CENTER FOR DEMOCRACY & TECHNOLOGY

February 17, 2022

Via ECFS.

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: *Report on the Future of the Universal Service Fund*, WC Docket No. 21-476

Dear Ms. Dortch:

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the Notice of Inquiry issued by the Federal Communication Commission, seeking public comment on the future of the Universal Service Fund (USF).[1] CDT is a nonprofit advocacy organization that champions civil rights and civil liberties in the digital age. Building on its 25-year history, CDT is committed to advancing these goals by shaping technology policy and architecture, including in education. CDT's Equity in Civic Technology Project engages with educators, school administrators, and policymakers at all levels to ensure that schools can best serve families and their students while also protecting their privacy.

CDT applauds the efforts of the Commission to close the homework gap and bridge the digital divide and offers these comments on how to connect students and families while protecting their privacy. The USF provides critical resources to connect students learning from home to their lessons and to help make broadband affordable for low-income families. However, a failure to garner students' and families' trust by protecting students' privacy can chill participation and hamper the USF's effectiveness. The pandemic has accelerated existing trends in education technology that exacerbate risks to student privacy and the security of their data. At the beginning of the semester, schools reopened their doors and students returned to classrooms, but educators were quickly confronted with the hard reality that the pandemic is not over. Surges of Covid-19 cases have prompted classes and

[1] *Report on the Future of the Universal Service Fund*, WC Docket No. 21-476, Notice of Inquiry, FCC 21-127 (2021).

even entire schools to cancel in-person classes and once again switch to remote learning.[2] In many cases, remote learning infrastructure developed during the 2020-2021 school year was no longer in place.[3] Even beyond Covid-19 outbreaks, extreme weather events such as hurricanes, wildfires, or flooding have been forcing schools to close for days at a time, necessitating schools' use of remote learning strategies.

The past year has given schools unprecedented experience with online learning, and the ongoing pandemic continues to clearly demonstrate the continuing need for these kinds of technologies. However, as schools continue to rely on remote learning technology, student privacy remains at risk, including through the use of student activity monitoring software and escalating cybersecurity risks. To help schools, families, and student navigate those risks, the Commission should:

- Clarify that the monitoring requirement of the Children's Internet Protection Act does not require schools to engage in pervasive tracking of students' online activity.
- Expand flexible USF support for mitigating increasing cybersecurity threats posed to schools.

I. The Commission Should Clarify the Monitoring Requirement of the Children's Internet Protection Act to Ensure that Students Are Not Subject to Unnecessary Invasions of Their Privacy

As CDT has previously urged,[4] the Commission should clarify that the "monitoring" requirement of the Children's Internet Protection Act (CIPA)[5] does not require students who benefit from Commission programs to sacrifice their privacy to connect to online resources. CIPA's requirements apply to schools that receive funds under the Commission's E-Rate and Emergency Connectivity Fund programs. Recent research by CDT indicates that schools are implementing invasive software to

[2] *E.g.*, Maggie Astor, *'Insurmountable': Parents Grapple With Omicron's Upending Force in Schools*, N.Y. Times (Jan. 5, 2022), https://www.nytimes.com/2022/01/04/us/school-closing-omicron-covid.html; Ray Sanchez, *States Sound Alarm Over Covid-19 Outbreaks Among School Kids*, CNN (Sept. 15, 2021), https://www.cnn.com/2021/09/15/us/covid-school-children-outbreaks/index.html.
[3] Danielle Abril, *Back in the Classroom, Teachers Are Finding Pandemic Tech Has Changed Their Jobs Forever*, Wash. Post (Oct. 1, 2021), https://www.washingtonpost.com/technology/2021/10/01/virtual-teaching-hybrid-learning-coronavirus/.
[4] *Establishing Emergency Connectivity Fund to Close the Homework Gap*, WC Docket No. 21-93, Notice of *Ex Parte* of the Center for Democracy & Technology (filed Nov. 8, 2021), *available at* https://www.fcc.gov/ecfs/filing/110841407570; *Establishing Emergency Connectivity Fund to Close the Homework Gap*, WC Docket No. 21-93, CDT Comments at 2-9 (filed Apr. 5, 2021), *available at* https://www.fcc.gov/ecfs/filing/1040520868433.
[5] 47 U.S.C. § 254(h)(5)(B); 47 CFR § 54.520(c)(1)(i).

