epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, 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

Bridging the Digital Divide for Low-Income Consumers

47 CFR 54

January 27, 2020

The Electronic Privacy Information Center ("EPIC") submits these written comments in response to the Federal Communication Commission's ("FCC") Further Notice of Proposed Rulemaking, *Bridging the Digital Divide for Low-Income Consumers*.[1] This Notice concerns the administration of the FCC's Lifeline Program, which assists economically disadvantaged Americans in accessing broadband internet services.[2]

EPIC recommends that the Commission make clear that eligible telecommunications carriers ("ETCs") should not collect or retain detailed subscriber usage data. Instead, the Commission should implement an eligibility verification system that minimizes or eliminates the collection of personal

[1] FCC, *Bridging the Digital Divide for Low-Income Consumers*, 84 Fed. Reg. 71,338 (Dec. 27, 2020), https://www.federalregister.gov/documents/2019/12/27/2019-27221/bridging-the-digital-divide-for-low-income-consumers (hereinafter "Notice").

[2] The Lifeline Program, which is part of the Universal Service Fund, was established after the breakup of AT&T. *See* 49 Fed. Reg. 48325-01 (Dec. 12, 1984). The program originally provided support for access to telephone services. Congress expanded the program to include "advanced telecommunications services" and created a Federal-State Joint Board on Universal Service in the 1996 Telecommunications Act. 47 U.S.C. § 254. The Commission modernized the program in 2012 by providing Lifeline access to broadband internet services. *In re: Lifeline and Link Up Reform and Modernization*, 27 FCC Rcd. 6656 (2012).

data.[3]

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[4] EPIC contributed to the development of the Telephone Consumer Protection Act ("TCPA") and has advised Congress about emerging challenges to consumer protection law.[5] EPIC has also submitted numerous petitions and comments to the FCC advocating for greater privacy protections for telecommunications subscribers,[6] including the protection of Customer Proprietary Network Information and the end of an unnecessary data retention mandate.[7] EPIC has long advocated for protection of economically disadvantaged communities from surveillance and unnecessary data collection.[8]

---

[3] EPIC previously recommended that the Commission require Internet-Based Services comply with strict data security standards, including "Privacy Enhancing Technologies that minimize or eliminate the collection of Personally Identifiable Information ("PII"), as well as [techniques] for anonymization and deidentification that are robust, provable, scalable, and independently verified." EPIC, *Comments In re: Protecting Privacy of Customers of Broadband and Other Telecommunications Services*, WC Dkt. No. 16-106 (May 27, 2016) [hereinafter EPIC Broadband Privacy Comments], https://ecfsapi.fcc.gov/file/60002079241.pdf.

[4] *See About EPIC*, EPIC, https://epic.org/epic/about.html.

[5] *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 Marc Rotenberg), http://www.c-span.org/video/?18726-1/telephone-solicitation; S.1963, The Wireless 411 Privacy Act: Hearing Before the S. Comm. on Commerce, Sci., & Transp., 108th Cong., 2d Sess. (Sept. 21, 2004), (Testimony of Marc Rotenberg discussing privacy issues raised by a proposed wireless directory for customers of wireless telephone services).

[6] EPIC has filed more than 30 comments with the Commission since 1997. *See* EPIC, Administrative Procedure Act Comments: Federal Communications Commission (2020), https://epic.org/apa/comments/index.php?a=Federal+Communications+Commission.
See, e.g., EPIC et al., Comments in the Matter of Telemarketing Rulemaking, FTC File No. R411001 (2002), https://epic.org/privacy/telemarketing/tsrcomments.html; EPIC et al., Comments in the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278 (2002), https://epic.org/privacy/telemarketing/tcpacomments.html.

[7] EPIC's 2005 petition led to the Commission's further rulemaking on CPNI in 2007, which was upheld by the D.C. Circuit in 2009. *Nat'l Cable & Telecomm. Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009). EPIC also recently filed comments on the Commission's proposed broadband privacy rule. *See* EPIC Broadband Privacy Comments, *supra*.

[8] *See* EPIC, *Poverty and Privacy*, https://epic.org/privacy/poverty/; Brief of EPIC and Twenty-Two Technical Experts and Legal Scholars in Support of Respondent, *Kansas v. Glover*, No. 18-556, *cert. granted* 139 S. Ct. 1445 (Mem) (2019), https://epic.org/amicus/fourth-amendment/glover/EPIC-

Congress created the FCC to ensure that "all people in the United States shall have access to rapid, efficient, nationwide communications service with adequate facilities at reasonable charges."[9] The Lifeline Program is essential to the FCC's core mission, and the Commission has rightly expanded the program to cover broadband service in order to ensure that economically disadvantaged Americans have access to the services "essential to participate in today's society."[10] But Americans should not be required to sacrifice their privacy in order to access the Internet. The FCC has the authority and the obligation to protect subscribers from privacy invasions and unnecessary data collection.

