CENTER FOR DEMOCRACY & TECHNOLOGY

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

July 27, 2026

Via ECFS

To: Federal Communications Commission
Office of the Secretary
45 L Street NE
Washington, DC 20554

RE: Advancing Methods to Target and Eliminate Unlawful Robocalls

I. Introduction

The Center for Democracy & Technology (CDT)[1] and the Electronic Privacy Information Center (EPIC)[2] respectfully submit these comments in response to the Federal Communications Commission's (FCC's or the Commission's) Further Notice of Proposed Rulemaking (FNPRM) on Know Your Customer (KYC) requirements for originating voice service providers.[3]

CDT and EPIC support the Commission's efforts to combat illegal robocalls and scam traffic, which cause real harm to consumers and remain the FCC's top consumer complaint. As the Commission has stated, "[t]he most effective way to prevent illegal calls from reaching American consumers is by ensuring they never enter the network."[4] We agree, and the Commission should continue to aim for that goal. But, as the Commission has also explained in its more recent Rulemaking proposal, many voice service providers are not meeting the mitigation standards and should be "remov[ed] ... from the voice ecosystem"[5] through improved vetting and oversight standards.

[1] CDT is a nonpartisan 501(c)(3) nonprofit dedicated to advancing civil rights and civil liberties in the digital age, including protecting privacy and promoting the responsible use of data by governments and private actors. *See* Center for Democracy & Technology, *Who We Are*, https://cdt.org/who-we-are/.
[2] EPIC is a 501(c)(3) research and advocacy center whose mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. About Us, EPIC (2026), https://epic.org/about/.
[3] Federal Communications Commission, Enhancing Know-Your-Customer Requirements, Further Notice of Proposed Rulemaking, FCC 26-27, CG Docket Nos. 17-59 & 02-278 (rel. May 1, 2026), https://docs.fcc.gov/public/attachments/FCC-26-27A1.pdf [hereinafter KYC FNPRM].
[4] KYC FNPRM at 1.
[5] Federal Communications Commission, Enhancing Know-Your-Upstream-Provider Requirements and Strengthening STIR/SHAKEN, Further Notice of Proposed Rulemaking, FCC 26-32, CG Docket Nos. 17-59 & 17-97 (rel. May 20, 2026), https://docs.fcc.gov/public/attachments/FCC-26-32A1.pdf.

The Commission has posed a number of questions in the KYC notice that these comments provide responses to, but the Commission's more recent proposal recognizes that most of the solutions will be found by imposing oversight and verification obligations on providers, rather than collecting more personal data from and about individual customers. Any KYC requirements must balance consumer protection against the privacy costs they impose and should be narrowly tailored to actual risk.

The Commission's further notice on KYC requirements fails to strike that balance. It seeks comment on a potential expansion of the agency's KYC requirements to impose a government mandate to "obtain, at a minimum, the name, physical address, government-issued identification number, and an alternate telephone number of any new and renewing customer,"[6] and retain that data for four years beyond the end of the customer-carrier relationship. The Commission should not impose such a sweeping identity documentation requirement on individuals seeking access to voice services, as it would impose severe privacy harms on all phone subscribers and cut off vulnerable populations that lack these documents from an essential service that has become a lifeline for most Americans.[7] A significant loss of privacy and equitable access to communications, in exchange for a proposal with unclear and likely limited benefits, is not a tradeoff the Commission should impose on Americans, especially as low-volume individual callers are unlikely to be the source of robocalls and the entities (often located overseas) that are engaging in fraud are likely capable of producing fraudulent (or dead-end) identification records. As a result, the Commission should either significantly narrow the proposal, or close the proceeding altogether.

II. The Proposal Would Cause Serious Privacy Harm

Mandatory collection of identification documents from every phone subscriber would seriously harm anonymous access to phones, burden freedom of expression, and put every subscriber at risk. Requiring providers to obtain and retain sensitive data like government-issued identification numbers creates a vast new target for bad actors who have repeatedly targeted this industry and places even more private data in the hands of companies that have undermined consumer trust in their ability to hold data securely.

