

REPLY COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Federal Communications Commission

on

Addressing the Homework Gap Through the E-Rate Program

88 Fed. Reg. 85,157, WC Docket No. 21-31

January 29, 2024

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Federal Communication Commission (FCC or the Commission)'s December 7, 2023 notice of proposed rulemaking to use E-Rate program funding to provide students with Wi-Fi hotspots when they lack internet access at home.¹ In this rulemaking, the FCC would align the older E-Rate program with the Emergency Connectivity Fund (ECF), allowing the Commission to continue disbursing funds to schools and libraries for remote learning.

EPIC is a public interest research center in Washington, DC established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC has long

¹ *In re* Addressing the Homework Gap Through the E-Rate Program, WC Dkt. No. 21-31 (Rel. Nov. 8, 2023), <https://docs.fcc.gov/public/attachments/FCC-23-91A1.pdf> [hereinafter NPRM]. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 85,157 (Dec. 7, 2023), and is available at <https://www.federalregister.gov/documents/2023/12/07/2023-26033/addressing-the-homework-gap-through-the-e-rate-program>.

advocated for consumer privacy protections in online services and regularly files comments with the FCC.² EPIC also advocates specifically for the protection of student privacy.³

EPIC supports the Commission’s proposal to expand the E-Rate program and urges the FCC to (1) not collect personal financial information from program recipients, (2) require only a certification that devices are used for primarily educational purposes, (3) permit multi-user hotspots, (4) decline to require consequences for non-educational use of devices, and (5) prohibit monitoring of students’ use of Wi-Fi hotspots.

Background

In this rulemaking, the Commission proposes to update definitions in the E-Rate program administered through the Universal Service Fund to allow schools and libraries to receive funding to distribute Wi-Fi hotspots to students without access to reliable broadband internet at home. The Universal Service Fund allows the Commission to address gaps in accessible telephone and internet service by defraying unusually high costs for telecommunications providers and subsidizing the price of internet and phone service for low-income individuals.⁴ It has not previously supported Wi-Fi hotspots.

The Commission began providing schools and libraries funding to distribute Wi-Fi hotspots through the Emergency Connectivity Fund in 2021 to address remote learning in the midst of the

² See, e.g., Reply Comments of EPIC, *In re* Safeguarding and Securing the Open Internet, WC Dkt. No. 23-320 (Jan. 17, 2024), <https://www.fcc.gov/ecfs/search/search-filings/filing/1011892947581>; Reply Comments of EPIC, Center for Democracy and Technology, Privacy Rights Clearinghouse, and Public Knowledge, *In re* Data Breach Reporting Requirements, WC Dkt. No. 22-21 (Mar. 24, 2023), <https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814>; Comments of EPIC, *In re* Location-Based Routing for Wireless 911 Calls, PS Dkt. No. 18-64 (Feb. 16, 2023), <https://www.fcc.gov/ecfs/search/search-filings/filing/10216148603009>; Comments of EPIC, et al., *In re* Supporting Survivors of Domestic and Sexual Violence, WC Dkt. Nos. 22-238, 11-42, 21-450 (Apr. 12, 2023), <https://www.fcc.gov/ecfs/search/search-filings/filing/104131354805768>.

³ See, e.g., “Student Privacy”, <https://epic.org/issues/data-protection/student-privacy/>.

⁴ See FCC, Universal Service Fund, [fcc.org](https://www.fcc.gov/general/universal-service-fund) (last accessed Jan 29, 2024), <https://www.fcc.gov/general/universal-service-fund>.

COVID-19 crisis.⁵ The ECF aims to address the “Homework Gap” created when some students are unable to access broadband internet at home and therefore face obstacles to completing homework not faced by wealthier or less-remote peers.⁶ After more than two successful years supporting schools, libraries, and students, the ECF will sunset June 30, 2024.⁷

In this rulemaking, the Commission seeks to build upon the success of the ECF program by expanding devices and services that may be funded through the E-Rate program to include Wi-Fi hotspots and telecommunications services. In particular, the Commission is considering how to ensure that funds are used to support remote learning and proposes several methods for monitoring use of hotspots.

