Before the Federal Communications Commission
Washington, D.C. 20554

In the Matter of Establishing Emergency Connectivity Fund to Close the Homework Gap	WC Docket No. 21-93

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Elizabeth Laird
Cody Venzke

Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, D.C. 20005
202.637.9800

April 5, 2021

Executive Summary

The Center for Democracy & Technology (CDT) applauds the ongoing efforts of the Federal Communications Commission (Commission) and Congress to close the homework gap. As part of its twenty-five year history advocating to advance civil rights and protect civil liberties in the digital age, CDT works to ensure that schools and educators are able to use technology and data to support students while protecting their privacy. CDT submits these comments to encourage the Commission to address two issues to protect student privacy in closing the homework gap:

- the Commission should clarify the meaning of the "monitoring" requirement under the Children's Internet Protection Act (CIPA) and distinguish it from "tracking"; and,
- the Commission should adopt an approach to funding, documentation, and audits that relies on aggregate rather than individual student data to both protect student privacy and ensure use of reliable data.

First, under CIPA, schools are required to "monitor[] the online activities of minors." That requirement is not defined and raises significant privacy concerns, which would be exacerbated if it were applied to devices and services used off-campus. Thus, if the Commission determines that CIPA does apply to devices and services funded through the Emergency Connectivity Fund, it should clarify the meaning of the monitoring requirement.

Schools have adopted overly broad, invasive means of surveillance, purportedly to fulfill CIPA's requirements. That surveillance occurs at all levels of students' online experience, including on school-issued devices, on school networks, through web apps, and even by "force installing" browser extensions. This surveillance has harmed students through:

- wasted resources spent on surveillance technologies that far exceed CIPA's requirements,
- invasion of student privacy and loss of trust in schools as stewards of student data,
- the overcollection and potential misuse of data, and
- increased inequities for over-surveilled populations such as students of color, LGBTQ+ students, and low-income students.

These harms would be increased to the extent that monitoring were to occur in students' homes. For example, some schools have accessed device cameras and microphones, which in an off-campus context could lead to monitoring of family conversations and activities.

To address those harms, the Commission should clarify that the "monitoring" requirement under CIPA may be satisfied by the community-centered, non-technical approach envisioned by Congress and should be limited to only the minimal data access and collection needed to achieve the statute's requirements.

Second, the Commission should ensure that its funding, documentation, and audit requirements are protective of student privacy and effective at reducing waste, fraud, and abuse by relying on aggregate rather than individual-level data. The Family Educational Rights and Privacy Act restricts the sharing of students' names and addresses, and schools may face legal obstacles in sharing that information with external auditors. That sharing also raises ethical and administrative obstacles in obtaining meaningful, non-coerced parental consent. Moreover, it will be difficult for schools to collect reliable individual data due to various factors including the significant percentage of students from vulnerable populations who change schools each year. Given these challenges, the Commission should adopt funding, documentation, and audit procedures that are based on school- or district-level aggregate data, such as those currently in place under E-Rate.

Table of Contents

Introduction

On March 16, 2021, the Wireline Competition Bureau of the Federal Communications Commission (Commission) released a Public Notice[1] (Notice) seeking comment on the Emergency Connectivity Fund established by the American Rescue Plan[2] to support education connections and devices for students, staff, and educators off-campus.

The Center for Democracy & Technology (CDT) applauds the ongoing efforts of the Commission and Congress to close the homework gap and ensure that all students have equal access to broadband internet. For twenty-five years, CDT has advocated to advance civil rights and protect civil liberties in the digital age by shaping technology policy and architecture. As part of that advocacy, CDT works to ensure that schools and educators are able to use technology and data to support students while protecting their privacy.[3]

CDT submits these comments to encourage the Commission to address two issues that are central to protecting student privacy while closing the homework gap:

- first, the Commission should clarify the meaning of the "monitoring" requirement under the Children's Internet Protection Act (CIPA) and distinguish it from "tracking"; and,
- second, the Commission should adopt an approach to funding, documentation, and audits that relies on aggregate rather than individual student data to both protect student privacy and ensure use of reliable data.

