

REPLY COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL COMMUNICATIONS COMMISSION

Advanced Methods to Target and Eliminate Unlawful Robocalls

CG Docket No. 17-59 FCC 17-24

July 31, 2017

---

By notice published May 17, 2017 the Federal Communications Commission requests comments on a proposed rule to block calls that are reasonably likely to be illegal based on objective criteria.<sup>1</sup> The rule would allow phone providers to block calls from numbers they know to be unassigned, invalid, or not allocated to any provider. The Electronic Privacy Information Center (“EPIC”) submits these comments to (1) urge that blocking of numbers that cannot be valid occur as soon as possible; (2) address concerns about not obtaining consumer consent before engaging in the proposed form of call blocking and (3) emphasize the need for security in any database or list of blocked numbers that may be created.

**Numbers That Cannot Be Valid Should Be Blocked Immediately**

Some commenters expressed concerns that the proposed blocking of numbers that have been allocated but not assigned and international numbers could result in legitimate calls being

---

<sup>1</sup> *Advanced Methods To Target and Eliminate Unlawful Robocalls*, 82 Fed. Reg. 22,625 (May 17, 2017).

blocked.<sup>2</sup> While EPIC understands the concerns that these comments raised, we again wish to underscore the need for the FCC to take action on these illegal robocalls as quickly as possible. If there is concern about potentially valid numbers being blocked then the FCC should explore this problem further, perhaps through a separate rulemaking or working with consumers and service providers to develop a method for eliminating robocalls from valid numbers.

While there may be concern that valid but unassigned numbers could potentially be legitimate calls, other categories of numbers cannot possibly be valid. Numbers that subscribers know have not been allocated or unassigned and numbers purporting to be from North America but do not comply with the North American Numbering Plan cannot possibly be from legitimate callers. There is no legitimate or legal purpose that can be served by allowing these calls to continue. Should the Commission choose not to block calls from allocated but unassigned numbers it should continue implement its proposal to block numbers that are invalid or that a subscriber knows have not yet been allocated or assigned to a subscriber.

### **Obtaining Consumer Consent for Blocked Numbers Is Not Necessary**

EPIC agrees with the majority of commenter's who believe that the Commission does not need to obtain consumer consent from numbers that cannot possibly be valid. While some commenters believe that consent is necessary before any blocking occurs,<sup>3</sup> EPIC reiterates that such consent will be burdensome, time consuming, and will ultimately allow more time for scammers to prey on individuals.

---

<sup>2</sup> See e.g. Comments of Microsoft Corporation, *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, 12, Jul. 3, 2017, <https://ecfsapi.fcc.gov/file/10703558104752/Microsoft%20Robocalling%20Comments%20-%20filed%203%20July%202017.pdf> [hereafter "Microsoft Comments"]; Comments of the USTelecom Association, *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, 11, Jul. 3, 2017, <https://ecfsapi.fcc.gov/file/10703149098952/USTelecom-Blocking-Comments-2016-07-03-FINAL.pdf>.

<sup>3</sup> Microsoft Comments at 10-11.

The FCC has proposed to block numbers that no individual or business would use to actually make contact with people. Furthermore, EPIC and many other commenters noted the immense harm that occurs every year due to illegal robocalls.<sup>4</sup> While there are many cases where consumer consent should be necessary before engaging in a widespread program it is not necessary in this instance. Consumers have made it clear that they find the behavior of these robocalls to be annoying and harmful.<sup>5</sup> Engaging in a widespread effort to obtain consent from millions of people would be time consuming and may not result in successfully contacting and receiving responses from individuals. Furthermore, during this period of attempting to obtain consent, individuals would be at risk of identity theft, fraud, and harassment by phone scammers. This is a unique situation where the harms of illegal robocall activity have been documented and there is universal consensus that people do not want to receive these calls and want them to stop. As such, obtaining individual consent for the blocking of numbers that cannot possibly be valid and where there is ample evidence that individuals do not want to receive these calls is not necessary.

### **Strong Security Measures Are Necessary for Any Database of Blocked Numbers**

EPIC has long been an advocate for strong security measures to protect personal information stored in databases.<sup>6</sup> Furthermore, government databases have proved to be

---

<sup>4</sup>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>; *Consumer Information: Robocalls*, FTC, <https://www.consumer.ftc.gov/features/feature-0025-robocalls>; 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/>; *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>.

<sup>5</sup> *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>.

<sup>6</sup> See e.g., Comments of EPIC, *Privacy Act of 1974; Department of Homeland Security/ALL—038 Insider Threat Program System of Records*, Mar. 28, 2016, <https://epic.org/apa/comments/EPIC-DHS-Inisder-Threat-Comments.pdf>; Comments of EPIC, *Department of Defense (DoD) Insider Threat Management and Analysis Center*

vulnerable to hacks.<sup>7</sup> As such, EPIC agrees with commenters that databases and “white lists” that store lists of blocked numbers require strong security measures.