The consumers eligible for the Lifeline program are already at risk of significant privacy invasions due to their socioeconomic status.[11] Surveillance systems established to defend against fraud in government benefit programs have instead become instruments to exert control over economically disadvantaged individuals.[12] The FCC should not impose additional privacy costs on these individuals, especially when there is no evidence that collection of personal data about internet *subscribers* is necessary to prevent potential waste, fraud, and abuse by internet *providers*. Instead, the Commission should promote privacy enhancing techniques that minimize or eliminate the collection of user data. The Commission clearly has the authority to protect the privacy of internet

---

Amicus-Kansas-v-Glover.pdf; EPIC letter to U.S. House Comm. on Oversight & Gov't Reform, Subcomm. on Heathcare, Benefits, and Admin. Rules & Subcomm. on Intergovernmental Affairs (May 8, 2018) (concerning proposal to create federal database of SNAP recipients), https://epic.org/testimony/congress/EPIC-HCOGR-SNAP-May2018.pdf.

[9] Fed. Commc'ns Comm'n, *Universal Service Fund,* https://www.fcc.gov/general/universal-service-fund (last accessed Jan. 24, 2020); *see* 47 U.S.C. § 151.

[10] 31 FCC Rcd. 7048 (Apr. 27, 2016).

[11] See, e.g., Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (2018); Kaveh Waddell, *How Big Data Harms Poor Communities*, The Atlantic (April 8, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-big-data-harms-poor-communities/477423/.

[12] Barton Gellman and Sam Adler-Bell, *The Disparate Impact of Surveillance*, The Century Foundation (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance/.

subscribers and should take this opportunity to make clear that it will not endorse the unnecessary collection or retention of personal data.

I. The FCC Should Protect the Privacy of Lifeline Subscribers and Should Not Permit Installation of Unwanted Apps on Subscribers' Mobile Devices

In its Notice the Commission seeks comments on "ways to ensure the accuracy of [carriers'] claims that subscribers are actually using their broadband internet access service on an ongoing basis," positing that providers might "fabricate usage data" by "installing an application ('app') on a user's phone that would 'use' data without any action by the user."[13] The Commission also seeks comments on possible rules or requirements that might help verify usage by the Lifeline subscriber, including whether the FCC should "requir[e] subscribers to use an app to confirm continued usage."[14] The Commission also rightly seeks comments on "any potential privacy implications of modifying the usage requirement or requiring the installation of a specific app or method of usage."[15]

Requiring Lifeline participants to install a specific app to monitor usage would undermine user privacy and security. Indeed, there is evidence that Lifeline subscribers face substantial privacy and security risks due to unwanted software installed on their mobile devices. Recent reporting has revealed that one Lifeline provider, Assurance Wireless, offers a free Android device preloaded with Chinese malware.[16] Security researchers found that the malware creates a backdoor for hackers and is impossible to remove from the devices.[17] In 2019, research funded by the Department of

---

[13] 84 Fed. Reg. at 71,340.
[14] *Id*.
[15] *Id*.
[16] Thomas Brewster, *U.S. Funds Program With Free Android Phones For The Poor — But With Permanent Chinese Malware,* Forbes (Jan. 9, 2020), https://www.forbes.com/sites/thomasbrewster/2020/01/09/us-funds-free-android-phones-for-the-poor---but-with-permanent-chinese-malware/#5db9b73ababe.
[17] *Id*.

Homeland Security found 146 new vulnerabilities pre-installed across 29 Android devices.[18] Security researchers have noted that: "If malware or security issues can make its way as a preinstalled app, then the damage it can do is greater, and that's why we need so much reviewing, auditing and analysis."[19] The Assurance Wireless devices expose Lifeline subscribers to privacy and security risks that they would not face if they were not enrolled in the program. As Senator Ron Wyden explained:

> Privacy shouldn't just be for the wealthy and well-connected. It's outrageous that taxpayer money may be going to companies providing malware-ridden phones to low-income families. Americans that depend on this program shouldn't be paying the price with their security and privacy.[20]

EPIC advises the Commission to forbid ETCs—such as Assurance Wireless—from installing unwanted apps on Lifeline subscribers' phones. This practice violates the privacy and security of subscribers and imposes an unfair burden on these vulnerable communities.

