

Comments on regulations to implement the Child Data Protection Act

In response to NY AG request for public comment at <https://ag.ny.gov/sites/default/files/2024-08/child-data-protection-act.pdf>

September 23, 2024

The Parent Coalition for Student Privacy was founded in 2014 in response to the realization that student privacy had been significantly undermined over time, with increased data collection by schools and the proliferation and use of various ed technology programs and tools. Since our formation, our members have been critical to the passage of many state student privacy laws, including New York Education Law § 2-d in 2014.

As such, the comments that follow primarily focus on how to ensure that student privacy is not inadvertently weakened by the Child Data Protection (CDPA), and that instead, this law actually strengthens children's privacy, in and out of the educational context.¹

1. The regulations for the Child Data Protection Act (CDPA) should not pre-empt the considerably stronger existing federal and state laws that protect student privacy

We are concerned that CDPA does not explicitly mention either of the two major federal student privacy laws, the Family Educational Rights and Privacy Act [FERPA] or the Protection of Pupil Rights Amendment [PPRA], both passed by Congress in the 1970's. Nor does it mention the even stronger state legislation passed in 2014, New York Education Law § 2-d. We urge your office to issue regulations that make it clear that the more rigorous privacy protections provided by these laws should remain in force when a child uses online tools by their school or district.

For example, FERPA allows the disclosure of personal student information without parent consent under certain conditions: only if that data remains under the control of the school or district, which usually means a contract or other written agreement, and only if it is to be used for specific educational, school operational, or research purposes. The disclosure of that data for marketing purposes does not fall under any of those categories, and thus is not allowed without parental consent. Thus, the consent of students ages 13 to 17 for the disclosure of their data is insufficient, as CDPA would appear to allow.

¹ <https://www.nysenate.gov/legislation/laws/GBS/899-EE>

Another federal law, PPRA, prohibits the collection of highly sensitive information directly from students under 18 in schools only if there is prior parent notification and consent if the survey is mandatory; parent opt out is required if the survey is voluntary. Again, disclosure of such information from students themselves ages 13 to 17 be prohibited – though it would seem to be allowable by CDPA.²

New York Education Law § 2-d prohibits the disclosure of student data for marketing or commercial purposes in all cases, including for the use of product development or improvement– with or without parent or student consent. Yet CDPA would seem to allow this in some cases, again with consent.³

The only federal law that CDPA does mention, **15 U.S.C. § 6502**, or the Children’s Online Privacy Protection Act, [COPPA] deals with the subset of personal information collected directly from children under 13. COPPA currently prohibits the collection of this data unless there is parental consent.

The Federal Trade Commission that regulates COPPA has loosened its enforcement of this law over time via guidance, not regulations, and in recent years has given a greenlight to schools and districts to allow the collection of this data to ed tech vendors and other third parties without parent consent, but only if it is disclosed for “the use and benefit of the school, and for no other commercial purpose.” There are other detailed requirements that school operators must comply with, according to FTC guidance.⁴

Meanwhile, though the CDPA says that it would not prohibit anything permitted under COPPA and its implementing regulations, ***it does not explicitly say that it would prohibit any practice not allowed under COPPA.***

Thus the CDPA regulations should make clear that the student privacy protections provided by FERPA, PPRA, COPPA and Education Law § 2-d will not be pre-empted, and that any prohibitions to the collection, use or disclosure of personal student data that are currently barred by these laws shall prevail.

Example: In February 2024, the New York Attorney General’s office negotiated a consent decree with the College Board which agreed that they would cease marketing to students their own products and services and stop selling students’ personal data to other third parties, when that data is collected as part of the administration of the PSAT, SAT or AP exams in public schools.⁵ For nearly ten years, the College Board had continued to sell this information, including student names, contact information, demographic information, and test scores, even though this practice had been prohibited since 2014, when NY Education Law §2-d was passed. And yet the College Board had continued to reap many millions of dollars from this illegal sale.

² https://studentprivacy.ed.gov/sites/default/files/resource_document/file/20-0379.PPRA_508.pdf

³ NY Ed Law § 2-d at <https://www.nysenate.gov/legislation/laws/EDN/2-D> ; its implementing regulations at <https://www.counsel.nysed.gov/rules/indices-fulltext/2019/010>

⁴ <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS>

⁵ <https://ag.ny.gov/press-release/2024/attorney-general-james-and-nysed-commissioner-rosa-secure-750000-college-board>

Since the consent decree was signed, however, the College Board has been lobbying to create a loophole on the law that would allow them to continue to profit from the use of student data for marketing purposes, by authorizing them to target paid ads for colleges and other organizations directly to students, based on their demographic and test score data. Indeed, a bill has been introduced in the State Legislature that would allow this practice to occur, as long as there was student consent.⁶ We believe that allowing the disclosure of data for marketing purposes with student consent would likely be illegal under FERPA, as only parents and not students under 18 are able to consent to the disclosure of their data by school contractors, unless it is used for specific educational or school operational purposes as described above – which do not include marketing or targeted advertising.⁷

In any case, it would be a significant step backward if CDPA inadvertently allowed the targeted advertising based on personal student data collected in schools to resume.