[1] *Wireline Competition Bureau Seeks Comment on Emergency Connectivity Fund for Education Connections and Devices to Address the Homework Gap During the Pandemic*, WC Docket No. 21-93, Public Notice, DA 21-317 (WCB 2021) (Notice), *available at* https://www.fcc.gov/document/wcb-seeks-comment-emergency-connectivity-fund-close-homework-gap.

[2] American Rescue Plan Act, 2021, H.R. 1319, 117th Cong., tit. VII, sec. 7402 (2021) (enacted), *available at* https://www.congress.gov/bill/117th-congress/house-bill/1319/text.

[3] For more about CDT's policy priorities, please see our vision for the Biden Administration and the 117th Congress at https://cdt.org/insights/a-roadmap-for-new-white-house-congress-to-advance-civil-rights-liberties-in-the-digital-age/.

These measures are necessary to protect the privacy of students, who increasingly rely on school-supported devices and broadband connections to connect with their lessons online. Recent research by CDT shows that the percent of schools providing devices for use at home to all students increased from 30 percent prior to the pandemic to 68 percent now.[4] Additionally, 85 percent of teachers support increased online learning as part of classroom instruction even after students return to school in-person, so the urgency to close the homework gap will not subside when students return to school in-person.[5] With increasing numbers of students using school-supported devices and connections, it is important that students be able to access remote learning and resources online safely and privately.

I. The Commission Should Clarify the Meaning of "Monitoring" Under CIPA and Reiterate the Distinction with "Tracking"

The Children's Internet Protection Act "prohibits schools and libraries participating in the E-Rate program from receiving E-Rate funding . . . unless they comply with, and certify their compliance with, specific Internet safety requirements."[6] The Notice seeks comment "on whether the CIPA requirements extend to all school or library devices supported by funding through the Emergency Connectivity Fund that are used off-campus and outside the traditional E-Rate-supported networks."[7]

One of CIPA's requirements is that schools "monitor[] the online activities of minors."[8] That requirement raises significant privacy concerns, which would be exacerbated if it were applied to devices and services used off-campus. Thus, if the Commission determines that CIPA

[4] Elizabeth Laird & Hugh Grant-Chapman, Center for Democracy & Technology, *Research Report: With Increased EdTech Comes Increased Responsibility* 26 (2021), available at https://cdt.org/insights/research-report-with-increased-edtech-comes-increased-responsibility (see research slides).
[5] *Id.* at 5, 7.
[6] Notice at 14.
[7] Notice at 15.
[8] 47 U.S.C. § 254(h)(5)(B)(i).

does apply to devices and services funded through the Emergency Connectivity Fund, it should clarify that the monitoring required by CIPA is narrow, community-centered, and limited to the minimal amount of data collection needed to achieve CIPA's goals, both on- and off-campus. At minimum, the Commission should reiterate CIPA's "disclaimer" that "[n]othing" in the statute "shall be construed to require the tracking of Internet use by any identifiable minor or adult user."[9]

CIPA's "monitoring" requirement is not defined, which has resulted in schools adopting overly broad, invasive means of surveillance. Moreover, schools have implemented these surveillance tools at all levels of students' online experience, including on school-issued devices, on school networks, through web apps, and even by "force installing"[10] browser extensions. This invasive surveillance has harmed students in multiple ways:

- **Wasted resources and deterrent to use of funding**. The use of monitoring and surveillance software redirects schools' limited funds away from other priorities. Some school officials have stated that they believe invasive surveillance is required by CIPA.[11] However, the Commission has long maintained that Commission funds may not be used for compliance with CIPA's requirements.[12] If schools believe that the expenses for invasive software is required by CIPA,[13] they may be chilled from taking advantage of

