CENTER FOR DEMOCRACY & TECHNOLOGY

February 16, 2021

Via ECFS.

Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: Emergency Broadband Benefit Program, WC Docket No. 20-445

The Center for Democracy & Technology (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.[1] CDT's Student Privacy Project engages with educators, school administrators, and policymakers at all levels to ensure that schools can do the best for families and their students while also protecting their privacy. That engagement includes the critical issue of bridging the homework gap and closing the digital divide. CDT submits these comments to help ensure that students and families can get connected without sacrificing their privacy.

In particular, CDT seeks to address two issues regarding the proposed Emergency Broadband Benefit Program (EBBP):

1. to support suggestions that the Commission partner with schools to engage families and communities and permit schoolwide verification of EBBP eligibility based on schools' adoption of the Community Eligibility Provision (CEP) under the National School Lunch Program (NSLP); and
2. to ensure that any data sharing that occurs to enroll families in the EBBP fulfills legal requirements for student privacy and incorporates ethical data practices.

Schools and Other Institutions Should Serve as Anchors in the EBBP, and Schoolwide Eligibility Based on Adoption of the CEP Should Be Permitted

CDT supports the several commenters that urge the Commission to engage schools as anchor institutions in the EBBP.[2] Schools are likely familiar institutions to families and students and may be key to ensuring that they are aware of the EBBP's benefits. Likewise, engagement with families and

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

[2] Public Knowledge Comments at 5, *available at* https://www.fcc.gov/ecfs/filing/10126136623449; State Educational Technology Directors Association, Consortium for School Networking, Alliance for Excellent Education Comments at 3, *available at* https://www.fcc.gov/ecfs/filing/10126162270161; Common Sense Media Comments at 3, *available at* https://www.fcc.gov/ecfs/filing/10126547926608.

communities is essential to the ethical use of sensitive data like home addresses and will also be key to obtaining parental consent when necessary. Schools may help facilitate that engagement.

Similarly, CDT supports permitting schoolwide eligibility for the EBBP based on adoption of the NSLP's CEP.[3] As CDT argued in its comments in this docket,[4] CEP-based eligibility will not only ensure that students may obtain needed connections for their remote lessons, but it will obviate the need for collecting sensitive data about individual students' participation in the NSLP.

Federal Student Privacy Law and Responsible Data Practices Should Drive the Sharing of Student Information Such as Addresses

Closing the homework gap is a data-heavy exercise and may require collecting and sharing student data to identify and meet students' needs.[5] Several comments suggest that the Commission help schools and broadband providers identify students who lack internet access at home by facilitating the collection and disclosure of students' addresses.[6] Those comments recognize the importance of protecting student privacy and underscore that the sharing of student addresses must be carefully implemented to comply with both data ethics and the legal requirements for student privacy. CDT supports those comments' vision of schools facilitating enrollment and eligibility in the EBBP and shares their goal of ensuring that students and families get connected without sacrificing their privacy. CDT outlines some of the legal requirements for sharing student addresses below.

The primary federal law governing the disclosure of student information such as addresses is the Family Educational Rights and Privacy Act (FERPA).[7] FERPA prohibits the disclosure of personally identifiable information (PII) from education records without parental consent.[8] Under FERPA, PII includes any information that "is linked or linkable to a specific student that would allow a reasonable person in the school community . . . to identify the student with reasonable certainty."[9] Under FERPA's regulations, students' PII expressly includes addresses,[10] and thus disclosure of addresses requires parental consent or an exception to the consent requirement.[11]

---

[3] *See, e.g.*, EducationSuperHighway Comments at 7, *available at* https://www.fcc.gov/ecfs/filing/10119013048398; Council of the Great City Schools Comments at 3, *available at* https://www.fcc.gov/ecfs/filing/10125158501229; Wireless Internet Service Providers Comments at 10, *available at* https://www.fcc.gov/ecfs/filing/1012508002741.

[4] CDT Comments at 2-6, *available at* https://www.fcc.gov/ecfs/filing/10125234915784.

[5] *See, e.g.,* State Action to Close the Homework Gap, Digital Bridge K-12, https://digitalbridgek12.org/states/ (last visited Feb. 10, 2021); Maureen Wentworth, Leading Back to School With Digital Equity, Ed-Fi (July 9, 2020), https://www.ed-fi.org/blog/2020/07/leading-back-to-school-with-digital-equity.

[6] EducationSuperHighway Comments at 8-9; Council of the Great City Schools Comments at 3; State E-rate Coordinators' Alliance Comments at 4-5, *available at* https://www.fcc.gov/ecfs/filing/101252980328238.

[7] 20 U.S.C. § 1232g.

[8] 34 C.F.R. § 99.30(a).

[9] *Id.* § 99.3.

[10] *Id.* § 99.3, "Personally identified information."

[11] *Id.* §§ 99.30, .31.

One common exception to the consent requirement is for "directory information," including addresses; that exception, however, entails both legal and ethical requirements for schools. First, under FERPA, directory 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.[12] Thus, for a school to disclose addresses to broadband providers, it must meet those two procedural requirements.

Second, there is a risk that 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 participating in the NSLP. For example, if schools share the addresses only of students participating in the NSLP, then recipients may be able to infer students' NSLP status. Participation in the NSLP is sensitive and addresses that are expressly or implicitly tied to students' NSLP eligibility may not qualify as directory information.

Whether a specific system of disclosure meets FERPA's requirements, of course, is ultimately up to the U.S. Department of Education (Department). Other exceptions to the consent requirement, such as the School Official exception,[13] may apply as well, and guidance from the Department may prove helpful for schools, families, and broadband providers as they seek to comply with federal student privacy law.

Finally, schools and broadband providers should employ ethical data practices when sharing student information. In focus groups conducted by CDT this summer, middle and high school students expressed discomfort with disclosure of their home addresses.[14] Addresses may be combined with other information to glean insights into a person's health, sexual preferences, religion, and associations.[15] Schools can address these concerns by actively engaging with families and communities as well as entering into data sharing agreements between schools and broadband providers to ensure this information remains protected and is used responsibly—a measure for which other commenters have advocated.[16]

---

[12] *Id.* § 99.37(a)-(b).

[13] *Id.* § 99.31(a)(1)(i)(B), (a)(1)(ii); *see* Letter from Paul Gammill, Director, Family Policy Compliance Office, to Kristy Shirley, North Dakota State University (July 6, 2009), *available at* https://studentprivacy.ed.gov/resources/letter-north-dakota-state-university-regarding-ferpas-school-official-exception-july-2009.

[14] CDT, Research Slides: Teacher, Parent, and Student Views on Education Data, Technology, and Student Privacy at 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/.

[15] Stuart A. Thompson & Charlie Warzel, Twelve Million Phones, One Dataset, Zero Privacy, N.Y. Times (Dec. 19, 2019), *available at* https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[16] EducationSuperHighway Comments at 8-9; State E-rate Coordinators' Alliance Comments at 5.

CENTER FOR DEMOCRACY & TECHNOLOGY

CDT supports the Commission's efforts to connect students and families and urges the Commission to adopt measures to protect student privacy and ensure responsible data practices as an integral part of those efforts.

Sincerely,

Elizabeth Laird
Director, Equity in Civic Technology

Cody Venzke
Policy Counsel, Equity in Civic Technology

1401 K Street NW, Suite 200 Washington, DC 20005