I. The Commission should reduce surveillance and administrative burdens as much as possible to ensure the program is safe and effective for students.

Requiring schools and libraries to collect personal information and monitor use of Wi-Fi hotspots will pose a serious threat to recipients’ privacy and render the E-Rate program less effective. While addressing the homework gap is an important goal, EPIC urges the Commission to consider that ancillary uses of hotspots are not a waste of funds, and that the negative impacts of surveillance and compliance will be much higher than any asserted benefits. Ultimately, the Commission should be focused on program effectiveness, and surveillance imposes a barrier to access that does not further that effectiveness.

In the NPRM, the Commission proposes collecting surveys of individuals’ financial information to ensure that hotspots are only being distributed to those who cannot afford broadband services.⁸ We urge the Commission not to require any personal financial information in exchange for

⁵ See NPRM at ¶ 2.

⁶ See *id.* at ¶¶ 2-3.

⁷ See *id.* at ¶ 4.

⁸ See *id.* at ¶¶ 30-35.

a Wi-Fi hotspot.⁹ First, one of the primary recipients of hotspots are children, who may not have access to family financial information. Imposing a barrier between a child asking for a hotspot and receiving one will limit the effectiveness of the program without corresponding benefits. While aggregate surveys of recipients may be appropriate, we still caution the Commission that the benefits of such surveys may not outweigh the harms of discouraging qualified individuals from participating¹⁰ or the logistical costs this would impose on the public institutions administering the device program.

The NPRM further proposes requiring individuals to certify need and participation in other benefits programs like the National School Lunch Program.¹¹ Such requirements impose further barriers to access and threaten to exclude individuals who may not participate in specific benefits programs but still lack at-home internet access. There are also questions of stigma.¹² The American Library Association notes that circulation and data usage statistics at an aggregate level should be sufficient for programmatic audits, and we agree.¹³

Similarly, the Commission should go no further than requiring that schools and libraries distributing devices certify compliance on program forms that they will be used primarily for

⁹ See *id.* at ¶¶ 31-32.

¹⁰ See, e.g., Comment of American Library Association at 8 (Jan. 16, 2024), <https://www.fcc.gov/ecfs/search/search-filings/filing/101161546100253> [hereinafter “ALA Comment”] (“Patrons had reservations that the information could be shared with vendors or the government (would the Commission contact patrons during audit to verify use?) or that they could be faulted for exceeding the data limit or incorrect use.”). This could also impact institutions participating. See, e.g., Comments from the Wisconsin Department of Public Instruction at 5 (Jan. 16, 2024), <https://www.fcc.gov/ecfs/search/search-filings/filing/101161644305936> [hereinafter “WI DPI Comment”] (“Wisconsin library staff have told us they wanted to apply for ECF, but did not want to then have to filter all their in-building computers. This concern noted, we ask the Commission to minimize the impact of CIPA, which will then maximize the number of our libraries that can apply for E-Rate discounts on Wi-Fi hotspots and related services.”).

¹¹ See NPRM at ¶ 32.

¹² See, e.g., WI DPI Comment at 2 (“library staff must then ask patrons about their internet access, or lack thereof. Staff and patrons find this intrusive, embarrassing and an unnecessary intrusion on patron privacy”).

¹³ See ALA Comment at 8 (“Circulation and data usage statistics should be sufficient to demonstrate the reach and demand for a library’s hotspot lending program and should be sufficient for programmatic audits. For all these reasons, the Commission should not require the collection and retention of PII by libraries beyond the loan period of the Wi-Fi hotspot.”)

educational purposes.¹⁴ The Commission proposes requiring use policies that limit hotspots to “solely educational use” and an affiliated auditing program that would require monitoring actual device usage.¹⁵ Those requirements pose serious privacy and safety harms to children and their families who may end up using the hotspot.¹⁶ Any form of internet monitoring should be explicitly prohibited by the Commission. Monitoring individuals’ web browsing is a profound invasion of privacy and can expose children to risks of prosecution, violence, extortion, and reputational harm. For example, a student who uses their hotspot for primarily educational purposes might also look up abortion access information. In a state where abortions are now illegal, allowing school staff and librarians to review that student’s browsing history could expose the student to prosecution, reveal their reproductive health information to staff or the student’s family, and create other downstream harms.¹⁷

We further urge the Commission to permit multi-user hotspots and not to track whether multiple individuals in a household use the device. If other family members use a hotspot in addition to students, the Commission should view that as an ancillary benefit, not a misuse of E-Rate funds and equipment. The Commission proposes limiting permitted hotspots to single-user devices in line with the sunseting ECF program.¹⁸ However, the E-Rate program’s ambit is broader than the ECF

¹⁴ See NPRM at ¶¶ 34-36.