A. Harms to Anonymity and Protected Communications

Data minimization is the best way to protect privacy.[8] Yet, the Commission's proposed mandatory identity collection requirements would impose a significant and unreasonable

---

[6] KYC FNPRM at 4.

[7] The Pew Research Center reports that 98% of Americans now own a cellphone of some kind, and approximately 91% own a smartphone. Pew Research Center, Mobile Fact Sheet (Nov. 20, 2025), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[8] Eric Null, Statement Before the California Privacy Protection Agency on Data Minimization and Use Limitations (May 5, 2022), https://cdt.org/wp-content/uploads/2022/05/CA-Testimony-Eric-Null-Data-Minimization-Letterhead.pdf.

expansion of existing know-your-customer requirements. At base, this proposal presents a serious privacy violation: customers would now be subject to expanded, and likely unnecessary and ineffective, data collection and retention. Such mandates would open up opportunities for bad actors to access, misuse, or exploit that information through, for instance, data breaches, unauthorized access, or law enforcement overreach.

One of the most severe outcomes of increasing privacy risks for all phone subscribers would be endangering anonymous communications for the individuals who need it most, such as whistleblowers, activists, journalists, and domestic violence survivors. For people in situations where their safety is at risk, anonymous access to a phone can be life saving. And where a system forces people to identify themselves, to the carrier or an abuser or anyone else, those individuals will be deterred from taking protective safety measures like seeking a phone. These populations have clear and obvious reasons to require anonymity: a domestic violence survivor fleeing an abuser should not be forced to create a record that leads back to her address in order to get a phone, a whistleblower may not want their identity tied to their alternative phone number, and a trafficking survivor's safety may depend on keeping their location and identity out of any database their exploiters could reach. As the National Network to End Domestic Violence (NNEDV) observed, for survivors of abuse, "access to a phone is often access to safety itself" — the means by which a survivor reaches a victim service provider, secures emergency housing, communicates with an attorney, or contacts emergency services.[9] This logic applies to many other people seeking safe communications.

For decades, the Commission has been charged with protecting the privacy of customer information through its telecom privacy provisions and through laws like the Safe Connections Act (SCA), designed to protect victims of domestic violence. Pursuant to the SCA, the Commission has spent significant effort building safeguards to prevent carrier-held information from reaching abusers. The SCA rulemaking required carriers to redact calls and texts to domestic violence hotlines from consumer-facing bills and to keep line separations confidential, precisely because the Commission recognized that information in carrier hands can endanger survivors.[10] The know-your-customer proposal moves in the opposite direction. It would expand the private information carriers collect and retain from all subscribers, including survivors, when in reality the best way to protect them is not to force them to identify themselves unnecessarily to the carrier or otherwise.

Were this proposal to pass, individuals that previously relied on anonymous access to a phone would have to decide whether to accept the new privacy trade-off. The additional data collection,

[9] Comments of the National Network to End Domestic Violence (NNEDV), CG Docket Nos. 17-59 & 02-278, at 2 (filed June 2026), https://www.fcc.gov/ecfs/document/26109882043/1 [hereinafter NNEDV Comments].

[10] Supporting Survivors of Domestic and Sexual Violence; Lifeline and Link Up Reform Modernization, Report and Order, FCC 23-96 (Nov. 15, 2023), https://docs.fcc.gov/public/attachments/FCC-23-96A1.pdf. *See also* Safe Connections Act of 2022, Pub. L. No. 117-223, 136 Stat. 2280 (codified at 47 U.S.C. § 345).

combined with the possibility of breach, unauthorized access, civil subpoena, or law enforcement demand, may be sufficient to deter individuals from obtaining phone service at all, placing them in further danger.[11]