monitor students' activity online, often as a result of an overbroad interpretation of CIPA's "monitoring" requirement, with a disproportionate impact on lower-income and historically marginalized groups of students and families.[6]

With the advent of new technologies and the expansion of remote learning, schools have increasingly deployed technically sophisticated means of monitoring students' online activity.[7] Student activity monitoring software includes any technology that collects data on individual students such as apps that scan students' Gmail messages or software on school-issued devices and allow for real-time monitoring of students. It permits schools unprecedented glimpses into students' lives, from analyzing students' browsing habits to scanning their messages and documents to viewing or listening to activities in the home.[8] Overbroad, systematic monitoring of online activity can reveal sensitive information about students' personal lives, such as their sexual orientation, or cause a chilling effect on their free expression, political organizing, or discussion of sensitive issues such as mental health. Among other things, CDT's recent research showed:

- **Monitoring is widespread and used outside school hours.** In polling research conducted by CDT, 81 percent of teachers reported that their schools use student activity monitoring software.[9] Of those teachers, only one in four reported that monitoring is limited to school hours.[10] Seventy-one percent report that monitoring takes place on school-issued devices, while only 16 percent stated that monitoring also occurs on personal devices.[11]

- **Monitoring disproportionately affects low-income students.** In interviews with CDT, technology leaders in school districts with wealthier student populations reported that their students are more likely to have access to personal devices, which are subject to less monitoring than

[6] Center for Democracy & Technology, Student Activity Monitoring Software: Research Insights and Recommendations 2 (2021), *available at* https://cdt.org/insights/student-activity-monitoring-software-research-insights-and-recommendations; DeVan L. Hankerson et al., Center for Democracy & Technology, Online and Observed 10-11 (2021), *available at* https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software.
[7] Dian Schaffhauser, *K–12 Data Privacy During a Pandemic*, T.H.E. Journal (Sept. 10, 2020), https://thejournal.com/Articles/2020/09/10/K12-Data-Privacy-During-a-Pandemic.aspx.
[8] *See* Sidney Fussell, *Borrowed a School Laptop? Mind Your Open Tabs*, Wired (Oct. 7, 2021), https://www.wired.com/story/borrowed-school-laptop-mind-open-tabs; Mark Keierleber, *An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning*, The 74 (Sept. 14, 2021), https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning.
[9] CDT, Student Activity Monitoring Software, *supra* note 6, at 2.
[10] *Id.*
[11] *Id.*

school-issued devices.[12] In its polling research, CDT found that approximately two-thirds of rural, low-income, Hispanic, and African American students rely on school-issued devices and may consequently be disproportionately subject to student activity monitoring.[13]

- **Monitoring chills student expression.** Six in ten students in CDT's polls agreed with the statement, "I do not share my true thoughts or ideas because I know what I do online is being monitored," and 80 percent report being "more careful about what I search online when I know what I do online is being monitored."[14]

- **Parents and teachers are concerned about monitoring.** Although approximately two-thirds of teachers and parents believe that the benefits of student activity monitoring software outweigh its risks, they nonetheless have concerns about its use. Forty-seven percent of teachers and 51 percent of parents report concerns with monitoring software, such as the risk that LGBTQ+ students may be outed.[15] Fifty-seven percent of teachers and 61 percent of parents were concerned that student activity monitoring could cause "long-term harm to students" if it is used for discipline or out of context.[16]

CIPA's "monitoring" provision may be motivating overbroad surveillance of students' lives. In interviews with CDT, school district technology leaders reported that they have adopted monitoring software to comply with CIPA's perceived requirements.[17] CIPA, however, does not require invasive surveillance of students, and the Commission has the authority to clarify its interpretation. The law does not define the term "monitoring" but instead includes an express "disclaimer" that "[n]othing" in the statute "shall be construed to require the tracking of Internet use by any identifiable minor or adult user."[18]