[9] 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.
[10] *Initial Deployment of the GoGuardian Extensions*, GoGuardian, https://help.goguardian.com/hc/en-us/articles/360019263771-Installing-GoGuardian-Extensions-for-All-Products-Super-User- (last visited Mar. 30, 2021).
[11] 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.
[12] *Federal-State Joint Board on Universal Service, Children's Internet Protection Act*, CC Docket No. 96-45, Report and Order, 16 FCC Rcd 8182, 8204, paras. 54-55 (2001); *accord Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, 35 FCC Rcd 13793, 13795-96, para. 8 n.20 (WCB 2020).
[13] Keierleber, *Parent Outrage*, *supra* note 11.

support offered by the Commission. For example, in Minneapolis, schools spent $355,000 for an algorithm-driven surveillance tool that scans "student emails, chat messages and files."[14]

- **Invasion of privacy and loss of trust**. In Chicago, schools have deployed software that permits teachers to see what students have open on their computer screens, to open websites on a student's laptop, switch tabs, block sites, view browsing histories, and remotely start a Google Meet video session.[15] Invasive or unexpected monitoring can invade students' privacy, discourage them from using the provided devices, and jeopardize public trust in institutions such as schools that are stewards of student data.[16]
- **Overcollection and misuse of data, including in students' homes**. Overcollection of data can increase risks that the data will be used out of context or disclosed in a data breach.[17] Overcollection can occur through overbroad surveillance. For example, one study found that a majority of school districts in one state "retained the right to monitor the data and content of a school-loaned device without limitation" and permitted officials remote access to the devices' cameras and microphones.[18] Clearly, school officials should not be in a position to hear family conversations or see video of activities in the home. Again, the possibility that school officials may have such access will discourage students and their parents from using the devices for their intended educational purposes.

---

[14] Mark Keierleber, *'Don't Get Gaggled': Minneapolis School District Spends Big on Student Surveillance Tool, Raising Ire After Terminating Its Police Contract*, The 74 (Oct. 18, 2020)

[15] Nader Issa, *CPS Teachers Could Look Inside Students' Homes — Without Their Knowledge — Before Fix*, Chicago Sun-Times (Oct 5, 2020), https://chicago.suntimes.com/education/2020/10/5/21497946/cps-public-schools-go-guardian-technology-privacy-remote-learning.

[16] Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Data Ethics in Education & The Social Sector* 8 (2021), *available at* https://cdt.org/insights/report-data-ethics-in-education-and-the-social-sector-what-does-it-mean-and-why-does-it-matter/.

[17] *Id.* at 9.

[18] Hannah Stern, ACLU of Rhode Island, *Zooming in on Students* 9-11 (2020), *available at* https://riaclu.org/en/news/aclu-report-shows-alarming-lack-privacy-protections-students-engaged-remote-learning.

- **Increased inequities.** Marginalized student populations can be subjected to disproportionate surveillance, due to biases in data or algorithms used to monitor students, power dynamics between schools and students, or a lack of training on the proper uses and limitations of monitoring tools[19]:
    - For example, certain scanning algorithms disproportionately flag words relating to LGBTQ+ students' experiences as problematic,[20] and social media monitoring employed by some schools has been demonstrated to disproportionately flag posts by students of color for review.[21]
    - Likewise, monitoring software installed on school-issued devices may specifically surveil students who depend on those devices for remote learning,[22] especially students of color, who are more likely to be engaged in full-time remote learning.[23]

Although administrators may have good intentions to protect student safety or curb cyberbullying, there is little evidence supporting the effectiveness of these technologies, and they are disproportionately directed toward already over-surveilled populations.[24] Even if the technologies' benefits could be demonstrated, administrators must ensure the students' privacy is protected, particularly when devices are intended to be used at home or other non-school locations.