B. Phone Companies Have a Lackluster History with Protecting Private Data

The more data phone companies have, the more likely that data is breached, accessed, or otherwise used in harmful ways. Phone companies' track record with data is lackluster and inspires little faith that this additional data will be protected sufficiently. Phone companies have business incentives to exploit their data. We saw this explicitly when all four major wireless carriers sold customer location data to data brokers without consent, as required by law, ultimately reaching third parties like bounty hunters and bail bondsmen.[12] For that behavior, the FCC fined T-Mobile, AT&T, Verizon, and Sprint nearly $200 million.[13]

Phone company data is also frequently subject to unauthorized access, particularly given the amount of data and how useful that data is for fraud purposes. Major carriers have suffered repeated large-scale data breaches. In 2021, a T-Mobile breach exposed the Social Security numbers and driver's license numbers of approximately 77 million people.[14] In 2024, AT&T disclosed two separate breaches affecting over 100 million current and former customers. The second exposed the call and text message records of nearly all AT&T wireless customers, roughly 110 million subscribers, stored on a cloud platform protected only by a username and password with no multi-factor authentication.[15] The Salt Typhoon attack further demonstrated that U.S. communications networks remain vulnerable to state-sponsored intrusion, with experts

[11] Comments of the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU), CG Docket Nos. 17-59 & 02-278, at 5–6 (filed June 2026), https://www.fcc.gov/ecfs/document/26109924593/1 [hereinafter EFF/ACLU Comments].

[12] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Vice (Jan. 8, 2019), https://www.vice.com/en/article/i-gave-a-bounty-hunter-300-then-he-located-our-phone/.

[13] Press Release, Federal Communications Commission, FCC Fines Largest Wireless Carriers for Sharing Customers' Real-Time Location Data (Apr. 29, 2024), https://www.fcc.gov/document/fcc-fines-largest-wireless-carriers-sharing-location-data.

[14] T-Mobile, *Shares Updated Information Regarding Ongoing Investigation into Cyberattack* (Aug. 20, 2021), https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation; *see also In re* T-Mobile Customer Data Security Breach Litigation, No. 4:21-md-03019 (W.D. Mo.) ($350 million class action settlement).

[15] David Shepardson, *AT&T Says Data from 109 Million US Customer Accounts Illegally Downloaded*, Reuters (July 12, 2024), https://www.reuters.com/technology/cybersecurity/att-says-data-around-109-mln-us-customer-accounts-illegally-downloaded-2024-07-12/.

confirming that these threats are ongoing.[16] Requiring these same companies to collect more identifiable customer data would place their customers at even more unnecessary risk.

These examples cover only the largest, best-resourced carriers. The Commission's notice itself identifies over 4,000 small wired carriers and nearly 500 small wireless carriers that would be subject to the proposed requirements,[17] many that may have far less security infrastructure than the major carriers that already failed to protect customer data. Mandating that thousands of originating providers, including small carriers with limited resources, collect and retain government-issued identification numbers creates significant new exposure. The existence of these severe risks should caution the Commission from mandating expanded data collection.

The proposed retention requirements make this even more concerning. The Commission is proposing that providers retain KYC data for the entirety of any applicable statute of limitation period following termination of the customer relationship. That would mean that government-issued identification numbers, physical addresses, and other personal information about millions of subscribers will be sitting in databases across thousands of voice providers for years even after they have terminated their services. If the Commission is going to mandate retention at all, it should scope it to high-volume or high-risk customers, not every person with a phone.

III. Many Americans Lack Identifying Documentation Sufficient to Satisfy the Proposal, and Therefore the Proposal Would Exclude Vulnerable Populations from Phone Service

The Commission has requested comment on what privacy concerns may arise from expanded requirements to collect personally identifiable information and how they can be mitigated. In addition to the significant privacy harms that would be imposed by a broad KYC requirement for voice customers, it would pose unique risks to the most at-risk populations. The Commission's proposal would effectively condition access to phone service on possession of documentation that a significant portion of the American population lacks.[18] The result would be to cut off from an essential service the very populations the Commission's consumer protection mission is meant to serve.