---

[12] Hankerson et al., *supra* note 6, at 10-11.
[13] CDT, Research Slides: Key Views Toward Edtech, School Data, and Student Privacy 48 (2021), *available at* https://cdt.org/insights/report-navigating-the-new-normal-ensuring-equitable-and-trustworthy-edtech-for-the-future/.
[14] CDT, Student Activity Monitoring Software, *supra* note 6, at 4.
[15] *Id.*
[16] *Id.*; *see* Mark Keierleber, *Don't Get Gaggled*, The 74 (Oct. 18, 2020), https://www.the74million.org/article/dont-get-gaggled-minneapolis-school-district-spends-big-on-student-surveillance-tool-raising-ire-after-terminating- its-police-contract.
[17] Hankerson et al., *supra* note 6, at 11-12; *see* Mark Keierleber, *Minneapolis School District Addresses Parent Outrage Over New Digital Surveillance Tool as Students Learn Remotely*, The 74 (Oct. 28, 2020), https://www.the74million.org/minneapolis-school-district-addresses-parent-outrage-over-new-digital-surveillance-tool-as-students-learn-remotely.
[18] Consolidated Appropriations Act, 2001, Pub. L. 106–554, app. D, div. B, title XVII, sec. 1702(b), 114 Stat. 2763, 2763A–336 (2000), *available at* https://www.congress.gov/bill/106th-congress/house-bill/4577; 47 U.S.C. § 254 Note. As suggested by contemporaneous reports, "tracking" includes the gathering of data from activity online and connecting it with other data to make inferences about the user. See Federal Trade Commission, Online Profiling: A Report to Congress 3-6 (2000), *available at*

Given the harms caused by student activity monitoring software and Congress's intent that "monitoring" not entail the tracking of students, CDT urges the Commission to clarify that "monitoring" is narrow and limited to the minimal amount of data collection needed to achieve CIPA's goals, both on- and off-campus. For example, schools may limit the data they obtain by collecting only aggregate information whenever possible and minimizing where and when monitoring is occurring, such as by monitoring aggregate traffic on the school network, rather than over individual devices.

II. Cybersecurity Risks Pose an Increasing Threat to Schools, and the Commission Should Expand Flexible USF Support for Cybersecurity Mitigation

The number of cyberattacks against schools was on the rise before the onset of the 2020 pandemic, and the shift to remote learning forced by Covid-19 only exacerbated the problem due to schools' increased reliance on technology and remote learning tools.[19] According to the K-12 Cybersecurity Resource Center, "[T]he 2020 calendar year saw a record-breaking number of publicly-disclosed school cyber incidents," including district and vendor security breaches, ransomware, denial of service attacks, and invasions of online learning, meetings, and school email systems.[20] These attacks have interrupted both remote and in-person learning.[21] As schools have integrated technology more deeply into their operations, these types of attacks have caused increasingly significant disruptions, including by robbing students of valuable learning time. Even in those cases where districts are able to keep classes running, attacks put student privacy and financial wellbeing at risk,[22] and the

https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf.

[19] David Uberti, *Hackers Smell Blood as Schools Grapple With Virtual Instruction*, Wall St. Journal (Oct. 19, 2020), https://www.wsj.com/articles/hackers-smell-blood-as-schools-grapple-with-virtual-instruction-11603099802.

[20] Douglas Levin, K-12 Cybersecurity Resource Center, The State of K-12 Cybersecurity: 2020 Year in Review (2021), *available at* https://k12cybersecure.com/year-in-review/.

[21] *E.g.*, Karl Wehmhoener, *Eldon School District Canceled Classes Tuesday Due to Ransomware Attack*, KMIZ (Dec. 7, 2021), https://abc17news.com/news/2021/12/07/eldon-school-district-cancels-classes-due-to-ransomware/; Sarah Plake & Katelyn Brown, *Park Hill Schools Closed Monday, Tuesday Due to Malware Attack*, KSHB (Mar. 22, 2021), https://www.kshb.com/news/local-news/park-hill-schools-closed-monday-due-to-malware-attack; *Buffalo Public Schools Cancels Classes After Cyberattack*, Security Magazine (Mar. 16, 2021), https://www.securitymagazine.com/articles/94827-buffalo-public-schools-cancels-classes-after-cyberattack.

