To this end, the Commission has implemented its STIR/SHAKEN[7] standards.[8]

Further, the Federal Trade Commission (FTC) found that "a significant proportion, if not the majority, of illegal robocalls originate from overseas." [9]

Collecting troves of information from every "new and renewing consumer" will therefore not effectively mitigate unwanted calls. Not only do everyday consumers lack the capacity, let alone

[3] *Id.* at ¶ 9
[4] *Id.* at ¶ 3, 6, 9, 13, 19.
[5] *Id.* at ¶ 10, 12, 13, 18, 24.
[6] *Id.* at ¶ 2.
[7] Secure Telephone Identity Revisited / Signature-based Handling of Asserted Information Using toKENs
[8] *Combating Spoofed Robocalls with Caller ID Authentication*, Federal Communications Commission (accessed June 14, 2026), available at https://www.fcc.gov/call-authentication
[9] *Supra* note 1.

the desire, to make unwanted or high-volume calls, the actors who do cause harm may have the capacity to circumvent any new regime[10], or perhaps might not be subject to it in the first place. In practice, then, what the Commission proposes is a data collection regime that drives highly sensitive information about American consumers into the hands of private entities with a proven track record of privacy violations[11] and data breaches,[12] without protecting them from harm.

If the Commission truly wishes to stop spam or scam calls, it should accelerate adoption of STIR/SHAKEN. While STIR/SHAKEN is not perfect, it is better than nothing. Currently less than 50% of US telecoms have fully implemented the protocol.[13] Having 100% compliance would drastically reduce the number of unwanted calls.

IV. The Telecommunications Industry Cannot Prevent Data Breaches

The telecommunications industry has proven time and again to be poor stewards of personal information. Not only have they been at the center of several large-scale data breaches in recent years, but their data practices also leave much to be desired.

In 2024, AT&T disclosed two large data breaches, one in which 7.6 million existing account holders and more than 65 million former customers had their information leaked onto the dark web[14], and another in which more than 100 million customer account call and text logs were downloaded.[15] Another large provider, Comcast, suffered a data breach in 2023 where nearly 36 million account holders' information was stolen, including the last four digits of their Social Security Numbers and date of birth.[16]

---

[10] *Synthetic Identity Fraud is a Complex and Growing Challenge*, LexisNexis Risk Solutions (Last accessed June 18, 2026), available at https://risk.lexisnexis.com/insights-resources/article/synthetic-identity-fraud

[11] *EFF Sues AT&T, Data Aggregators For Giving Bounty Hunters and Other Third Parties Access to Customers' Real-Time Locations*, Electronic Frontier Foundation (July 16, 2019), available at https://www.eff.org/press/releases/eff-sues-att-data-aggregators-giving-bounty-hunters-and-other-third-parties-access

[12] *Experts Agree U.S. Communications Networks Remain Vulnerable Following Salt Typhoon Hack*, U.S. Senate Committee on Commerce, Science, and Transportation (December 2, 2025), available at https://www.commerce.senate.gov/press/dem/release/experts-agree-u-s-communications-networks-remain-vulnerable-following-salt-typhoon-hack/

[13] *Robocall Mitigation Database from the FCC*, US. PIRG (October 16, 2025), available at https://pirg.org/edfund/resources/robocall-mitigation-database-from-the-federal-communications-commission/

[14] Natalie Campisi, *73 Million AT&T Customers' Personal Info Found on Dark Web; What Should You Do?*, Forbes (April 2, 2024), available at https://www.forbes.com/advisor/personal-finance/att-data-breach-exposes-millions/

[15] David Shepardson, *AT&T Says Data from 109 Million US Customer Accounts Illegally Downloaded*, Reuters (July 12, 2024), available at https://www.reuters.com/technology/cybersecurity/att-says-data-around-109-mln-us-customer-accounts-illegally-downloaded-2024-07-12/; see also Jen Caltrider and Zoë MacDonald, *AT&T Had a Huge Data Breach: Here's What You Need to Know,* Mozilla Foundation (July 15, 2024), available at https://www.mozillafoundation.org/en/privacynotincluded/articles/att-had-a-huge-data-breach-heres-what-you-need-to-know/

[16] Carly Page, *Comcast says hackers stole data of close to 36 million Xfinity customers,* TechCrunch (December 19, 2023), available at https://techcrunch.com/2023/12/19/comcast-xfinity-hackers-36-million-customers/; see also *Notice to Customers of Data Security Incident*, Xfinity (Accessed June 14, 2026), available at https://assets.xfinity.com/assets/dotcom/learn/-Data-Incident.pdf?langtarget=es

In addition, the 2024 Salt Typhoon attack continues to loom large.[17] Experts maintain that U.S. communications networks remain vulnerable, and even this administration acknowledges these attacks as an ongoing threat.[18]

These are not isolated incidents. As cybersecurity attacks become more frequent across industries, the continued vulnerability of telecommunications providers presents real dangers to the privacy and safety of everyday Americans. Requiring these providers to collect and retain even more information for at least four years[19] will only exacerbate the harm of unwanted calls when bad actors inevitably access these databases. Data breaches are not a matter of if, but when.