---

[16] Press Release, U.S. Senate Committee on Commerce, Science, and Transportation, Experts Agree U.S. Communications Networks Remain Vulnerable Following Salt Typhoon Hack (Dec. 2, 2025), https://www.commerce.senate.gov/press/dem/release/experts-agree-u-s-communications-networks-remain-vulnerable-following-salt-typhoon-hack/; Derek B. Johnson, *FBI: Threats from Salt Typhoon Are 'Still Very Much Ongoing,'* Cyberscoop (Feb. 19, 2026).
[17] KYC FNPRM at Table 1; Table 2.
[18] Brennan Center for Justice, *Millions of Americans Don't Have Documents Proving Their Citizenship Readily Available*, https://www.brennancenter.org/our-work/analysis-opinion/millions-americans-dont-have-documents-proving-their-citizenship-readily.

Low-income Americans disproportionately rely on prepaid service, which currently offers a lower barrier to access than postpaid plans.[19] Imposing identity verification requirements on prepaid purchases would burden the populations least able to comply, for the type of service they most depend on.

Others most likely to have difficulty providing the required identifiers include unhoused individuals, who may lack both a physical address and government-issued ID; older adults, whose identity records may predate digital systems or contain outdated information; foster youth aging out of the system, who frequently lack standard documentation; survivors of intimate partner violence and commercial sexual exploitation, who may be unable to safely provide a home address or whose documents may be controlled by an abuser; and undocumented immigrants, who may be unable to obtain government-issued identification.

Indeed, nearly 29 million voting-age U.S. citizens lack a valid driver's license, and over 7 million lack any form of non-expired government-issued photo identification, with citizens of color almost four times more likely than white citizens to lack current government-issued photo ID.[20] People with disabilities are also less likely to have a valid driver's license than people without disabilities.[21] And as the Electronic Frontier Foundation has noted, children who lack ID and whose parents cannot provide one could also be effectively shut out of all communications if their household can no longer access a wireless line,[22] exacerbating the digital divide.[23]

The FNPRM asks whether the Commission should exclude virtual addresses, P.O. boxes, and mail forwarding services from the definition of "physical address" because bad actors use them to conceal their identity.[24] But these are also the address options relied upon by people experiencing housing instability, people fleeing domestic violence who cannot safely disclose a home address, and people in rural areas whose physical location does not correspond to a conventional deliverable address.

As the NNEDV noted, survivors often rely on state-administered address confidentiality programs that provide substitute addresses precisely because disclosure of a residential

---

[19] Pew Research Center, *supra* note 7.
[20] University of Maryland Center for Democracy and Civic Engagement & VoteRiders, Analysis of American National Election Studies 2020 Time-Series Study (2024), https://cdce.umd.edu/news/news-umd-analysis-millions-americans-don%E2%80%99t-have-id-required-vote.
[21] American Association of People with Disabilities, *Transportation*, https://www.aapd.com/transportation/.
[22] EFF/ACLU Comments, *supra* note 11.
[23] Digitunity, *The United States' Computer Ownership Gap Persists* (Sept. 25, 2025), https://digitunity.org/the-united-states-computer-ownership-gap-persists/ (analyzing U.S. Census Bureau 2024 American Community Survey data finding that 17.7 million U.S. households lack a large-screen computer or rely solely on a smartphone for internet access).
[24] FNPRM at 5.

address can expose them to renewed violence.[25] They are also more likely to use non-physical addresses, like P.O. boxes, to protect their privacy.[26] In addition, people with disabilities would also likely be disproportionately affected by this proposed requirement.[27] Research has shown that disabled women experience intimate partner violence at a rate that is 40% higher than non-disabled women, and both women and men with disabilities are more likely to experience stalking.[28] The FNPRM would treat the very mechanisms designed to protect survivors as indicators of fraud and prevent survivors from accessing phone service.

