epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL COMMUNICATIONS COMMISSION

Refreshed Record on Advanced Methods to Target and Eliminate Unlawful Robocalls

CG Docket No. 17-59

September 24, 2018

---

By notice published August 10, 2018 the Federal Communications Commission ("FCC") requests comments on a refreshed record regarding the FCC's rules to block calls that are reasonably likely to be illegal based on objective criteria.[1] The rules authorize telephone service providers to block defined categories of calls highly likely to be illegal.

Pursuant to the agency's request, the Electronic Privacy Information Center ("EPIC") submits these comments to highlight the substantial harms to consumers caused by unlawful robocalls and underscore privacy concerns that should be considered in the agency rulemaking. In these comments, EPIC recommends that the FCC (1) require phone providers to proactively block calls from numbers that are unassigned, unallocated, or invalid; (2) prohibit spoofing if there is an intent to defraud or cause harm; and (3) encourage the use of call authentication technology that safeguards caller anonymity.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment,

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd. 9706 (2017).

and constitutional values.[2] EPIC works to protect consumer privacy and has played a leading role in defending consumer privacy interests at the FCC for almost twenty years. EPIC also played a key role in the creation of the Telephone Consumer Protection Act ("TCPA") and continues to defend the Act,[3] which is one of the most important and popular privacy laws in the history of the United States.[4] EPIC provided numerous comments to both the FCC and the Federal Trade Commission ("FTC") on the implementation of the TCPA, and maintains online resources for consumers who seek to protect their rights under the TCPA.[5]

## I. Illegal and Unwanted Robocalls Cause Substantial Consumer Harm

Robocalls are a consistent source of annoyance and harm for American consumers, and are the vehicle through which bad actors engage in identity theft, financial fraud, and debt collection scams. Robocalls are consistently one of the top complaints made to both the FCC and the Federal Trade Commission ("FTC").[6] The FTC has brought more than a hundred lawsuits against individuals responsible for illegal robocalls and for "Do Not Call" violations.[7]

---

[2] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.

[3] *See, e.g.*, Telephone Advertising and Consumer Rights Act, H.R. 1304, Before the Subcomm. on Telecomms. And Fin. of the H. Comm. on Energy and Commerce, 102d Cong., 1st Sess. 43 (April 24, 1991) (testimony of CPSR Washington Office director Marc Rotenberg), https://www.c-span.org/video/?18726-1/telephone-solicitation; Brief of *Amici Curiae* Electronic Privacy Information Center (EPIC) and Six Consumer Privacy Organizations in Support of Respondents, *ACA Int'l v. FCC*, No. 15-1211 (D.C. Cir. Jan. 22, 2016), https://epic.org/amicus/acaintl/EPIC-Amicus.pdf; National Consumer Law Center et al., Petition for Reconsideration of Declaratory Ruling and Request for Stay Pending Reconsideration In the Matter of Broadnet Teleservices LLC Petition for Declaratory Ruling, CG Docket No. 02-278 (2016).

[4] Justice Brandeis described privacy as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[5] *See, e.g*, EPIC, EPIC Administrative Procedure Act (APA) Comments, https://epic.org/apa/comments/; EPIC, Telemarketing and the Telephone Consumer Protection Act (TCPA), https://epic.org/privacy/telemarketing/.

[6] *Consumer Complaint Center*, FCC, https://consumercomplaints.fcc.gov/hc/en-us/articles/115002234203-Unwanted-Calls; *FTC Releases Annual Summary of Consumer Complaints*, FTC, Mar. 3 2017, https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints.

[7] *Consumer Information: Robocalls*, FTC, https://www.consumer.ftc.gov/features/feature-0025-robocalls.

Robocall scams often have dire financial consequences for consumers. For example, a long running IRS robocall scam has cost Americans over $300 million over several years;[8] another scam in which a robot asks "Can you hear me?" prompting the recipient to say "yes" has been used to authorize fraudulent charges from credit cards stored on utility accounts;[9] and another promised to help individuals reduce their debt load while opening new credit card accounts in their name. Adding to the problems caused by these scams, individuals engaging in this illegal behavior are outside of the United States and are using cheap, readily available technology to target unwitting Americans.