Moreover, these providers abuse the information in their possession. In *Scott v AT&T,*[20] it was found that AT&T, among others, was actively making consumer information available to hundreds of third parties without the consumer's express consent. Specifically, AT&T and two location data aggregators were allowing private entities to access a wireless customer's real-time location without authorization for as little as $300. Though the case was dismissed on other grounds, it shows the lack of care with which providers treat their customers' data.[21] Giving these providers even more data will only expose American consumers to more harms.

V. This Proposal is Rife with Privacy and Free Speech Concerns

The Commission's approach will lead to a loss of privacy that directly harms and silences consumers, while also creating an exclusionary impact that disproportionately harms those the Commission should be serving. Anonymous phone calls give people the courage to participate in politics, organize themselves, reach out to a suicide or sexual-assault hotline or addiction-recovery sponsor, seek medical care, and much more.

Because not everyone will have all the information necessary to retain service, the Commission's data collection requirement means many Americans will lose, or be unable to retain, phone service.

For example, the Commission requires collecting a person's physical address, but seeks to exclude "virtual addresses, shared office locations without a dedicated suite or floor, P.O. boxes,

---

[17] Congressional Hearing, *Signal Under Siege: Defending America's Communications Networks*, U.S. Senate Committee on Commerce, Science, and Transportation (November 21, 2025), available at https://www.commerce.senate.gov/meetings/signal-under-siege-defending-americas-communications-networks/;see also Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications*, Congressional Research Service (January 23, 2025), available at https://www.congress.gov/crs_external_products/IF/PDF/IF12798/IF12798.14.pdf

[18] Derek B. Johnson, *FBI: Threats from Salt Typhoon are 'still very much ongoing,'* Cyberscoop (February 19, 2026), available at https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026/

[19] *Supra* note 2, at ¶ 24.

[20] Complaint, *Scott v. AT&T*, No. 3-19-cv-04063 (N.D. Cal. July 16, 2019), Available at https://www.eff.org/document/scott-v-att-geolocation-complaint-0

[21] Aaron Mackey, *Forced Arbitration Thwarts Legal Challenge to AT&T's Disclosure of Customer Location Data,* Electronic Frontier Foundation (April 14, 2021), available at https://www.eff.org/deeplinks/2021/04/forced-arbitration-thwarts-legal-challenge-atts-disclosure-customer-location-data

mail forwarding services, and hosted servers" from its definition of physical address.[22] Separate from the privacy interests one may have in using a P.O. box or a mail-forwarding service, many individuals do not have stable physical addresses. This requirement would prevent unhoused individuals from having phones. This proposal would also prevent people from getting an anonymous phone line for safety reasons, such as a person in a domestic violence situation who does not have control over her personal phone line and needs to call a shelter, or a teenager being coerced by human traffickers who just wants to call for help. Put plainly this could prevent honest citizens from getting a job and feeding their families, or from escaping domestic violence, human trafficking, or other dangerous situations.

Similar logic applies to those who seek prepaid and postpaid services,[23] which are often used by people who lack the financial means for a regular phone plan, as well as by privacy conscious consumers.

The Commission seeks comment on verifying and retaining consumer information for the purposes of verifying consumer identity, which would require collecting even more information.[24] The Commission notes one potential supporting record could be "copies of government-issued identification." [25] Not everyone has government-issued identification. About 15 million adult U.S. citizens do not have a driver's license, while about 2.6 million do not have any form of government-issued photo ID.[26] Estimates show another 21 million adult U.S. citizens do not have a non-expired driver's license, and over 34.5 million adult citizens have neither a driver's license nor a state ID card with their current name or address.[27] Furthermore children who don't have ID and don't have parents who can provide an ID would be effectively shut out of all communications.

These numbers do not include non-U.S. citizens who do not have current government-issued identification, including undocumented immigrants who cannot obtain a state ID or driver's license. Black Americans and Hispanic Americans are disproportionately less likely to have current driver's licenses.[28] And 18% of Black adult Americans do not have a driver's license at all.[29] Americans with disabilities and Americans with lower annual incomes are also less likely to have a current driver's license.[30]

VI. Conclusion

[22] *Supra* note 2, at ¶ 11.
[23] *Supra* note 2, at ¶ 14.
[24] *Supra* note 2, at ¶ 18.
[25] *Supra* note 2, at ¶ 19.
[26] Jillian Andres Rothschild et al., *Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge* 2, Univ. Md. Ctr. for Democracy & Civic Engagement (Jan. 2024), https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%202023%20survey%20Key%20Results%20Jan%202024%20%281%29.pdf
[27] *Id*. at 2, 5; Michael J. Hanmer & Samuel B. Novey, *Who Lacked Photo ID in 2020?: An Exploration of the American National Election Studies* 3, Univ. Md. Ctr. for Democracy & Civic Engagement (Mar. 2023), https://www.voteriders.org/wp-content/uploads/2023/04/CDCE_VoteRiders_ANES2020Report_Spring2023.pdf
[28] *Supra* note 26, at 2.
[29] *Id.*
[30] *Id.*

Joint Commenters urge the Commission to abandon this approach. The telecommunications companies have not been responsible stewards of consumer information and requiring them to collect more consumer information is a disaster waiting to happen. The mass collection of consumers' information will not appreciably prevent unwanted calls and will create information-rich databases that will actively harm Americans, chill the speech of everyday people, and prevent many from having access to an essential service.

Respectfully submitted,

/s/ Cooper Quintin

/s/ Chao Jun Liu

/s/ Jay Stanley

/s/ Jina John