The FCC should also not require Lifeline participants to install apps to monitor usage because that monitoring would be a significant invasion of subscriber privacy and would create new security risks. Moreover, it is not necessary to require that a subscriber install an app to continuously usage. The FCC should pursue privacy protective systems that can serve the goal of verifying Lifeline eligibility. The requirement that Lifeline subscribers use their broadband internet service once every thirty days can easily be satisfied without detailed usage data or the extensive collection of personal information. Usage tracking would invade the privacy of these subscribers, who are already at risk of unwanted monitoring, and would not actually target providers that perpetrate fraud.

---

[18] Brian Barrett, *146 New Vulnerabilities All Come Preinstalled on Android Phones,* Wired (Nov. 11, 2019), https://www.wired.com/story/146-bugs-preinstalled-android-phones/.
[19] Alfred Ng, *Android Malware That Comes Preinstalled Is a Massive Threat*, CNET (Aug. 8, 2019), https://www.cnet.com/news/android-malware-that-comes-preinstalled-are-a-massive-threat/.
[20] @RonWyden, Twitter (Jan. 10, 2020, 2:40 PM), https://twitter.com/RonWyden/status/1215720146033106951.

II. The FCC Should Not Require Carriers to Retain Detailed Subscriber Usage Records

In its Notice the Commission seeks comments on how the FCC can "best safeguard Lifeline subscribers' privacy" in adopting a requirement for ETCs to "maintain detailed data usage records" to document compliance with the usage requirement.[21] The term "detailed usage records" is not defined in the Notice, leaving open the possibility that the FCC would require ETCs to maintain records of all the data collected on subscribers including browsing history, app usage, and geolocation data. This level of data retention is inexcusably broad for the purpose of demonstrating compliance with the usage requirement.

The FCC should not require ETCs to maintain detailed data usage records on individual consumers. ETCs should only store the minimum amount of personal data necessary to confirm eligibility and compliance with the program requirements. This is essential to the basic structure of privacy law, which is based on the Fair Information Practices ("FIPs").[22] The OECD Privacy Guidelines, which were endorsed in 1980 by many countries (including the United States) to implement the FIPs, state that "[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[23] The OECD Privacy Guidelines also provide that "[t]he purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."[24] The FCC's

---

[21] 84 Fed. Reg. at 71,340.
[22] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, Stan. Tech. L. Rev. 1 (2001).
[23] *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD (Sept. 22, 1980), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.
[24] *Id.*

proposed requirement would be contrary to the FIPs and the OECD Privacy Guidelines because ETCs would collect and retain more information than necessary for the specified purpose.

The Commission has not established that this data is necessary to detect fraud and abuse in the Lifeline program. While the Commission hypothesizes that detailed data usage records might "reveal any trends that reveal indications of potential usage fabrication,"[25] there is no evidence that *subscriber* data would actually detect fraud by ETCs. Indeed, if the concern is that ETCs are fabricating usage data, then the Commission should not rely on any usage data collected by the ETCs to attempt to detect fraud.

The FCC should not mandate the collection and retention of detailed usage data.[26] Cell phones reveal more sensitive information than landlines. As Chief Justice Roberts wrote in *Riley v. California*, "[t]he term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."[27] As EPIC has previously explained, cell phones "are an extension of the contents of a user's mind, both by the information that they gather and their relation to the user."[28] Both the quantity and sensitivity of the data stored on cell phones advise against carriers maintaining detailed data usage records. Retention of phone records also implicates the privacy and freedom of association rights of Americans and exposes consumers to increased risk of data breaches.[29] As Justice Sotomayor stated in *United*

[25] 84 Fed. Reg. at 71,340.
[26] EPIC has previously advocated for the FCC to end to the retention mandate for telephone toll records, filing a petition to repeal 47 C.F.R § 42.6 with a coalition of civil society organizations, legal scholars, and technology experts. EPIC Coalition, *Petition to Repeal 47 C.F.R. § 42.6 ("Retention of Telephone Toll Records")* (Aug. 4, 2015), https://epic.org/privacy/fcc-data-retention-petition.pdf.
[27] Riley v. California, 573 U.S. 373, 393 (2014).
[28] Amanda Ottoway, *Top NJ Court Mines 5th Amendment for Password Privacy*, Courthouse News Service (January 21, 2019), https://www.courthousenews.com/top-nj-court-mines-5th-amendment-for-password-privacy/; EPIC, *State v. Andrews*, https://epic.org/amicus/fifth-amendment/andrews/.
[29] EPIC, *End the FCC Data Retention Mandate!*, https://epic.org/privacy/fcc-data-retention/.

