The National Telecommunications and Information Administration's (NTIA's) Listening Session on Screen-Based Instruction in K-12 Schools collected feedback from parents, students, educators, and child development experts, to contribute to the NTIA's comment for an FCC proceeding on the E-Rate program that funds connectivity in schools. CERU research points to limitations in the effectiveness of the Children's Internet Protection Act (CIPA) in protecting students' data, and how it might be improved.

Faith Boninger Comment to National Telecommunications and Information Administration (NTIA) Listening Session on Screen-Based Instruction in K-12 Schools

September 15, 2026

My name is Faith Boninger. I am a research professor at the University of Colorado Boulder, where I study the educational and privacy impacts of the digital technologies used in schools.[1] I offer this comment as a private individual.

Ubiquity and Nature of Digital Educational Products

So-called "ed tech" products present a special threat to students because their opaque algorithms mediate between teachers and students, deliver educational content, and make educational decisions—through all of it, collecting huge amounts of sensitive data from children as they learn and grow. Children are often *required* to use these products in their state-mandated schooling. As they are in New Mexico, which explicitly forbids parents from opting out of Amira, the state's chosen AI reading program.[2]

What We Don't Know

My concerns center on the lack of adequate public oversight of ed tech products. These products and their algorithms are proprietary and we cannot under current law and policy legally access and examine them to ensure that they are capable of providing the promised services and that they do not harm their users.

As things now stand, we do not know:

How an ed tech product makes educational decisions;

If, when, or how a product may embed cultural and other biases in curriculum and assessments and in so doing harm students; or

What data the product collects from students, with whom data is shared, or to what uses data is put.

Student Data Privacy

Federal and state laws currently allow providers to "de-identify" student data, retain it, share it, and use it—in perpetuity.[3] They may use it for all sorts of commercial purposes, such as developing products that predict the capabilities, intentions, and behaviors of students from whom data is collected and others like them. Although it is impossible to verify the basis for these predictions, they can and often are used for both for academic purposes like guiding students toward different academic tracks[4] and non-academic ones like determining insurance rates[5] or the likelihood of committing a crime.[6]

The Children's Internet Protection Act (CIPA) Fails to Protect Children's Sensitive Data

The Children's Internet Protection Act (CIPA) requires schools to certify that they have adopted and are enforcing internet safety policies to address, among other things, "unauthorized access…" and "unauthorized disclosure, use, or sharing of minors' personal information." But schools don't control and can't see either the algorithms that define the ed tech products they use or the business activities of the providers of those products. Of serious concern is *authorized* access to, sharing, and use of data extracted from students as part of their state-required schooling, especially including theoretically non-personal data. Such allowed but invisible use presents a significant threat to students in particular and to the public more generally.

Notes and References

[1] For a complete list of Commercialism in Education Research Unit (CERU) research, see: https://nepc.colorado.edu/ceru-home

[2] Padilla, M.D. (2026, August 4). *Memorandum: Early Years Literacy Assessment Benchmark, Screening and Progress Monitoring Reminders*. State of New Mexico Public Education Department. Retrieved August 10, 2026, from https://s3.documentcloud.org/documents/28539968/early-literacy-assessment-guidance-reminders.pdf

[3] "The provider collects metadata about student activity, including time spent online, desktop vs. mobile access, success rates, and keystroke information. If the provider de-identifies these metadata by removing all direct and indirect identifying information about the individual students (including school and most geographic information), the provider can then use this information to develop new personalized learning products and services (unless the district's agreement with the provider precludes this use)." (p. 3)

"It is important to remember, however, that student information that has been properly de-identified or that is shared under the "directory information" exception, is not protected by FERPA, and thus is not subject to FERPA's use and re-disclosure limitations." (p. 5)

Privacy Technical Assistance Center, USDOE (2014, February). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (pp. 3, 5). Retrieved April 14, 2026, from https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

"There is nothing wrong with a provider using de-identified data for other purposes; privacy statutes, after all, govern PII, not de-identified data."

Privacy Technical Assistance Center, USDOE (2016, March). *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service.* Retrieved April 14, 2026, from https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf

[4] Barshay, J. & Aslanian, S. (2019, August 6). Under a Watchful Eye - Colleges are using big data to track students in an effort to boost graduation rates, but it comes at a cost. *APM Reports*. Retrieved September 14, 2026, from https://www.apmreports.org/episode/2019/08/06/college-data-tracking-students-graduation

[5] Maryville University (2020, October 28). *Predictive Analytics in Insurance: Types, Tools, and the Future* [blog post]. Retrieved September 14, 2026, from https://online.maryville.edu/blog/predictive-analytics-in-insurance/#tools-insurance-industry

[6] Lau, T. (2020, April 20). Predictive policing explained. Brennan Center for Justice. Retrieved September 14, 2026, from https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained