Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Schools and Libraries Cybersecurity Pilot Program	)	WC Docket No. 23-234
	)	

REPLY COMMENTS ON NOTICE OF PROPOSED RULE MAKING

by

Electronic Privacy Information Center (EPIC)

Submitted February 27, 2024

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

Chloe Le
Spring Intern
Electronic Privacy Information Center
Georgetown University Law Center

Table of Contents

Comments

I. Introduction and Summary

The **Electronic Privacy Information Center (EPIC)**[1] files these reply comments to applaud the Federal Communications Commission ("Commission" or "FCC") for its efforts to strengthen cybersecurity practices at schools and libraries, and to recommend important safeguards that simultaneously strengthen both cybersecurity and privacy, such as data minimization.

We encourage the Commission to permit schools and libraries to implement cybersecurity measures that best fit their needs, including measures recommended by the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Education (ED). We also encourage the Commission to design its Pilot Program such that a diverse range of entities can participate.

The Commission should be clear that its cybersecurity measures are not meant to erode student privacy protections. The Commission should additionally re-iterate the limits of a school's obligations under the Children's Internet Protection Act (CIPA), to avoid a similar privacy-diminishing outcome.

We agree with commenters who recommend that the Pilot Program should be administered annually rather than once every three years, to ensure nimbleness.

EPIC is heartened to see the Commission moving the needle on data security, especially as it relates to student data.

[1] 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 advocated for consumer privacy and data security protections, and regularly files comments with the FCC. *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, 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. EPIC also advocates specifically for the protection of student privacy. *See, e.g.*, Reply Comments of EPIC, *In re* Addressing the Homework Gap Through the E-Rate Program, WC Dkt. No. 21-31 (Jan. 29, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10129270690080 [hereinafter "EPIC Homework Gap Reply Comment"]; "Student Privacy", https://epic.org/issues/data-protection/student-privacy/.

II. The Commission should articulate eligible support in terms of general criteria rather than specific technologies.

The Commission requested comment on whether it should "specify eligibility in terms of general criteria rather than as a list of specific technologies" regarding the services and equipment eligible for support under the Pilot Program.[2] We urge the Commission to implement the former. Schools and libraries vary in size, structure, network topology, technology use, discount levels, and network configurations, among other considerations relevant to the selection of an effective cybersecurity solution.[3] For instance, while some K-12 schools may have robust IT departments, by some estimates two-thirds of school districts lack a full-time cybersecurity position to even implement resources from this Pilot Program.[4] However, many of these schools still have data that needs to be protected.

There is remarkable consistency across cybersecurity frameworks regarding what types of practices are most likely to prevent unauthorized access to data and systems, including the Cybersecurity and Infrastructure Security Agency (CISA)'s Cross-Sector Performance Goals (CPGs).[5] Schools should not be prevented from implementing these best practices.[6] As other

[2] *In re* Schools and Libraries Cybersecurity Pilot Program, WC Dkt. No. 23-234 at ¶ 40 (Rel. Nov. 13, 2023), https://docs.fcc.gov/public/attachments/FCC-23-92A1.pdf [hereinafter NPRM]. The Proposed Rule was published in the Federal Registrar at 88 Fed. Reg. 90141, and is available at https://www.federalregister.gov/documents/2023/12/29/2023-27811/schools-and-libraries-cybersecurity-pilot-program.

[3] *See* Crown Castle Fiber Comment at 3.

[4] *See* The Conversation, *Why Federal Efforts to Protect Schools From Cybersecurity Threats Fall Short* (Dec. 14, 2023), https://theconversation.com/why-federal-efforts-to-protect-schools-from-cybersecurity-threats-fall-short-216866.

[5] *See, e.g.*, EPIC, *In re* Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations at Appendix 1 (Oct. 31, 2023), https://epic.org/wp-content/uploads/2023/11/EPIC-CR-ONCD-RFI-2023.pdf [hereinafter "EPIC ONCD Comment"]. We further note that one of the Department of Education's K-12 Digital Infrastructure Briefs outlines questions that also align with these frameworks, including data mapping and data minimization principles such as purpose and retention limitations. Dep't of Ed., Office of Educational Technology, *K-12 Digital Infrastructure Brief: Privacy Enhancing, Interoperable, and Useful* at 11 (Aug. 2023), https://tech.ed.gov/files/2023/08/FINAL_Privacy_Interop_Useful.pdf.