¹⁵ *Id.* at ¶¶ 36-38.

¹⁶ We disagree with the Commission’s proposal to prohibit multi-user hotspots. See NPRM at ¶¶ 20-21. We believe users should be able to enjoy incidental, non-educational uses of hotspots, such as telehealth and completing government forms, but do not need special dispensation from the Commission to do so. See NPRM at ¶ 38. Or applying for jobs. See, e.g., Comment of Cindy Murdock Ames (Jan. 3, 2023), <https://www.fcc.gov/ecfs/search/search-filings/filing/1010333357694> (also noting it is wasteful to limit bandwidth to a single user when a hotspot can support multiple simultaneous users in a family’s home).

¹⁷ See Sara Geoghegan and Dana Khabbaz, Reproductive Privacy in the Age of Surveillance Capitalism, epic.org (July 7, 2022), <https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/>. This may be true for gender-affirming care in some states as well. See, e.g., Brian Klosterboer, Texas’ Attempt to Tear Parents and Trans Youth Apart, One Year Later (Feb. 23, 2023), <https://www.aclu.org/news/lgbtq-rights/texas-attempt-to-tear-parents-and-trans-youth-apart-one-year-later>.

¹⁸ See NPRM at ¶¶ 20-21.

program, covering a variety of populations with unmet needs for internet service. There is no conflict between a student using an E-Rate program hotspot for their homework and a parent using it to apply for jobs, to seek government benefits, or stay in touch with other family members. Schools and libraries should have flexibility to purchase and provide the hotspot products that best suit the specific populations they serve. And reducing the requirements that schools and libraries have to meet to qualify for E-Rate funds will make the program easier to administer and more cost-effective for already overburdened librarians.

Because the E-Rate program operates through many small disbursements to local institutions, requiring detailed data collection increases the odds that a single bad actor with access to user browsing information may misuse that information. Data minimization, a fundamental risk-reduction concept in cyber hygiene and information management,¹⁹ counsels that you don't have to protect what you don't collect.²⁰ As the Commission is aware, schools are increasingly targets of successful cyber-attacks resulting in breaches of student data.²¹ Collecting potentially sensitive information

¹⁹ See, e.g., Fed. Trade Comm'n, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,277 (advanced notice issued Aug. 22, 2022), <https://www.federalregister.gov/d/2022-17752/p-88> (The term "data security" in this ANPR refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices); Joint Task Force Transformation Initiative Interagency Working Group (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 20, 2020, at 72, 270, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>; NIST, Using Risk Management to Improve Privacy in Information Systems (Sept. 11, 2015), [https://csrc.nist.gov/CSRC/media/Presentations/Using-Risk-Management-to-Improve-Privacy-in-In-\(2\)/images-media/day3_research_1035-1125.pdf](https://csrc.nist.gov/CSRC/media/Presentations/Using-Risk-Management-to-Improve-Privacy-in-In-(2)/images-media/day3_research_1035-1125.pdf); Federal Privacy Counsel, Fair Information Practice Principles (FIPPs), <https://www.fpc.gov/resources/fipps/>; 16 C.F.R. pts. 314.4(c)(6), 682; Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0 at 73-101 (Requirement 3) (March 2022), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf. See also N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022); NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Apr. 16, 2018), at 34 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

²⁰ See John Davison, Data Minimization: A Pillar of Data Security, But More Than That Too (June 22, 2023), <https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/>.