EPIC has long advocated for minimizing the amount of data collected as data that is not collected and stored cannot fall into the wrong hands in the event of a breach.<sup>8</sup> However, in this case a list of numbers that have been blocked by providers must include all numbers that have been blocked and will be an attractive target for hackers.<sup>9</sup> Furthermore, if such a database is compromised it would not only allow scammers to continue with their illegal behavior, it would severely hamper any further efforts of the Commission to implement widespread blocking of invalid numbers.

Strong privacy protections are also a necessary and pragmatic part of risk mitigation in the age of the ubiquitous cybersecurity breach. Failure to protect privacy frequently stems from failure to adequately secure data. While minimizing data would not be possible in this situation,

---

(DITMAC) and DoD Component Insider Threat Records System, Jun. 2, 2016,

<https://epic.org/apa/comments/index.php?y=2016>; Comments of EPIC, *Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs Enforcement-016 FALCON Search and Analysis System of Records*, Jun. 5, 2017, <https://epic.org/apa/comments/EPIC-DHS-FALCON-Database-Comments.pdf>.

<sup>7</sup> U.S. Gov’t Accountability Office, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System* (Jan. 2016) <http://www.gao.gov/assets/680/674829.pdf>; U.S. Gov’t Accountability Office, *Federal Agencies Need to Better Protect Sensitive Data 4* (Nov. 17, 2015), <http://www.gao.gov/assets/680/673678.pdf>; Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People Federal Authorities Say*, Washington Post, Jul. 9, 2015, [https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm\\_term=.befc40c3cbb8](https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.befc40c3cbb8); Jada F. Smith, *Cyberattack Exposes I.R.S. Tax returns*, New York Times, May 26, 2015, <https://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html>.

<sup>8</sup> See, e.g., Comments of EPIC, *Standards for Safeguarding Customer Information Request for Public Comment*, Docket no. 2016-21231, Nov. 7, 2016, <https://epic.org/apa/comments/EPIC-FTC-Safeguards-Rule-Comments-11-07-2016.pdf>; Reply Comments of EPIC, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 11-12, WC Docket NO. 16-106, Jul. 6, 2016, <https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-Reply-Comments-07.06.16.pdf>; Comments of EPIC, *Request for Information: Big Data and the Future of Privacy*, Apr. 4, 2014, <https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf>; Brief of Amicus Curiae Electronic Privacy Information Center in Support of Respondent, *City of Ontario v. Quon*, 560 U.S. 746 (2010), [https://epic.org/privacy/quon/Quon\\_Brief\\_Draft\\_final.pdf](https://epic.org/privacy/quon/Quon_Brief_Draft_final.pdf).

<sup>9</sup> Bruce Schneier, *Data Is A Toxic Asset*, Schneier on Security, Mar. 4, 2016, [https://www.schneier.com/blog/archives/2016/03/data\\_is\\_a\\_toxic.html](https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html) (“saving [data] is dangerous because failing to secure it is damaging. It will reduce a company's profits, reduce its market share, hurt its stock price, cause it public embarrassment, and—in some cases—result in expensive lawsuits and occasionally, criminal charges. All this makes data a toxic asset, and it continues to be toxic as long as it sits in a company's computers and networks.”)

there are several steps that the FCC should take to minimize the risk that any database of blocked numbers is compromised such as:

- Checking references or doing background checks before hiring employees who will have access to the database;
- Ensuring that any phone provider that allows employees to have access to the database is trustworthy and has been trained in safeguarding data;
- Using trusted cybersecurity measures to secure the database;
- Reporting and investigating suspicious attempts to access the database
- Maintaining a careful inventory of the computers and any other equipment that is responsible for the security and storage of a database of blocked numbers
- Encrypting the database;
- Designating a manager to supervise the database and any updates or changes made to the database;
- Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information; and
- Keeping logs of activity on internal networks with access to the database and monitoring them for signs of unauthorized access to the database.

Implementing procedures such as these would help enhance the security of a database of blocked numbers ensuring the integrity of the database, the blocking program, and protecting consumers.

## **Conclusion**

For the reasons stated above EPIC urges the Commission (1) to continue with its plan to allow phone providers to block numbers that cannot possibly be from legitimate callers; (2) allow blocking to occur without obtaining consumer consent; and (3) to enact strong privacy and security measures should any database or white list of blocked numbers be created.

Respectfully Submitted,

/s/ Marc Rotenberg  
Marc Rotenberg  
EPIC President

/s/ Kim Miller  
Kim Miller  
EPIC Policy Fellow