CENTER FOR DEMOCRACY & TECHNOLOGY

Unintended Consequences

Consumer Privacy Legislation and Schools

March 2024

Authored by
Hannah Quay-de la Vallee, *Senior Technologist*
Kristin Woelfel, *Policy Counsel, Equity in Civic Technology*

The United States needs to enact comprehensive privacy legislation that limits the collection, use, and sharing of personal information to protect everyone, including children. Although such a bill has yet to be enacted at the federal level, state and federal legislators have proposed, and in some states enacted, legislation that limits the ways that companies can collect and use individuals' data. Such legislation also often expands individuals' rights to access and manage data about them held by companies.[1] If not carefully crafted, however, privacy and child safety laws can inadvertently undermine the ability of schools and their vendors to carry out important educational functions.

Schools, and in turn the vendors they use (for services like managing student records and hosting educational content), have different data needs and uses than non-education private sector companies or non-profits. Quality data is required to support the core functions of schools including class assignments, transportation, nutrition, and even school funding. School operations can be actively hamstrung by an ill-suited law. Policymakers can, however, create a coherent legal regime that protects everyone's privacy and safety while ensuring seamless education operations.

---

1 *Which States Have Consumer Data Privacy Laws?*, Bloomberg Law (Nov. 27, 2023), perma.cc/Q3HS-9XBH; Alexander Borovsky, John Brigagliano, & Amanda Witt, *A U.S. Data Privacy Law Update: Data Transfers, Delayed CCPA Regulatory Enforcement, and Data Privacy Laws Galore*!, JD Supra (July 18, 2023), perma.cc/2XTW-XHBY.

Existing Data Laws for Children and Education

A complex legal regime already governs data in an education context, making it important to consider how new laws will interact with these existing frameworks. These authorities include the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), the Individuals with Disabilities Education Act (IDEA), and a host of state student privacy laws.

These laws provide specific protections for a wide range of student data and how schools and companies must handle that data. For instance, FERPA addresses schools' handling of education records and personally identifying information (PPI) of students, affording specific rights to parents to inspect and correct student records, including information maintained by vendors and third parties acting on behalf of the school.[2] IDEA addresses, among other things, special confidentiality concerns for students with disabilities and their families.[3]

Federal education privacy laws like FERPA and IDEA create a floor for student privacy that can then be supplemented by additional state laws. Many states have enacted laws that impose additional obligations on education agencies, such as creating breach notification procedures and limiting the types of information that can be collected about a student.[4] At least 128 state student privacy laws in effect today govern educational agencies and their vendors, providing an ever-widening range of additional protections to supplement federal student privacy laws.[5]

Additionally, COPPA requires parental consent prior to certain operators of websites and online services collecting data about children under the age of 13. While not technically a student privacy law, COPPA can impact edtech companies. While the Federal Trade Commission (FTC) has long been clear that COPPA does not impose obligations on schools, it limits when a school can consent on behalf of a parent, requiring companies to obtain parents' verifiable consent for any data collection that is not exclusively for educational purposes.[6]

---

2 *Responsibilities of Third-Party Service Providers under FERPA*, Privacy Technical Assistance Ctr. (Aug. 2015), perma.cc/HSM4-TD3J.

3 *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies*, Nat'l Ctr. for Educ. Statistics 17 (Mar. 2004), perma.cc/HFX6-GXF9.

4 *See* Colo. Rev. Stat. §6-1-716 (2018) (enacting sector non-specific breach notification procedures); Fla. Stat. §1002.222 (1)(a) (2023) (prohibiting the collection or retention of information regarding the political affiliation, voting history, religious affiliation, or biometric information of a student or a parent or sibling of the student).

5 Adam Stone, *Understanding FERPA, CIPA and Other K–12 Student Data Privacy Laws*, Ed Tech Magazine (Apr. 28, 2022), https://perma.cc/N5ZK-8KVS.

6 Lisa Weintraub Schifferle, *Business Blog: COPPA Guidance For Ed Tech Companies and Schools During The Coronavirus*, Fed. Trade Comm'n (April 9, 2020), perma.cc/YZD9-RC9S; *FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts*, Fed. Trade Comm'n (May 22, 2023), perma.cc/76UA-K33J.

While these frameworks are incomplete and should be improved, those improvements should be made intentionally with an eye to supporting students and school communities. These benefits are unlikely to result from bills that are targeted to other sectors but inadvertently impact education.