[6] *See* NPRM at ¶ 32.

commenters have noted, these measures could include offerings that defend against viruses, ransomware, denial of service, unauthorized access, and domain name system attacks.[7] Endpoint detection and response (EDR) systems can offer real-time monitoring and rapid response capabilities to identify and contain malicious activities targeting endpoint devices within the network.[8] Additionally, authentication protocols play an important role in verifying the legitimacy of users and preventing unauthorized access to sensitive information and resources.[9] We note however that multi-factor authentication (MFA) should not be SMS-based, as the prevalence of SIM swapping has demonstrated that it is not a secure method of authentication.[10]

The Commission's goals with this Pilot Program include collecting data on effective cybersecurity measures;[11] as such, it should empower schools and libraries to implement the solutions that best meet their needs and evaluate the results.

III. The Commission should strive to include a diverse range of entities from the E-Rate Program to participate in this Pilot Program.

The Commission also seeks comment on what types of entities should be allowed to participate in the Pilot Program.[12] A key purpose of the program is to obtain valuable data about the current cybersecurity practices of K-12 schools and libraries and to help the Commission

[7] *See* Comment of Crown Castle Fiber LLC, WC Dkt. No. 23-234 at 3 (Jan. 29, 2024), https://www.fcc.gov/ecfs/document/101290188720791/1 [hereinafter Crown Castle Fiber Comment].
[8] *See id.* at 3.
[9] *See, e.g.*, EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* at 194-95, 201-02 (Nov. 2022), https://epic.org/ftc-rulemaking-on-commercial-surveillance-data-security/; EPIC ONCD Comment at 11-12; NPRM at ¶ 37.
[10] *See, e.g.*, Comment of EPIC, *In re* Protecting Consumers from SIM-Swap and Port-Out Fraud, WC Dkt. No. 21-341 at 2-5 (Jan. 16, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1011728090306. *See also* Cyber Safety Review Board, *Review of the Attacks Associated with Lapsus$ and Related Threat Groups* 48 (July 24, 2023), https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf ("NIST, CISA, and Okta are among those organizations that consider SMS/voice MFA the weakest form of MFA").
[11] *See* NPRM at ¶ 2.
[12] *See id.* at ¶ 34.

better understand the most effective way to use USF support to strengthen cybersecurity.[13] To collect representative data and capture different cybersecurity needs and challenges, it is essential to include a diverse range of entities in the program. First, the program should incorporate data from schools and libraries in various districts, encompassing both urban and rural areas.[14] Second, the program should involve schools from different education levels to account for varying cybersecurity needs across age groups and academic environments. Third, the program should analyze both small and large schools and libraries[15] because adequate cybersecurity is just as important for a child in a town with a population of 1,000 as it is for a child in a city with a population of 100,000. Lastly, the program should select entities with varying levels of technology infrastructure, including those with sophisticated IT systems and those with more limited resources. By including a diverse range of entities in the program, the Commission can gather comprehensive data on effective cybersecurity measures that can inform future initiatives and ensure that limited USF funds are utilized effectively on a larger scale.

One question that the Commission asked is whether the program should be limited to E-Rate participants.[16] We think that it should. While it would be ideal to provide all K-12 schools and public libraries with money for cybersecurity, the USF funds are limited. Therefore, it is important to prioritize high-need schools and libraries for participating in this Pilot Program, consistent with E-Rate's longstanding system.[17]

[13] *Id.* at ¶ 2.
[14] *Id.* at ¶ 34.
[15] *Id*.
[16] *Id*.
[17] *See* Comment of Foresight Law + Policy, PLLC, *Notice of Ex Parte, Schools and Libraries Cybersecurity Pilot Program*, WC Dkt. No. 23-234 at 2 (Jan. 10, 2024), https://www.fcc.gov/ecfs/document/10111298051611/1.

IV. The Commission should recognize that cybersecurity and privacy are complementary priorities, especially in the context of data minimization.

The Commission should be clear that raising defenses to improve cybersecurity does not come at the expense of student privacy; in fact, strong privacy practices can bolster a school's or library's data security program. The White House National Cybersecurity Strategy recognizes privacy as an important component to advancing cybersecurity,[18] as have Profs. Dan Solove and Woodrow Hartzog:

> [V]iewing data security policy primarily as a collection of requirements for breach notifications and technical controls excludes many of the most important issues from security, and it silos privacy and security in ways that are unproductive…[19] There are several ways that bad privacy can lead to bad security: (1) Weak privacy controls can lead to improper access through the front door; (2) Collecting and storing unnecessary data can make data breaches much worse; (3) Poor privacy regulation can allow for more tools and practices that compromise security; and (4) A lack of accountability over data can increase the likelihood that the data will be lost, misplaced, or misused.[20]

Data minimization, for example, fulfills the reasonable expectations of consumers (including purpose limitations for use of their data) at the same time it addresses data security concerns (companies "don't have to protect what [they] don't collect").[21] The FTC has explicitly listed data minimization alongside risk mitigation and data management and retention as a data security best practice.[22] This same principle applies to student data as well.