2. The definition of purchase and sale of children’s personal data under CDPA needs to be clarified

CDPA states that operators may not purchase or sell, or allow another to purchase or sell, the personal data of minors (GBL section 899-ff(5)), but allows the data to be used for certain marketing purposes, as long as there is consent. The CDPA’s definition of “sell” includes the sharing personal data for “monetary or other valuable consideration.”

The AG office asks the following relevant question, “*Are there examples of ways operators may share personal data that do not constitute a sale that should be explicitly noted in OAG regulations?*”

We urge you to draft regulations that bar the transfer or disclosure of children’s personal information by operators to third parties **for any financial benefit**. See how the California Consumer Privacy Act (CPRA) in Section 1798.140 (t) deals with this issue:

“Sell,” “selling,” “sale” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by

⁶ Assembly Bill 9967/ Senate Bill S9597, introduced in 2023 by AM Hyndman and Sen. Cleare <https://www.nysenate.gov/legislation/bills/2023/A9967> We believe that allowing student consent for the disclosure of this data for marketing purposes would likely be illegal under FERPA, as only parents and not students under 18 are able to consent to the disclosure of their data by school contractors, unless it is used for specific educational or school operational purposes as described above – which do not include marketing or targeted advertising. We believe that allowing the disclosure of data for marketing purposes with student consent would likely be illegal under FERPA, as only parents and not students under 18 are able to consent to the disclosure of their data by school contractors, unless it is used for specific educational or school operational purposes as described above – which do not include marketing or targeted advertising. See the 2018 guidance issued by the Privacy Technical Assistance Center of the US Department of Education: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TA%20College%20Admissions%20Examinations.pdf

electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.”⁸

See also the recent authoritative Federal Trade Commission report, ***A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services***, which describes in detail how numerous online services directed at children and teen share data with ad brokers and social media companies to monetize their personal information.⁹

Example: Talkspace, a company that provides mental health online services to teens vs its program, Teenspace, exchanges their personal information with third parties for financial benefit. Here is an excerpt from the Talkspace Privacy Policy:

Our Policy on Sales and Sharing of Personal Information: Although we do not sell Personal Information, our website uses advertising and analytics tools provided by third parties that may constitute a “sale” or “sharing” of personal information or “targeted advertising” in certain states. We do not target advertising to users who we know are under the age of 16. Once you become a patient and use our portal, we do not engage in any sales, sharing, or targeted advertising.

We may “sell” or “share” the following categories of Personal Information to these data analytics providers, advertising technology vendors, and social media platforms as described in this Policy: Identifiers/biographical information, internet or other electronic network information, commercial information, and inferences derived from the above.¹⁰

Here, Talkspace suggests that they disclose the personal data of children 16 and older to third parties for the purpose of “targeted advertising.” This statement also implies that the data of any visitor to their website who is lured into filling out an online survey that requests extremely sensitive personal information, but who subsequently declines to become a patient, can be used for marketing and further disclosed to third parties, including advertising vendors and social media platforms for commercial purposes.¹¹

According to a recently filed class action lawsuit in California, one of Talkspace’s marketing partners is TikTok. TikTok allegedly combines this information with other personal identifiers that it already has collected for these individuals, including minors, allowing both companies to profit by

⁸ The California Consumer Privacy Act took effect in 2020 and was amended and expanded by the California Privacy Rights Act (CPRA), which became effective on January 1, 2023. <https://codes.findlaw.com/ca/civil-code/civ-sect-1798-140/>

⁹ https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf

¹⁰ <https://www.talkspace.com/public/privacy-policy>

¹¹ On September 10, 2024 PCSP along with NYCLU and AI for Families sent a letter to the NYC Mayor, the Chancellor and Commissioner of Health, pointing out our concerns regarding the weak privacy protections for student data in the Talkspace Privacy Policy that would violate Education Law § 2-d if the contract was signed by the Dept. of Education rather than the Dept. of Health, and urged them to halt their promotion of the use of Teenspace to NYC public school students and other teens. See <https://studentprivacymatters.org/privacy-concerns-about-nycs-promotion-of-the-teenspace-online-counseling-service/>

targeting ads to them more effectively. By building a more complete “customer profile,” both TikTok and Talkspace benefit financially from the exchange of personal data.¹²

By using the Blacklight webtool sponsored by The Markup, one can see that when a student visits Teenspace website on their phone, their personally identifiable information is shared with 15 ad trackers, 34 cookies, and the companies Facebook, Amazon, Meta, Google, and Microsoft, among others, for commercial purposes.¹³ This highly intrusive data tracking also appears to occur when they entered even more personal data in the Teenspace online mental health survey, which asks questions that would be prohibited without parental consent or opt out by PPRA.¹⁴ This commercial exploitation and exchange for the purpose of monetizing children’s personal information should be explicitly barred by the CDPA regulations.