Inadvertent Detrimental Effects of General Privacy and Child Safety Laws on Education

Although drafters of privacy and child safety laws that are targeted at the private sector or non-education nonprofits often seek to exempt the education sector, educational institutions may end up being inadvertently covered. This oversight can impact schools' ability to provide education to their communities, whether by limiting their ability to support students, limiting their ability to obtain core data required to provide critical services, or forcing schools to spend resources complying with additional conflicting or confusing frameworks. This inadvertent coverage can happen in a number of ways:

- **Bills that do not account for vendors providing services to schools, such as a February 2022 version of the Kids Online Safety Act (KOSA 2022),[7] can require vendors to adhere to different standards for data than the school itself** (for example, a right to deletion that might obligate a company that holds an education agency's data to comply with a deletion request that the education agency itself would have the discretion to decline). Such different standards can create inconsistencies in how student data is handled and limit a school's ability to rely on their vendors to handle data as expected in an educational context. Additionally, bills without clear treatment of vendors may also create legal complexity and inconsistency for schools, as they are ultimately responsible for student data, even if it is held by vendors, which is untenable if vendors are expected to follow different regulations than the school.
- **Bills that do not account for private schools can leave those schools with a legal framework not designed for the broader educational context.** As an example, private schools may still be impacted by a bill that tries to account for education contexts by exempting any data covered by or entities subject to FERPA, because FERPA's scope is limited to schools that accept federal funding, leaving out most private K-12 schools.
- **Occasionally bills do not differentiate between private sector actors like companies and public sector actors like schools**, such as the Online Privacy Act, which would thus require schools to abide by the same consumer frameworks as private companies, which can limit their ability to provide an effective education.[8]

---

7 Kids Online Safety Act, S. 3663, 117th Cong. (2022).

8 Online Privacy Act of 2023, H.R. 2701, 118th Cong. (2023).

Legal frameworks that inadvertently cover schools or their vendors can negatively impact how schools deliver educational services. Some requirements can create legal challenges for schools, while some can more directly affect students' educational experiences.

- **Data deletion:** Many consumer data privacy laws, such as the proposed American Data Privacy Protection Act (ADPPA), give consumers the right to request or require that a "covered entity" delete any data about the consumer they hold.[9] That requirement makes sense when a consumer wants to delete, for instance, an advertising profile about themselves. It makes much less sense when a parent wants to delete their child's disciplinary history from their education record (FERPA already provides the parent the right to correct the record if they feel it is wrong).

  Consequently, these laws must be carefully drafted to ensure that schools are able to maintain their records as necessary to perform their role of educating students. ADPPA protects consumers by outlining data rights they have when data about them is held by "covered entities." ADPPA, as introduced in Congress, takes care to exempt "governmental entities," which would include schools, allowing them to maintain control of their records. However, an earlier discussion draft which does not include this exemption would have interfered with schools' record keeping requirements.[10] The updated version actually goes further than exempting schools themselves though; it also exempts people and entities that manage data on *behalf of* governmental entities like schools. This is crucial in an education context where schools rely heavily on edtech vendors in their technology ecosystems. Without this further exception, a *vendor* could be required to comply with, for instance, a parent's request to delete their child's transcripts, thus undercutting the reliability of educational records.

- **Correction:** Consumer laws sometimes give consumers the right to correct data about them. As mentioned above, FERPA protects this right as well, giving parents and students the ability to contest inaccuracies in students' educational records. However, under FERPA, a correction request typically goes through the school, and schools are able to determine whether a correction is warranted. If a consumer law is not drafted to ensure such requests go to the school, but rather enables parents and students to go directly to vendors employed by the school, it could prevent the school from determining whether the correction is valid and, if so, ensuring that the correction is done appropriately and accurately. Although many bills require the requesting consumer to prove the record is incorrect, allowing parents to request a change directly with a vendor rather than through the school could create significant confusion, or potentially allow for students to change grades or otherwise alter their academic record without the school's awareness or involvement.

---

9 American Data Privacy and Protection Act , H.R. 8152, 117th Cong. §203 (2022).

10 Discussion Draft, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

- **Profiling:** Some laws place restrictions on profiling users under a certain age, where profiling generally means using the user's past actions or other information about the user to make decisions about how to interact with or present information to the user in the future. Some of these profiling laws protect people in certain age ranges, generally under 13. Without appropriate carve outs for schools, both public and private, these restrictions could apply to many students in K-12 schools. However, some systems used by schools generate profiles of students that schools use to inform their instructional and educational practices. For example, schools may analyze data to personalize student learning in a number of ways, including allowing for individualized project-based learning or personalizing student goals.[11] Disallowing profiling would render these systems ineffective, essentially removing a tool from the toolbox of schools that are aiming to support their most at-risk students.