To avoid such unwarranted privacy intrusions, disproportionate surveillance, and inequitable use of public funds, the Commission should clarify that the "monitoring"

---

[19] *See* Laird & Quay-de la Vallee, *Data Ethics*, *supra* note 16, at 11-12, 14, 22.
[20] Keierleber, *Don't Get Gaggled*, *supra* note 14.
[21] Brennan Center for Justice & Center for Democracy & Technology, *Social Media Monitoring in Schools* 3 (2019), *available at* https://cdt.org/insights/social-media-monitoring-in-k-12-schools-civil-and-human-rights-concerns.
[22] *See* ACLU of Rhode Island, *Zooming in on Students*, *supra* note 18.
[23] Institute of Education Statistics, *Monthly Schools Survey Dashboard*, U.S. Department of Education, https://ies.ed.gov/schoolsurvey/ (last visited Mar. 30, 2021).
[24] Brennan Center & CDT, *Social Media Monitoring*, *supra* note 21, at 1-2.

requirement under CIPA may be satisfied by the community-centered, non-technical approach envisioned by Congress and should be limited to only the minimal data access and collection needed to achieve the statute's requirements.[25]

In passing CIPA, Congress envisioned a community-centered, non-technical approach to "monitoring" and coaching. Community engagement plays a central role in CIPA's requirements,[26] and Senator Rick Santorum, the author of some of CIPA's provisions, described the statute as requiring that "there be a community effort put together for the community to get involved and make the decision."[27] Similarly, Senator Patrick Leahy envisioned that "many schools and libraries put their screens in the main reading room. One has to assume not too many kids are going to go pulling up inappropriate things on the web sites when their teachers, their parents, and everybody else are walking back and forth and looking over their shoulder saying: What are you looking at?"[28]

Engaging parents and the community is even more vital when students are learning from their homes. As the Supreme Court has observed, "the very core" of the personal rights secured by the Constitution is the right for a person "to retreat into his own home and there be free from unreasonable governmental intrusion."[29] The privacy concerns around monitoring online activities are heightened when students are off-campus, particularly if students, and potentially

[25] CDT does not concede that CIPA's blocking or filtering requirements under 47 U.S.C. § 254(h) and (l) are constitutional as applied to schools or as applied to users at locations other than a school or library. *Cf.* United States v. American Library Ass'n, 539 U.S. 194, 209 (2003) (plurality opinion) (upholding CIPA's filtering requirement for internet access provided at public libraries, because libraries can disable filtering software upon request by adult patrons). CIPA's filtering and blocking requirements chill the expressive activities of minors and block minors' and adults' constitutionally protected access to information. *Id.* at 222 (Stevens, J., dissenting) ("In my judgment, a statutory blunderbuss that mandates this vast amount of 'overblocking' abridges the freedom of speech protected by the First Amendment.").

[26] 47 U.S.C. § 254(h)(5)(A)(iii) (requiring public notice and a public hearing in developing an Internet safety policy).

[27] 146 Cong. Rec S5823-45 (daily ed. June 27, 2000) (statement of Sen. Santorum), available at https://www.congress.gov/congressional-record/2000/06/27/senate-section/article/S5823-8.

[28] *Id.* (statement of Sen. Leahy).

[29] Silverman v. United States, 365 U.S. 505, 511 (1961); *accord* Griswold v. Connecticut, 381 U.S. 479 (1965).

other members of the household, use the provided devices and connectivity for incidental personal use. Although the Commission should clarify the narrow scope of "monitoring" under CIPA under all circumstances, that clarification is even more important in an age of remote learning, given the special consideration given to privacy in the home.

The Commission should clarify that schools may fulfill CIPA's requirements by minimizing the collection of sensitive information about students and increasing the reliance on non-technical tools that might be more effective and less intrusive:

- **Minimize the collection of sensitive information**. Schools should collect only aggregate information whenever possible, such as trend analysis of security threats or identification of problematic sites that are being accessed by multiple students. Schools should also minimize where monitoring is occurring, such as by monitoring aggregate traffic on the school network, rather than over individual devices, to identify unauthorized access or activity.[30] Further, schools should not be permitted to enable and monitor device cameras and microphones, which foreseeably would capture private family conversations and activities inside the home.
- **Increase reliance on non-technical tools**. The Commission should clarify that schools should employ non-technical methods of "monitoring" minors' online activities to the greatest extent possible, especially when students are learning largely off-campus and from home. Instead of scanning students' messages or actively monitoring their open applications or browser tabs, schools should engage parents and community members to