States v. Jones, "[a]wareness that the Government may be watching chills associational and expressive freedoms."[30]

As a result of this prosed rule, detailed personal data about the Internet browsing habits of Lifeline subscribers would be available to ETCs and to FCC staff. This requirement would chill the ability of economically disadvantaged Americans ability to access information that is vital to their health, well-being, safety, and education. Subscribers who wish to use their devices to access sensitive information, including topics such as mental health and addiction, depression and alcoholism could be deterred.[31] Beneficiaries of government programs such as Lifeline should not be subject to regular government intrusions to maintain their eligibility for benefits.[32]

The Commission should instead deploy a privacy enhancing techniques to confirm only program eligibility while minimizing the collection of personal data. For example, ETCs could maintain records that indicate only whether or not the subscriber used the account within a thirty-day period to satisfy the Lifeline program's usage requirement. Participants could be given the option to self-certify their eligibility with the Commission through a simple web form. Any benefit derived from maintaining detailed usage records would be outweighed by the substantial privacy harm that would be caused by the collection of that data. Therefore, EPIC advises the FCC not to adopt a requirement for ETCs to maintain detailed data usage records.

III. The FCC Has the Authority and an Obligation to Protect Subscriber Privacy

The Commission also seeks comments on the scope of its authority to regulate the business practices of ETCs, including whether the FTC has the authority to "prohibit ETCs from installing an

[30] *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
[31] *See, e.g.*, EPIC, *Online Tracking and Behavioral Profiling*, https://epic.org/privacy/consumer/online-tracking/.
[32] Barton Gellman and Sam Adler-Bell, *The Disparate Impact of Surveillance*, The Century Foundation (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance/.

app that 'uses' data without direction from the subscriber" or to "regulate the distribution of handsets."[33]

The Commission has broad statutory authority to implement "policies for the preservation and advancement of universal service," including providing "low-income consumers and those in rural, insular, and high cost areas" access to advanced communications services "reasonably comparable to those services provided in urban areas."[34] The Commission is also authorized, pursuant to its universal service mandate, to implement policies "necessary and appropriate for the protection of the public interest, convenience, and necessity"[35] and must ensure that "universal service"—including broadband internet access—"is available at rates that are just, reasonable, and affordable."[36] The Commission has the authority to perform "any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."[37]

The Commission is also uniquely positioned to protect the privacy of all communications subscribers. Indeed, most federal privacy laws fall within the FCC's jurisdiction. The Commission has the authority promulgate privacy regulations and enforce privacy obligations for telecommunications carriers,[38] cable providers,[39] satellite providers,[40] and other communications providers within the FCC's jurisdiction.[41] For example, the Commission protects the "privacy of customer information" through promulgation and enforcement of its Customer Proprietary Network

[33] 84 Fed. Reg. at 71340, 71341.
[34] 47 U.S.C. § 254(b), (b)(3).
[35] 47 U.S.C. § 254(b)(7).
[36] 47 U.S.C. § 254(i).
[37] 47 U.S.C. § 154(i).
[38] 47 U.S.C. § 222.
[39] 47 U.S.C. § 551.
[40] 47 U.S.C. § 338.
[41] *See, e.g.*, 47 U.S.C. § 615a-1.

Information rules pursuant to Section 222. The Commission also has an important obligation to protect consumers of common carriage services, as the FCC and FTC have explained in their consumer protection memorandum.[42]

Conclusion

It is imperative that the Commission enact rules that protect the privacy of Lifeline subscribers. That means both restricting the actions of carriers that invade subscriber privacy—such as surreptitiously installing apps on users' mobile phones—and understanding the privacy impact of data collection and retention obligations. It would not be in the public interest for the Commission to mandate the collection and retention of detailed usage data for Lifeline subscribers. But it would be in the public interest for the Commission to protect Lifeline subscribers by prohibiting carriers' installation of unauthorized apps and by bringing enforcement actions against carriers who have violated their subscribers' privacy.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Alan Butler*
Alan Butler
EPIC General Counsel

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

[42] FCC-FTC Memorandum of Understanding (2015), https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.