[22] *See, e.g.*, Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 13 (2020), *available at* https://www.gao.gov/products/gao-20-644; Joe Heim, *Hackers Post Stolen Information from Fairfax School District*, Wash. Post (Oct. 10, 2020), https://www.washingtonpost.com/local/education/hackers-post-stolen-information-from-fairfax-school-district/2020/10/10/edf5f050-0b1a-11eb-859b-f9c27abe638d_story.html.

time and money spent adjusting lesson plans to handle the loss of technology, investigating the cause of the breach, restoring systems, and performing recovery tasks pulls resources from other priorities.[23] Maintaining the security of school networks is essential to serving our students.

Neither E-Rate nor the Emergency Connectivity Fund (ECF) currently provide schools sufficient flexibility to meet escalating cybersecurity risks. Although E-Rate includes firewalls in its list of eligible services,[24] other cybersecurity measures are not eligible for support.[25] ECF support is limited to cybersecurity measures "included in the price of the connected devices," such as laptops or tablets.[26] The Wireline Competition Bureau has repeatedly determined that the Commission's previous orders prohibit it from providing schools funding to meet cybersecurity challenges,[27] and the Commission should act now to ensure that schools can provide safe and security online resources for students and families.

The Commission has authority under the Communications Act to provide cybersecurity support to schools. The Communications Act requires the Commission to "consider the extent to which telecommunications services are essential to education, public health, or public safety" in defining "universal service" and permits it to "designate additional services for [USF] support mechanisms for schools, libraries, and health care providers."[28] Under the Act, telecommunications carriers must provide the services designated by the Commission to schools "for educational purposes."[29]

---

[23] *See* Sarah Coble, *Cyber-Attack on Mississippi Schools Costs $300,000*, Infosecurity (Oct. 19, 2020), https://www.infosecurity-magazine.com/news/cyberattack-on-mississippi-schools/.

[24] *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, DA 21-1601, 9, 12 (WCB 2021) [hereinafter *FY 2021 Eligible Services List*].

[25] *E.g.*, *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Comments of Consortium for School Networking 2 (filed Sept. 27, 2021) ("The E-rate covers basic firewall services and firewall components separate from basic firewall protection when provided as a standard component of a vendor's Internet access service, but due to an outdated conception of the technology, and as implemented by the Universal Service Administrative Company (USAC), this eligible use exists in name only."); *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Comments of SHLB Coalition 3 (filed Sept. 27, 2021); *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Comments of Fortinet, Inc. 3-4 (filed Sept. 27, 2021); *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Reply Comments of Microsoft Corporation 2-3 (filed Oct. 12, 2021).

[26] Federal Communications Commission, Emergency Connectivity Fund Frequently Asked Questions Q 2.4 (2021), *available at* https://www.fcc.gov/emergency-connectivity-fund-faqs.

[27] *FY 2022 Eligible Services List* at 3, para. 8; *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, DA 18-1173, 4, para. 9 n.31 (WCB 2018)

[28] 47 U.S.C. § 254(c)(1), (3).

[29] *Id.* § 254(h)(1)(B).

Funding for cybersecurity measures meets those requirements. With school networks facing increasing cybersecurity threats, both remote and in-person learning depend on robust cybersecurity measures. Cybersecurity measures are consequently "essential for education" and serve "educational purposes."

Thus, the Commission can — and should — ensure that cybersecurity measures are eligible for E-Rate support. To permit schools flexibility in meeting both their connectivity and security needs — and to maintain reasonable spending controls — the Commission should, at minimum, expand the services included as a component of a "firewall" and allow for Category 2 support for *all* firewall-related services. Currently, Category 2 funding does not extend to "network security services" under the Wireline Competition Bureau's interpretation of the Commission's rules,[30] and the Universal Service Administrative Co. consequently requires schools to allocate the cost of firewalls, disallowing support for cybersecurity measures such as spam filtering or intrusion prevention.[31] Instead, Category 2 should cover intrusion prevention and detection, virtual private networks, distributed denial of service (DDoS) protection, and network access controls.[32] Further, because Category 2 budgets are capped,[33] expanding the scope of firewall-related services eligible under Category 2 will not impose exorbitant costs on the E-Rate program. Expanding the eligibility of firewall-related service under Category 2 will permit schools flexibility in meeting their need for safe, secure, and reliable broadband.