[30] Cybersecurity & Infrastructure Security Agency (CISA), *Ransomware Guide* 5 (2020), *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf; Readiness and Emergency Management for Schools Technical Assistance Center (REMS TAC), U.S. Department of Education, *Cybersecurity Considerations for K-12 Schools and School Districts* at 3 ("To protect their networks and systems as part of overall preparedness program, schools and school districts can . . . [m]onitor network continually to assess the risk from cyber threats.")

monitor students' online activities and coach them on digital literacy and online citizenship. The Commission should likewise consider providing schools and households with resources on cybersecurity and digital literacy to navigate the online world. Some resources already exist and have been provided by governmental and nonprofit entities as well as public-private partnerships.[31]

The Commission also should reiterate that CIPA's monitoring requirement does not entail "tracking" students and distinguish "monitoring" and "tracking." CIPA was passed as part of the Consolidated Appropriations Act, 2001. The Consolidated Appropriation Act expressly provides a "disclaimer" that "[n]othing" in the statute "shall be construed to require the tracking of Internet use by any identifiable minor or adult user."[32] As suggested by contemporaneous reports, "tracking" includes the gathering of data derived from activity online, is often associated with identifiers, and may be later connected with other data and analyzed to infer information about the user.[33]

CIPA was passed twenty years ago, well before the proliferation of automated student monitoring algorithms and software, and was designed for school computers hardwired to school networks.[34] It does not require invasive surveillance of students' online lives. Clarifying the statute's "monitoring" provision will help protect student privacy and address the effects of

---

[31] *E.g.*, *Addressing Adversarial and Human-Caused Threats That May Impact Students, Staff, and Visitors*, REMS TAC, https://rems.ed.gov/Resources_Hazards-Threats_Adversarial_Threats.aspx (last visited Mar. 30, 20210; *OnGuard Online*, Federal Trade Commission, https://www.consumer.ftc.gov/features/feature-0038-onguardonline (last visited Jan. 11, 2021); *Digital Citizenship Curriculum*, Common Sense, https://www.commonsense.org/education/digital-citizenship/curriculum (last visited Jan. 11, 2021); *STOP. THINK. CONNECT.*, stopthinkconnect.org (last visited Jan. 11, 2021).

[32] 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.

[33] *See* Federal Trade Commission, Online Profiling: A Report to Congress 3-6 (2000), *available at* https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf.

[34] Keierleber, *Parent Outrage*, supra note 11.

surveillance that fall disproportionately on marginalized students. The Commission should clarify the narrow scope of that requirement for schools.

II. The Commission Should Rely on Aggregate Data for Funding, Documentation, and Audit Purposes to Both Protect Student Privacy and Ensure Reliable Data

The Notice also seeks public comment on whether the Commission should "require that schools document the student(s) and staff member served at each supported location"[35] and provide that documentation in connection with any audit conducted by the Universal Service Administrative Co. (USAC).[36] The Commission should instead use aggregate data in lieu of personally identifiable information in its funding decisions and for its documentation and audit requirements to both protect student privacy and ensure reliable data for reducing waste, fraud, and abuse.

As described below, requiring schools to provide individual-level student information to external auditors may pose legal and ethical obstacles for schools seeking to protect student privacy. Moreover, such data is unlikely to be reliable. In light of those challenges, the Commission should adopt funding and audit procedures that are based on school- or district-level aggregate data. Similar processes are already in place for funding under E-Rate, which take into account the number of students enrolled in the district, the percent of students eligible for the National School Lunch Program, and status as a rural or urban district.[37] The Commission should establish similar, aggregate-level procedures for funding schools and audits under the Emergency Connectivity Fund.

[35] Notice at 8.
[36] Notice at 17.
[37] *See Calculating Discounts*, USAC, https://www.usac.org/e-rate/applicant-process/applying-for-discounts/calculating-discounts/ (last visited Mar. 30, 2021).