Despite the success of the TCPA, consumers continue to be plagued by unwanted robocalls and text messages. The transition from land lines to mobile phones[10] has only made the problem worse. Unsolicited calls and texts facilitate fraud, drain battery life, eat into data plans and phone memory space, and interrupt consumers' daily routines. Because we carry our phones with us everywhere,[11] unwanted calls and texts interrupt our sleep, disturb meetings and meals, and disrupt the most important (or mundane) moments in our lives. We are no longer concerned solely with being interrupted by an unwanted telemarketing call during the dinner hour. For low-income consumers who often rely on pay-as-you-go, limited-minute prepaid wireless plans,[12] these

[8]Helaine Olen, *The Feds Raided the Scammers behind Those Fake IRS Robocalls. It's Not Enough.*, Slate, (Oct. 28, 2016), http://www.slate.com/blogs/moneybox/2016/10/28/the_feds_busted_the_fake_irs_robocall_scam_it_s_not_enough.html.

[9] Mike Snider, *Don't Say 'Yes' When Robocall Scam Rings*, USA Today, Mar. 27, 2017, https://www.usatoday.com/story/tech/talkingtech/2017/03/27/dont-say-yes-when-robocall-scam-rings/99709634/.

[10] 95% of American adults own at least one cell phone and 77% own smartphones. *Mobile Fact Sheet*, Pew Research Ctr. (Jan. 12, 2017) http://www.pewinternet.org/fact-sheet/mobile/; Over half of American households do not have a land line. Stephen J. Blumberg & Julian V. Luke, Ctrs. for Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2016*, at 2 (May 2017), https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201705.pdf.

[11] More than 70% of smartphone users keep their phones within five feet a majority of the time. Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf.

[12] Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless*, Eighteenth Report, WT Docket No. 15-125, ¶¶ 44, 73, 95-96 (Dec. 23, 2015).

unwanted calls and texts are particularly harmful.[13] These calls are especially harmful to the elderly because they are a frequent target of financial scams and may be unable to tell that they are being taken advantage of, or unlikely to report that a crime has occurred.[14]

Current laws and penalties for illegal robocalls have not been enough to stop these calls that plague consumers year after year. There are additional technical safeguards that can ensure that illegal calls are blocked at the outset. While consumers now have more options to block calls from their home and cell phones, they can only do so after they have received and flagged unlawful calls. The FCC should ensure that providers are more proactive in preventing abusive calls.

## II. EPIC's Recommendations on the Refreshed Record

EPIC is in favor of rules that would (1) require phone providers to proactively block calls from numbers that are unassigned, unallocated, or invalid; (2) prohibit spoofing to the extent it involves an intent to defraud or cause harm; and (3) encourage the effective use of call authentication technology while safeguarding important privacy interests for anonymous callers.

### *a. Proactive Blocking of Invalid and Unauthorized Numbers*

Proactive blocking of calls from invalid numbers is the most effective way to protect consumers. If providers wait until complaints pile up, consumer will be exposed to calls that are predatory and fraudulent. Some consumers choose not to answer calls from numbers that they suspect are invalid based on caller ID information. But other consumers may not have or use caller

[13] Bill Moack, *Feds, Fla. Shut Down Robocall Ring That Targeted Seniors,* Clarion Ledger Jun. 9, 2017, http://www.clarionledger.com/story/business/2017/06/09/feds-fla-authorities-shut-down-robocall-ring-targeted-seniors/371452001/.

[14] *Fraud Against Seniors,* Federal Bureau of Investigation, https://www.fbi.gov/scams-and-safety/common-fraud-schemes/seniors; Anne-Marie Botek, *Robocalls and Fear Tactics Help Scammers Swindle Seniors,* Aging Care, https://www.agingcare.com/articles/robocalls-fear-tactics-scam-seniors-167323.htm.