Requiring an alternate telephone number as a condition of service assumes that every prospective customer already has a phone. Per the National Center for Health Statistics, as of 2024, 78% of Americans lived in a household that was wireless only, meaning most Americans do not have a landline, and only 4.5% used both landlines and wireless phones.[29] The overall share of people living alone has also increased, with one-person households making up 27.6% of all households in the U.S.[30] It stands to reason that most households have only one phone number; for someone purchasing their first or only phone line, this requirement is impossible to satisfy.

The proposal effectively prevents these populations from accessing phones, even as they are highly unlikely to be the source of the illegal robocall problem.

IV. The Commission Has Not Established That Universal Collection Is Necessary or Effective

In balancing privacy and effective robocall identification, the Commission has sorely missed the mark. The key question is not whether additional identity information could ever be useful, but whether identity uncertainty is the problem most in need of solving. In fact, past enforcement actions and the Commission's own evidentiary record has not established that collection of government ID numbers, physical addresses, alternate phone numbers, and similar identifiers will result in any significant effect.

---

[25] NNEDV Comments at 3–4. *See also* Financial Crimes Enforcement Network, Customer Identification Program Rule — Address Confidentiality Programs, FIN-2009-R003 (Jan. 12, 2010), https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/customer-identification-program-rule-address.

[26] *Id.*

[27] KYC mechanisms can also pose accessibility concerns to people with disabilities. See: Comments of Accessibility Organizations, CG Docket Nos. 17-59 & 02-278 (filed June 2026), https://www.fcc.gov/ecfs/document/26109927828/1.

[28] Sanctuary for Families, *Disability and Domestic Violence*, https://sanctuaryforfamilies.org/disability-domestic-violence/.

[29] National Center for Health Statistics, NHIS Early Release: Wireless Phone Use (2025), https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless202506.pdf.

[30] U.S. Census Bureau, *Home Alone: More Than a Quarter of All Households Have One Person* (June 8, 2023),https://www.census.gov/library/stories/2023/06/more-than-a-quarter-all-households-have-one-person.html.

The Commission has sought comment on its views that the collection of customer identification information by originating providers will be beneficial in deterring scammers and facilitating their identification by enforcement authorities. But there is no evidence that either of those benefits would flow from the specific KYC requirements proposed. Indeed, any entity that is already engaging in frauds and scams is likely capable of producing fraudulent (or dead-end) identification records,[31] and certainly can't be expected to provide accurate information that will enable enforcement authorities to track them down.

For instance, the Federal Trade Commission (FTC) has found that "a significant proportion, if not the majority, of illegal robocalls originate from overseas."[32] Collecting identity documents from hundreds of millions of domestic subscribers would not impact foreign actors. Even for domestically originated illegal calls, the Department of Justice has documented that the most harmful scam operations rely on foreign intermediaries and VoIP providers to access U.S. communications networks.[33]

The FTC's enforcement record overwhelmingly targets VoIP service providers and gateway carriers facilitating calls from overseas, not individual retail subscribers.[34] In the FCC's largest robocall case, they stated that operators used "a multitude of shell companies, aliases and fly-by-night phone providers" to place more than five billion illegal calls over three months, using stolen identities and facially valid credentials that likely would have satisfied the proposed verification requirements.[35] These enforcement actions demonstrate that the actors causing the most harm are precisely the ones best positioned to circumvent domestic identification requirements.

Even setting aside the overseas origination problem, the Commission has other tools at its disposal that it has not fully deployed. STIR/SHAKEN, the call authentication framework the Commission has already adopted, has been fully implemented by less than half of U.S. telecom