A. Documentation and Audit Requirements That Require Sharing Individual Student Data with External Auditors May Pose Legal and Ethical Challenges for Schools

Schools would face legal obstacles to sharing individual student information with third parties, including the Commission and USAC auditors. In particular, federal and state law provide privacy protections for students' personally identifiable information.[38] At the federal level, the Family Educational Rights and Privacy Act (FERPA) is the primary law governing student privacy.[39] FERPA generally prohibits the disclosure of students' "personally identifiable information" (PII) without parents' consent, unless a statutory or regulatory exception to the consent requirement applies.[40] Under FERPA, PII includes any information that "is linked or linkable to a specific student," including, expressly, a student's address.[41]

Consequently, the Notice's proposed documentation and audit requirements[42] may implicate FERPA's protections to the extent the Notice envisions disclosing student-level data to entities that are outside of the schools, including the Commission and USAC.[43] Although FERPA contains exceptions to the prohibition on sharing student data without parental consent, neither of the two most relevant exceptions are likely to apply here:

- **Directory Information Exception**. "Directory information" is student data that, if released, would generally be considered harmless and could include a student's name and

[38] There are currently approximately 130 state laws related to student privacy. *See State Student Privacy Laws*, Student Privacy Compass, https://studentprivacycompass.org/state-laws/ (last visited Mar. 29, 2021). Although we will not be addressing state laws in these comments, schools must still comply with them in meeting the Commission's documentation and audit requirements.

[39] Other laws such as the Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h, and the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06, may apply as well.

[40] 34 C.F.R. § 99.30.

[41] 34 C.F.R. § 99.3.

[42] *E.g.*, Notice at 16 ("[W]e also propose to require applicants to maintain a record of the service address for the broadband service and the actual installation date of service.").

[43] Schools' collection and retention of data for internal tracking or audits does not generally implicate FERPA's requirements, but schools should still consider limitations imposed by other federal laws, state law, and best practices for collecting and storing data.

address.[44] However, this information may be disclosed without parental consent only if (1) the school has provided notice to parents of the PII it has designated as directory information, and (2) parents have not opted out of its disclosure.[45] Given these two requirements, USAC would be unlikely to receive complete individual-level student data from schools, thus undercutting its ability to rely on that data for purposes of auditing and preventing fraud and waste. Additionally, disclosure of addresses could go beyond the scope of the directory information exception if it is expressly or implicitly understood to be limited to students who lack broadband access. For example, if schools only share the addresses of students participating in the Emergency Connectivity Fund, then recipients may be able to infer students' participation in the Fund and lack of broadband access at home. Addresses that are expressly or implicitly tied to students' participation in the Fund may not qualify as directory information.

- **Audit or Evaluation Exception**. FERPA's "audit or evaluation" exception[46] is limited to disclosures to state and educational authorities, the Comptroller General, the Attorney General, or the Secretary of Education for the evaluation of an educational program.[47] USAC and the Commission are not on the list of permissible recipients.

Because the exceptions described above do not appear to allow schools to share personally identifiable information for purposes of limiting fraud and waste, the only available mechanism under FERPA to share this information would be parental consent. Requiring schools

[44] 34 C.F.R. § 99.3 ("Directory information includes, but is not limited to, the student's name; address . . . ."); *see also* Student Privacy Policy Office, U.S. Department of Education, *Model Notice for Directory Information* (2011), *available at* https://studentprivacy.ed.gov/node/428 (designating name and address, among other things, as directory information).
[45] *Id.* § 99.37(a)-(b).
[46] *Id.* § 99.35.
[47] *Id.* § 99.31(a)(3).

to obtain parental consent to share student information with USAC or another external auditor would pose a variety of administrative obstacles and add to schools' burdens at a time of significant challenge.