²¹ See, e.g., *In re Schools and Libraries Cybersecurity Pilot Program*, Notice of Proposed Rulemaking, WC Dkt. No. 23-234 (Rel. Nov. 13, 2023), <https://www.fcc.gov/document/fcc-proposes-schools-libraries->

about students for the purposes of program administration wrongly elevates fraud, waste, and abuse concerns over the protection of student privacy. Moreover, tracking is not required under Children’s Internet Protection Act (CIPA).²² Multiple commenters from schools and libraries also flagged challenges with costs, training burdens, and conflicts with state privacy laws that would result from imposing reporting or filtering requirements such as those required under CIPA.²³ The American Library Association has found that CIPA does not apply to many scenarios involving library patrons.²⁴ EPIC agrees with these commenters and emphasizes the questionable benefit, if any, that

cybersecurity-pilot-program; U.S. Gov’t Accountability Off., GAO-20-644, Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm (Sept. 2020), <https://www.gao.gov/products/gao-20-644>; U.S. Dep’t of Education, Privacy Technical Assistance Center, SPPO-21-03, A Parent’s Guide for Understanding K-12 School Data Breaches, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Parent%20Guide%20to%20Data%20Breach.pdf (last accessed Jan. 29, 2024).

²² See Fed. Comm’n Comm’n, Children’s Internet Protection Act (CIPA), <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act> (last accessed Jan. 29, 2024) (“CIPA does not require the tracking of Internet use by minors or adults”). E-Rate Central interprets CIPA’s monitoring requirement as requiring only supervision, not technical measures. See E-Rate Central, Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries at 2 n 7 https://e-ratecentral.com/Portals/0/DocFiles/files/cipa/cipa_policy_primer.pdf, available at <https://e-ratecentral.com/Resources/Educational-Information/CIPA> (last accessed Jan. 29, 2024). At least two states seem to follow this interpretation. See, e.g., Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries, maine.gov, https://www.maine.gov/msl/erate/cipa_policy_primer.pdf (last accessed Jan. 29, 2024); North Carolina Department of Public Instruction Instructional Technology/Connectivity Services, A Brief on Internet Safety and E-rate Compliance with the Children's Internet Protection Act (CIPA) The Neighborhood Children's Internet Protection Act (NCIPA) and the Broadband Data Improvement Act (BDIA) (a.k.a. The Protecting Children in the 21st Century Act) (May 26, 2010), <https://files.nc.gov/dpi/documents/erate/training/cipa-faq.pdf>. Moreover, even if online tracking were a requirement under CIPA, the Commission would have the discretion to waive compliance beyond the first year. See Universal Services Administrative Co., FAQs, “Q20: How long do E-Rate program participants have to implement the requirements under CIPA?”, https://www.usac.org/?s=cipa&post_type=eratefaqs (last accessed Jan. 29, 2024).

²³ See, e.g., WI DPI Comment; ALA Comment; Notice of ex parte (Dec. 20, 2023), <https://www.fcc.gov/ecfs/search/search-filings/filing/1220177182004>; Comment of Cindy Murdock Ames *supra* note 16; Comment of EveryLibrary Institute NFP (Jan. 8, 2024), <https://www.fcc.gov/ecfs/search/search-filings/filing/1010868329828>; Comment of Suzanne Hall (Dec. 20, 2023), <https://www.fcc.gov/ecfs/search/search-filings/filing/12200276606432>.

²⁴ See, e.g., ALA Comment at 2 (CIPA does not apply to “the use of off-premises patron-owned devices”, nor to “library-owned computers when a library receives E-Rate only for Wi-Fi hotspots for off-site use and is not receiving any E-Rate funds for its in-building internet access or internal connections”); *id.* at 10 (“a We are pleased to see that in its ECF regulations the Commission recognized that personally owned devices are not subject to CIPA’s filtering requirement. (This is a position ALA has ascribed to for about twenty years.),,,We

might result from this data collection.²⁵ Ultimately, librarians are not parents and should not be put in the position of monitoring children’s (or adults’) internet usage for inappropriate or off-program content.