3. If properly regulated and enforced, CDPA could significantly strengthen children’s privacy outside the school context – but only if the privacy policies and consent documents of operators are clear and concise.

Any consent made by either parents or students aged 13 or older cannot be meaningful unless there is a transparent and concise privacy policy, linking to a separate clear and unambiguous consent form, allowing parents or students to affirmatively opt-into the transfer of their data for specific purposes allowed under law.

The following should be required to ensure that there is meaningful consent:

- The privacy policies and consent documents should make it clear exactly what categories or types of personal data or metadata will be shared with third parties and for what purposes. As the California CPRA states, consent must be “freely given, specific, informed, and unambiguous.”
- The privacy policy and consent forms should also make it crystal clear exactly how long the data will be retained and/or disclosed for such purposes, and how individuals who have consented can withdraw their consent, leading to the deletion of the data.
- Those who consent, whether parents or minors 13 or older, must be alerted by the operator if the privacy policy changes at any time, otherwise their consent is not meaningful and cannot be binding.
- The data security mechanisms protecting the information from hacking, breach or inadvertent exposure should be described clearly, including whether the data will be encrypted in motion and at rest. Without strong cybersecurity protections there can be no real privacy. Currently, it appears that the issue of cybersecurity is not even mentioned in the CDPA.

¹² <https://www.classaction.org/news/talkspace-lawsuit-claims-therapy-website-secretly-shares-user-data-with-tiktok>

¹³ <https://themarkup.org/blacklight?url=https%3A%2F%2Fwww.talkspace.com%2Fcoverage%2Fnyc&device=mobile&location=us-ca&force=false>

¹⁴ See the Appendix to the letter sent by Parent Coalition for Student Privacy, AI for Families & NYCLU to the Mayor, Commissioner of Health and Chancellor Banks, posted at <https://studentprivacymatters.org/privacy-concerns-about-nycs-promotion-of-the-teenspace-online-counseling-service/>

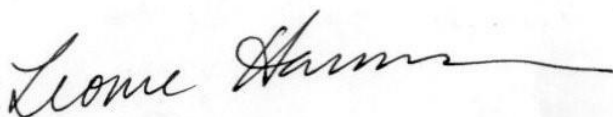
Example: Although the AG consent decree negotiated with the College Board in February 2024 prohibits the sale of student data when that data is collected in school, there is no current prohibition against the Board selling personal student data, including demographic information and test scores, when that information is obtained via the administration of tests outside the school context. Currently, the sale of that data or its exchange for marketing purposes is legal as long as the student consents. It would be a step forward if that sale were now prohibited by the CDPA.

However, the College Board privacy policies are confusing, often deceptive, and link to three different webpages, that in turn link to more than forty separate other pages. Thus, consent by students to the disclosure of their data by the College Board to third parties is hollow, as no individual has the time to peruse and comprehend all the information expressed in more than forty different documents.¹⁵

To make things worse, the College Board frequently revises their privacy policies and reserves the right to do so without notifying users or website visitors, making any prior consent to the disclosure of their personal data under an earlier privacy policy essentially irrelevant.¹⁶

Finally, according to a link on the College Board website, only Colorado residents are provided with the right to opt out of cookies placed on their computers for the purposes of marketing or targeted advertising.¹⁷ Only California residents are provided with a way to opt out of the use of their personal information for marketing purposes.¹⁸ It would be a significant step forward if New York children under the age of 18 were provided with these same and even stronger rights, as enumerated in CDPA and its regulations.

Please feel free to contact me if you have any questions,



Leonie Haimson
Co-chair, Parent Coalition for Student Privacy
phone: 917-435-9329
info@studentprivacymatters.org
<http://www.studentprivacymatters.org/>

¹⁵ See College Board's "Privacy Principles" at <https://privacy.collegeboard.org/data-privacy-principles> where it says the following: "For a comprehensive and meaningful view of our privacy practices, see the College Board [Privacy Statement](#), [Program-Specific Privacy Policies](#), and [Supplemental Resources](#) on our Privacy Center." Those pages then link to more than 40 other separate webpages, some of them relevant to privacy and some of them not.

¹⁶ <https://privacy.collegeboard.org/privacy-statement/changes>

¹⁷ <https://privacy.collegeboard.org/privacy-statement/colorado-privacy-notice>

¹⁸ <https://privacy.collegeboard.org/privacy-statement/california-privacy-rights>