Moreover, consent alone is insufficient to protect student privacy.[48] There are important challenges to obtaining informed, meaningful consent, including whether the user really reads and understands the ways their data may be used, and whether the user feels they have a meaningful, non-coerced choice.[49] Parents forced to decide between their student receiving educational services through a school-issued device or internet connection and not disclosing information about their family for unclear purposes without use or retention limitations may not have a meaningful choice. Students are also concerned about their addresses being shared, as middle and high school students expressed discomfort with disclosure of their home addresses in focus groups that CDT conducted last summer.[50]

B. Individual-Level Data May Not Be Sufficiently Reliable

Outside of FERPA's legal requirements, using individual level data may be of limited value for audit purposes because of its lack of reliability. As an initial matter, many schools do not have the centralized data infrastructure or student information systems (SIS) that would be needed to collect this data. In creating a blueprint for collecting data in service of closing the homework gap, it was noted that many of the data fields, including which students have received

---

[48] *See* Center for Democracy & Technology, *Comments to the FTC on the 2019 COPPA Rule Review* 3 (2019), *available at* https://cdt.org/insights/comments-to-the-ftc-on-the-2019-coppa-rule-review/ ("Notice, consent, and transparency will always be a major pillar of U.S. privacy laws, but decision makers are increasingly proposing limitations on data use that cut across different opt-in or opt-out models."); *CDT's Federal Privacy Legislation Section-by-Section Analysis and Explanation*, Center for Democracy & Technology (Dec. 13, 2018), https://cdt.org/insights/cdts-federal-privacy-legislation-section-by-section-analysis-and-explanation/.

[49] Laird & Quay-de la Vallee, *Data Ethics*, *supra* note 16, at 15.

[50] Center for Democracy & Technology, *Research Slides: Teacher, Parent, and Student Views on Education Data, Technology, and Student Privacy*, 15 (Oct. 22, 2020), available at https://cdt.org/press/research-shows-teachers-parents-students-need-more-support-to-protect-privacy-and-advance-digital-equity/.

devices, "are not yet built into most systems—and given that SIS vendors ordinarily require significantly more lead time to develop required changes— some LEAs may not be able to utilize their SIS for managing this data in the immediate term."[51]

The collection of reliable individual data is particularly challenging as students frequently move, sometimes without notice to their existing schools, and school districts and states are not prepared to track and share this information as students change schools. In particular, students who are part of vulnerable populations — such as children of migrant workers, children experiencing homelessness, or children involved with the foster care system — are disproportionately likely to exit their school during the course of the school year. One study in Colorado suggested that 36.9 percent of migrant children, 39.8 percent of children experiencing homelessness, and 54.0 percent of children in foster care exited their school or district during the 2014-15 school year, compared to 16.5 percent overall and 6.1 percent for students labeled gifted and talented.[52] Some student mobility is involuntary, "less carefully planned," and more disruptive for students, schools, and normal transfer procedures.[53]

Thus, student mobility and other challenges present obstacles to using individual level data as a reliable basis to prevent fraud and waste. The Commission should avoid requiring the collection and sharing of information that will not meet its intended purpose of preventing fraud, waste, and abuse as it increases risks to privacy and burdens resource-strapped entities like schools.

---

[51] Council of Chief State School Officers, *Home Digital Access Data Collection: Blueprint for State Education Leaders* 5 (2020), *available at* https://digitalbridgek12.org/states/data-collection-blueprint.
[52] Colorado Department of Education, *Dropout Prevent and Student Engagement* 27 (2016), *available at* http://www.cde.state.co.us/dropoutprevention/2015dropoutpreventionpolicyreport.
[53] Russell W. Rumberger, University of California, Santa Barbara, *Student Mobility: Causes, Consequent, and Solutions* 10-11 (2015), *available at* https://files.eric.ed.gov/fulltext/ED574695.pdf.

Conclusion

To protect student privacy while ensuring they may access the benefits of an increasingly online world, the Commission should provide guidance to schools on CIPA's narrow "monitoring" provisions and strive to ensure that its funding, documentation, and auditing procedures are protective of privacy and effective for the situations facing many schools and vulnerable populations.