As the Commission itself notes, there are privacy concerns related to library patrons’ data and to third-party-owned devices accessing E-Rate funded Internet.²⁶ While CIPA requires schools and libraries to adopt and enforce policies that include technological protections to block obscene content,²⁷ this does not require tracking the user’s online activity. The Commission’s proposal of permitting uses of E-Rate hotspots for incidental non-educational purposes should be unnecessary.²⁸

Eliminating surveillance requirements will reduce the risk of harm to program recipients, protect their privacy, and strengthen the effectiveness of the program. EPIC urges the Commission to require at most a certification from the distributing school or library that devices are used for “primarily” educational purposes.

II. Resources

We also offer three resources that address the problematic consequences of public benefits means-testing through surveillance, specifically where algorithms are used:

do not think this language in any way can be stretched to encompass personally-owned devices. Thus, whether patron’s personal devices are used within the library or at home, CIPA does not apply.”).

²⁵ See WI DPI Comment at 3 (“For example, if an audit is performed in 2027 for device used in 2025, of what use or purpose is it to know the device was loaned to a particular patron? Would the auditors really try and contact that patron and ask what they were using the Wi-Fi hotspot device for during a two-week loan period that happened several years ago?”).

²⁶ See NPRM at ¶ 58; WI DPI Comment at 4 (noting that Commission has already found that CIPA does not apply to the use of third-party owned devices and proposing to find otherwise now is fundamentally out of scope of the Commission’s authority under CIPA).

²⁷ We note that interpretation of “obscenity” may have harmful implications for students in states hostile to members of the LGBTQ+ community. See, e.g., Jo Yurcaba, *Under West Virginia bills, exposing minors to transgender people could be a crime*, NBC News (Jan. 20, 2023), <https://www.nbcnews.com/nbc-out/out-politics-and-policy/west-virginia-bills-exposing-minors-transgender-people-crime-rcna66742>. (2023); and again in 2024, see JP Leskovich, *West Virginia legislator introduces bills classifying transgender people as ‘obscene matter’ and banning gender-affirming care for people under 21*, Jurist, Jan. 12, 2024), <https://www.jurist.org/news/2024/01/west-virginia-legislator-introduces-bills-classifying-transgender-people-as-obscene-matter-and-ban-gender-affirming-care-for-people-under-21/>.

²⁸ See NPRM at ¶ 38.

- (1) *Screened & Scored in the District of Columbia* was published by EPIC in November 2022. The report sheds light on how the D.C. government outsources critical decisions to automated decision-making systems in areas such as public benefits, healthcare, policing, and housing. As a result, District residents are surveilled, screened, and scored every day. The report is available at <https://epic.org/screened-scored-in-dc/>.
- (2) EPIC Complaint and Request for Investigation, Injunction, and Other Relief, *In re Thomson Reuters et al.* (Jan. 3, 2024). This complaint concerns the development, sale, and operation of the “Fraud Detect” automated fraud detection system, which purports to accurately detect public benefits fraud through an opaque, proprietary algorithm and commercial data derived from sources like social media, credit reports, and housing records, but in reality leaves hundreds of thousands of legitimate claimants without access to public benefits more often than not. The complaint is available at <https://epic.org/wp-content/uploads/2024/01/EPIC-FTC-Thomson-Reuters-Complaint.pdf>.
- (3) *Public Benefits, Private Vendors: How Private Companies Help Run our Welfare Programs*, by Grant Fergusson, Equal Justice Works Fellow (Jan. 26, 2023). This article addresses the inaccurate and inefficient automated systems developed by the private companies to which governments have outsourced their public benefits programs. The post is available at <https://epic.org/public-benefits-private-vendors-how-private-companies-help-run-our-welfare-programs/>.

Conclusion

We applaud the Commission’s efforts to close the homework gap for students without internet access while not at school. We urge that the Commission not allow this program to create new vulnerabilities by which student data could be compromised, nor chill participation in the program due to invasive or labor-intensive requirements, nor fall into the trap of systematized inaccurate denials of benefits to which other programs have succumbed.

Please reach out with any questions to EPIC Counsel Jake Wiener at wiener@epic.org or EPIC Counsel Christopher Frascella at frascella@epic.org.

Respectfully Submitted,

/s/ Jake Wiener
Jake Wiener
EPIC Counsel

/s/ Chris Frascella
Chris Frascella
EPIC Counsel