ID and, upon answering the phone, may have no way to know that the call they are receiving is likely an illegal robocall. Even worse, scammers are known to mimic numbers associated with legitimate entities (even when those numbers are never used to make calls).[15]

Phone providers should take the proactive step of blocking calls from invalid numbers. No reasonable consumer wants to receive calls from an unassigned, unallocated, or invalid number. Robocalls are consistently the number one complaint at both the FTC[16] and the FCC. Requiring that consumers "opt-in" to the blocking of the most abusive calls would leave individuals, and particularly seniors, at risk of identity theft, fraud, and harassment by phone scammers.

*b. Focus Regulation on Malicious Spoofing*

EPIC supports the FCC's recommendations to protect callers who choose to keep their caller information private. To protect caller information, spoofing rules should contain an intent requirement—"intent to defraud or cause harm." This language would cover the problem of pretexting, where bad actors use the number of a trusted entity, such as a bank or government agency, to fool people into giving the caller personal information. But it would also preserve legitimate uses of spoofing where callers wish to withhold their phone number, including calls to drug treatment services, suicide prevention, domestic abuse, and crime tip lines. The default for disclosure of identity should be in control of the non-commercial callers. Imposing a spoofing regulation without this intent requirement could hurt the privacy interests of callers.

[15] *See, e.g.*, Internal Revenue Serv., *Tax Scams/Consumer Alerts* (2018), https://www.irs.gov/newsroom/tax-scamsconsumer-alerts (warning that scammers "may know a lot about their targets" and "usually alter the caller ID to make it look like the IRS is calling").
[16] *FTC Releases Annual Summary of Consumer Complaints*, FTC, Mar. 3, 2017, https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints

*c. Call Authentication Technologies*

EPIC urges the FCC to ensure that authentication technologies safeguard the privacy of legitimate callers who remain anonymous. While certain authentication technologies, such as SHAKEN/STIR,[17] pinpoint illegal robocalls, call verification procedures can also undermine the privacy of legitimate callers who do not want to be identified. The FCC acknowledged last year that SHAKEN/STIR can authenticate calls without providing the recipient with the caller's ID.[18] This feature is essential to protecting the privacy of callers who do not wish to reveal their identity and should be mandatory. Before approving a rule that requires widespread implementation of SHAKEN/STIR, the FCC should also verify that each step of the authentication process is supported with strong data security mechanisms to protect anonymous callers.[19] Specifically, the FCC should determine:

1. Whether SHAKEN/STIR can successfully strip call identifying information from a call while authenticating its source.
2. Whether there are efficient oversight mechanisms to ensure that service providers and other parties involved in the authentication process securely protect any data that is used to authenticate the call.
3. Whether service providers and others involved in the authentication process will retain in stored databases any personal data. If so, the FCC should require strong security measures to ensure that such data is protected.

**Conclusion**

EPIC supports the Commission's action to refresh the record on targeting and eliminating unlawful robocalls. To this end, EPIC requests that the FCC take special consideration of the privacy implications discussed above.

---

[17] *See* TransNexus, *Understanding STIR/SHAKEN* (2018), https://transnexus.com/whitepapers/understanding-stir-shaken/ (describing the proposed public/private key system for verifying the source of a call).
[18] Fed. Comm'ns Comm'n, Call Authentication Trust Anchor, Notice of Inquiry (July 14, 2017) at ¶ 43, available at https://ecfsapi.fcc.gov/file/07141096201120/FCC-17-89A1.pdf.
[19] *Id*. at 42, fn. 67. (The FCC's Notice of Inquiry indicated that certain middleware authentication technologies like PASSporT can leak identifying information "outside of a trusted domain" without effective security safeguards).

Respectfully Submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Consumer Protection Counsel

/s/ *Alan Butler*
Alan Butler
EPIC Senior Counsel

/s/ *Spencer K. Beall*
Spencer K. Beall
EPIC Administrative Law Fellow