---

[18] *See* The White House, *Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy* (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/ (promoting privacy and security of personal data).

[19] *See* Daniel J. Solove & Woodrow Hartzog, *Breached! Why Data Security Law Fails and How to Improve It*, 132-33 (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4173764.

[20] *Id.* at 143.

[21] John Davisson, *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/.

[22] *See* 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

Cybersecurity should not be a justification for diminishing student privacy. Fundamental cybersecurity practices such as segmentation of systems and patching known vulnerabilities are largely independent of user activity. Even user-related cybersecurity best practices such as access controls and authentication do not require monitoring all of a user's online activity.

Limiting the amount of information that an organization collects reduces the risk of misuse of that information. Implementing cybersecurity measures in a manner that respects privacy can ultimately strengthen both aspects of online safety.

V. The Children's Internet Protection Act (CIPA) does not apply to third party devices; where it does apply, the Commission should ensure safeguards for student privacy.

The Commission seeks comment on the "scope of the Commission's authority to impose CIPA requirements on third-party devices that may connect with school- or library-owned broadband networks."[23] The Commission has previously determined that CIPA does not extend to the use of third-party owned devices,[24] and holding otherwise would fundamentally exceed the Commission's jurisdiction under CIPA.[25]

breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices").

[23] NPRM at ¶ 63.

[24] *See in re* Addressing the Homework Gap Through the E-Rate Program, WC Dkt. No. 21-31 at ¶ 54 (Rel. Nov. 8, 2023), https://docs.fcc.gov/public/attachments/FCC-23-91A1.pdf.

[25] Comment of the Wisconsin Department of Public Instruction, *In re* Addressing the Homework Gap Through the E-Rate Program, WC Dkt. No. 21-31 at 4 (Jan. 16, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/101161644305936 (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).

The Commission has previously recognized student privacy implications of CIPA.[26] These concerns arise from the possibility of schools having the ability to monitor all online student activity. While CIPA mandates that schools and libraries implement policies with technological safeguards to block obscene content, it does not mandate tracking of users' online behavior.[27] It is important for the Commission to consider the unique privacy needs of students. For instance, LGBTQ+ students may require protection from discriminatory monitoring of their online activity by schools. Similarly, the Commission should not permit schools or libraries to use CIPA as a justification to intrude into student searches for information on reproductive health in a state where abortions are banned.

VI. The Pilot Program should last for three years, in one year increments, to account for changes in technology and cybersecurity challenges.

The Commission seeks comment on whether a three-year term provides sufficient data to evaluate how effective the Pilot funding is in protecting K-12 schools and libraries and their broadband networks and data, from cyberattacks and other cyber threats.[28] A model operating in one-year increments for a period of three years would more effectively reflect the nimbleness with which schools must respond to current cybersecurity threats. As one school district observed: cybersecurity challenges change too quickly, and data will degrade with a longer program.[29] Additionally, as technology becomes increasingly integrated into classrooms and

[26] *See* Notice of Proposed Rulemaking, *In re* Addressing the Homework Gap Through the E-Rate Program, WC Dkt. No. 21-31 at ¶ 58 (Rel. Nov. 8, 2023), https://docs.fcc.gov/public/attachments/FCC-23-91A1.pdf.
[27] *See* EPIC Homework Gap Reply Comment at 5-8.
[28] *See* NPRM at ¶ 16.
[29] *See* Comment of Clear Creek Amana CSD, WC Dkt. No. 23-234 (Nov. 22, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1122020917203.

libraries, cybersecurity risks expand in turn. For example, the emergence of remote learning during the pandemic paved the way for novel cyber incidents, including "Zoom bombing."[30]

VII. Conclusion

EPIC commends the Commission for taking action to ensure cybersecurity in K-12 schools and public libraries. We urge the Commission to define eligible support through general criteria rather than specific technologies, promote inclusivity by involving a diverse range of entities from the E-Rate Program in the Pilot Program, recognize that cybersecurity and privacy are complementary goals, ensure safeguards for student privacy where CIPA applies, and implement the Pilot Program for a year to accommodate technological changes.

Respectfully submitted, this the 27th day of February 2024, by:

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

Chloe Le
Spring Intern
Electronic Privacy Information Center
Georgetown University Law Center

[30] *See* Harvard University, *What is Zoom Bombing*, https://projects.iq.harvard.edu/user-services/faq/what-zoom-bombing; *see also* Hugh Taylor, *Risks on the Rise: Why K-12 Cybersecurity is More Important Than Ever*, https://preyproject.com/blog/cybersecurity-risks-k12-schools (Oct. 2, 2023) (discussing email invasion).