---

[31] Financial Crimes Enforcement Network, FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FIN-2024-Alert004 (Nov. 13, 2024), https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.
[32] Federal Trade Commission, FTC Ramps Up Fight to Close the Door on Illegal Robocalls Originating from Overseas Scammers and Imposters (Apr. 11, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters.
[33] U.S. Department of Justice et al., Announcement of Results of Nationwide Initiative to Curtail Illegal Telemarketing Operations (July 18, 2023), https://www.justice.gov/archives/opa/pr/us-department-justice-federal-trade-commission-federal-communications-commission-and-other.
[34] See *supra* note 33; Federal Trade Commission, Operation Stop Scam Calls (July 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-law-enforcers-nationwide-announce-enforcement-sweep-stem-tide-illegal-telemarketing-calls-us.
[35] Brian Fung, *FCC Issues Historic $300 Million Fine Against the Largest Robocall Scam It Has Ever Investigated*, CNN (Aug. 4, 2023), https://www.cnn.com/2023/08/04/tech/fcc-robocall-scam-biggest-fine/index.html.

companies.[36] Full deployment would provide a less privacy-invasive means of authenticating calls across the network instead of mandating universal identity collection whose efficacy remains unproven.

The FNPRM specifically seeks comment on "risk-based differences" and on "differences based on prepaid and postpaid service."[37] Risk thresholds should be defined with specificity and grounded in evidence; vague standards invite both over-inclusion of legitimate users and gaming by sophisticated actors.[38] Given the enforcement record described above, the Commission should draw the obvious conclusion: individual, low-volume subscribers are not a meaningful source of illegal robocall traffic and should not be subject to expanded identity collection requirements.[39] Any risk thresholds the Commission adopts should be defined with specificity and grounded in evidence.

V. If the Commission Proceeds, It Should Adopt Safeguards

Should the Commission determine that some expansion of KYC requirements is warranted, it should adopt safeguards to limit the privacy and access harms we have identified. Heightened KYC requirements should be limited to those callers most likely to originate robocalls with a focus on indicators of robocall operations,[40] like high-volume callers, buying numbers in bulk, and foreign-based customers.[41] Individual prepaid and postpaid customers should not be subject to these requirements.

That data should be subject to further privacy requirements. Specifically, the data should be kept confidential and encrypted when possible. The data should be minimized to ensure only the necessary data is collected. It should also not be used for any purpose other than fraud and not allowed to be sold or otherwise transferred to data brokers or other third parties. Retention of any data should be limited to the shortest period demonstrably necessary, and accompanied by binding security obligations. The data also should not be disclosed to law enforcement without appropriate legal process.

VI. Conclusion

---

[36] U.S. PIRG Education Fund, *Robocall Mitigation Database from the FCC* (Oct. 16, 2025), https://pirg.org/edfund/resources/robocall-mitigation-database-from-the-federal-communications-commission/.
[37] KYC FNPRM at 5-6.
[38] EPIC, Comments on VoIP Robocall Response and Access to Numbering System, https://epic.org/documents/voip-robocall-response-access-to-numbering-system/.
[39] Statement of Commissioner Anna M. Gomez, Re: Call Authentication Trust Anchor; Advanced Methods to Target and Eliminate Unlawful Robocalls, Further Notice of Proposed Rulemaking, WC Docket No. 17-97; CG Docket No. 17-59 (May 20, 2026), https://docs.fcc.gov/public/attachments/FCC-26-32A3.pdf.
[40] David Frankel, *Myth-Busting Call Blocking*, Legal Calls Only (Sept. 17, 2021), https://legalcallsonly.org/myth-busting-call-blocking/.
[41] *See supra* note 33.

Reducing illegal robocalls is an important goal, and CDT and EPIC support the Commission's efforts to use its authorities effectively. But the proposal as written would impose severe privacy costs on every phone subscriber in the country, exclude vulnerable populations from phone service, and be unlikely to meaningfully reduce illegal calls given how easily the proposed requirements can be circumvented by the actors causing the most harm. We urge the Commission to either significantly narrow this proposal or close this proceeding altogether.

Respectfully submitted,

/s/ Sydney Saubestre
Senior Policy Analyst
Center for Democracy and Technology (CDT)

/s/ Alan Butler
Executive Director
Electronic Privacy Information Center (EPIC)