Students, Especially LGBTQ+, Disapprove of Increased Parental Access To Online Activity

Many recent state and federal online child safety laws propose varying levels of parental access to their children's online activities, assuming that more parental control will keep kids safer. However, though our research indicates that parents are already implementing measures to supervise what their children do online and would like additional controls, students do not share this perspective. This is even more pronounced among LGBTQ+ students, who are more likely to experience abuse, neglect, and homelessness if their parents are unsupportive.

Approximately half of students overall report that they would be comfortable with their parents being able to see a report of all of their online activity at school – similar to what their school's student activity monitoring system captures. This drops to just **35 percent** for LGBTQ+ students, compared to **55 percent** among their non-LGBTQ+ peers.

Students express even less support for their parents being able to see a report of their online activity *wherever they are* – only **42 percent** of students said they would be comfortable with this. Again, LGBTQ+ students report being less comfortable than their non-LGTBQ+ peers with their parents having this ability (**24 percent** vs. **49 percent** who would be comfortable). In line with these views, **67 percent** of students said they would be likely to turn off their parents' ability to see their online activity if they could, and LGBTQ+ students would be even more likely at **74 percent**.

11 Michael Yang, *Risks From Personalized Learning Technologies*, Ctr. For Democracy & Technology (Jan. 23, 2023) https://perma.cc/DAU2-5CXZ.

As previously stated, parents play an active role in supervising their children's online activity, but they agree that older students deserve more privacy and less oversight than younger children. Just over **90 percent** of parents agree that it is important for them as a parent to see everything their child is looking at and doing online from 3-8th grades, but that drops to **83 percent** for students in 9-12th grades.

Given these findings, it is imperative to think about whether state and federal online child safety laws would actually keep students "safe." The majority of students express not feeling comfortable with increased parental access to their online activity and data, and this sentiment is even more pronounced among LGBTQ+ students. This raises questions about whether parental access would cause a chilling effect and hamper kids' freedom of speech and expression.

Drafting Legislation that Minimizes Unintended Consequences to the Education Sector

Policymakers should think carefully about whether and how educational institutions are implicated by the privacy and safety bills they draft. If policymakers do not intend to include the education sector, they can take a number of different approaches.

- **Exempt organizations by class or statutory framework:** This approach would entail exempting organizations by class, such as schools and vendors providing services to them (which would then be governed by existing legal frameworks like FERPA and IDEA, as described above). Legislators would have to create a robust definition of schools and vendors to avoid some of the unintended consequences detailed previously.[12]

- **Exempt by activity:** Another approach that could be used to exempt the education sector would be to exempt data by purpose or activity. This would mean exempting data that is acquired and used for a legitimate educational purpose from provisions such as the right to delete (this language might mirror the "school official exception" language in FERPA that allows schools to outsource certain functions to vendors when there is a "legitimate educational interest in the education records").[13] This approach could allow for schools and their vendors to engage in activities like profiling if they have a legitimate educational reason to do so.

12 For an example of a robust definition of schools, see Federal Trade Commission's Notice of Proposed Rulemaking on Children's Online Privacy Protection Rule at 2072 (Jan. 11, 2024), https://perma.cc/7VHU-FYAF.

13 *Who is a "School Official" Under FERPA?*, U.S. Department of Education Student Privacy Policy Office, https://perma.cc/TP84-NCE5 (last visited Jan. 8, 2023).

- **Exempt by existing legal framework:** Another approach to exempting schools is to exempt any *data* already covered by FERPA, as in the North Carolina Consumer Privacy Act.[14] This approach has the advantage of covering both schools themselves and any vendors when they are handling FERPA-protected data. However, as noted previously, most private schools do not receive federal funding and are therefore not governed by FERPA. In this case, private schools and their vendors would not be exempted, and legislators would have to address them specifically, likely through a direct definitional carve out as there is not a similar legislation framework to FERPA that addresses private school data.

Conclusion

Regardless of how legislators and policymakers choose to approach and account for schools, it is critical to the functioning of our education system that they do so. Student data can be a great tool for improving education delivery and supporting students, but also contains highly sensitive personal information about young people that is worthy of well-designed protections. Policymakers need to ensure that schools can leverage that data effectively even as they take strides to provide much needed protections to consumers and their data.

For more from CDT's Equity in Civic Tech team, find their work on CDT's website at *cdt.org*.

The Center for Democracy & Technology (CDT) is the leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. We shape technology policy, governance, and design with a focus on equity and democratic values. Established in 1994, CDT has been a trusted advocate for digital rights since the earliest days of the internet.

14 North Carolina. S.B. 525 (2023).