The Commission also should enable E-Rate support to be used to establish a more comprehensive program to meet schools' cybersecurity needs. Expanding support for firewalls under

[30] *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, DA 21-1602 at 3, para. 8 & n.20 (WCB 2021); *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, 33 FCC Rcd 11219, 11222, para. 8 n.31 (WCB 2018); *Modernizing the E-rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, 30 FCC Rcd 9923, 9925, para. 18 (WCB 2015).

[31] *Cost Allocations for Services*, Universal Service Administrative Co., https://www.usac.org/e-rate/applicant-process/before-you-begin/eligible-services-overview/cost-allocations-for-services/ (last visited Jan. 26, 2022).

[32] *See Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Petition for Declaratory Relief and Petition for Rulemaking Allowing Additional Use of E-Rate Funds for K-12 Cybersecurity of Consortium for School Networking, Alliance for Excellence in Education, State Education Technology Directors Association, Council of the Great City Schools, State E-Rate Coordinators' Alliance, Schools Health & Libraries Broadband Coalition, attachment at 9 (filed Feb. 8, 2021).

[33] *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Report & Order, 34 FCC Rcd 11219, 11224, para. 15 (2019).

Category 2 will likely be insufficient on its own to meet the cybersecurity threats schools are increasingly facing. Adequate preparation for a cybersecurity incident requires more than firewalls or services included with connected devices — it must include robust data backups, planning for restoring school computer systems, training staff, utilizing multifactor authentication, and updating systems' and devices' firmware and software.[34] The Commission should make clear that schools can use E-Rate support to establish a comprehensive cybersecurity program to meet their needs for technical infrastructure, human capital, and resources for mitigating the costs of attacks.[35]

That technical infrastructure may include anti-virus and anti-malware software, spam filtering, Domain Name System security, and multifactor authentication. Further, investment in human capital will be necessary to meet schools' cybersecurity needs: dedicated staffing, training for educators, digital literacy resources for students and families, security assessments, and consulting services. Finally, resources for mitigating the financial and human costs of attacks and breaches are an essential component of a robust response to the security threats that schools face, including lost learning time, school closings, financial risks for students and staff, and a loss of community trust. A self-standing program addressing schools' technical infrastructure, human capital, and resources, is essential to establishing a comprehensive K-12 cybersecurity response.

Conclusion

CDT supports the Commission's efforts to update the Universal Service Fund and the Fund's goals to provide equitable, accessible broadband. Broadband access should be private and secure, especially for students. The Commission should clarify that the monitoring requirement of the Children's Internet Protection Act does not require schools to engage in pervasive tracking of students'

[34] *See* Hannah Quay-de la Vallee, *Ransomware is Still Plaguing Schools: What Can They Do About It?*, Center for Democracy & Technology (Nov. 24, 2021), https://cdt.org/insights/ransomware-is-still-plaguing-schools-what-can-they-do-about-it; Consortium for School Networking et al., Petition for Declaratory Relief and Petition for Rulemaking Allowing, *supra* note 32, attachment at 9.

[35] A comprehensive cybersecurity program for schools fulfills E-Rate's requirement that eligible services be "essential for education" and serve "educational purposes" and thus is within the Commission's authority. However, to the extent the Commission believes that Congressional action is warranted, CDT encourages the Commission to recommend that Congress establish a comprehensive cybersecurity program for schools, as requested in the Notice of Inquiry. *Report on the Future of the Universal Service Fund*, WC Docket No. 21-476, Notice of Inquiry, FCC 21-127 at 20, para. 49 (2021).

online activity and expand flexible USF support for mitigating the increasing cybersecurity threats posed to schools.

Sincerely,

Elizabeth Laird
Director, Equity in Civic Technology, CDT

Cody Venzke
Senior Counsel, Equity in Civic Technology, CDT