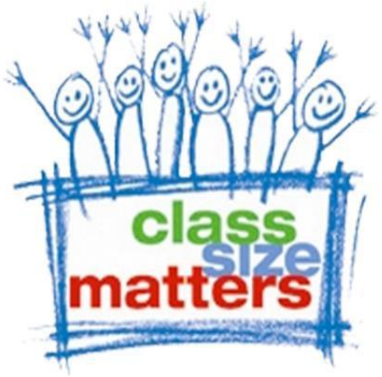
Critical weaknesses in proposed Chancellor Reg A-820 and DOE protection of Student Privacy



Presentation to NYC Schools Data Privacy Working Group

Leonie Haimson, CSM/PCSP

With support from Shannon Edwards, AI for Families

March 2025

NYS Ed Law §2-d: fairly strong student privacy law passed in 2014 result of inBloom controversy

- inBloom Inc. launched in February 2013 with more than $100M in Gates funds, designed to collect personal data of millions of public-school students in 9 states and districts, and share it with for-profit vendors to build their ed tech tools around.

- Many parents, educators and district leaders protested & every participating state and district pulled out of inBloom. NY was last when Legislature passed a bill requiring this in March 2014. In April 2014, inBloom closed its doors.

- Same time, NY Legislature also passed new privacy law Ed Law §2-d; after years of delay, SED finalized regs for the law in January 2020. Covers all public schools, charters & certain Pre-K and non-public schools, described here.

- In June 2014, the Parent Coalition for Student Privacy was founded, as we along with other parents nationwide had realized that federal privacy laws not strong enough. Soon thereafter, more than 100 new state student privacy laws were passed.

- Yet DOE has never fully complied with Ed Law §2-d and now is proposing to revise Chancellors regs A-820 to weaken its privacy protections.

How does Ed Law §2-d protect student privacy ?

- Ed Law **§ 2-d** Every school vendor with access to student PII must have privacy addendum that establishes how that data will be protected & that doc must be posted on the district website
- PII must be encrypted at all times at high level of security, as specified by National Institute for Standards and Technology Framework Cybersecurity version 1.1
- Vendor access to PII must be minimized & deleted when no longer needed to carry out contracted services
- Parents must be told how they can access their children's data held by DOE or the vendor & challenge it if inaccurate
- Parents must be notified within 60 days of the district becoming aware of a breach
- Student PII cannot be sold or used for marketing or commercial purposes --including used to improve products or create new ones
- Parents can file complaints to the district and/or State if their children's data has been improperly disclosed
- Vendors can be penalized financially if they don't comply with law &/or barred from future contracts

What is student personally identifiable information or “PII” ?

- A student’s name and the name of their parents or other family members;
- Their contact information, including phone, email, home address or IP address, based on their Wi-Fi network or router;
- Personal identifiers, such as social security number, student ID number, or biometric records;
- Other indirect identifiers, like date of birth, place of birth, or mother's maiden name;
- School-based education and health records, whether in the form of printed documents, photos, film, audio or video files that could identify them.
- Any other information, including school, ethnicity, grade, or class, that alone or in combination could identify the student with reasonable certainty.
- All this data can be shared with vendors and other third parties according to Ed Law 2d, if they are performing services for schools, or for research purposes, as long as they are under the direct control of the school
- This usually means a written agreement or contract explaining how PII will be collected and used only for that specific purpose and protected from further disclosure.

Reason for the Data Privacy Working Group

- After the proposed revisions to Chancellor regulation A-820 were posted Sept. 13, 2024, Parent Coalition for Student Privacy, AI for Families, NYCLU, AQE and other advocates sent in comments pointing out their weakness and urging they be strengthened.

- While a few changes were made, when the regs were re-released a few weeks later, they still were highly inadequate. Parents sent more than 3,000 parent emails to the Chancellor and to PEP members, urging further revisions.

- UFT President Michael Mulgrew sent a letter to the Chancellor, expressing his concerns, as did NYC Education Chair Rita Joseph and CMs Shekar Krishnan and Alexa Aviles, pointing out the dangers to student privacy and safety if these regs were adopted.

- We met with the Chancellor in November, and she agreed to set up Data Privacy Working Group to improve the regs as well as other DOE privacy policies and practices.

- We are hopeful that this collaboration will be productive and lead to stronger data privacy protections for NYC students.

DOE now proposing to WEAKEN rather then strengthen Chancellor's privacy regs!

- Chancellors reg A-820 on student privacy hadn't been updated since 2009; yet proposed revisions would severely jeopardize student privacy & in our view, are NOT aligned with state law
- Example: DOE &/or individual schools could share a huge range of nearly unlimited and highly sensitive PII w/o parent consent & w/anyone they please, by calling it Directory Info & with only an unreliable parent opt out method to protect it
- The data would "*include but are not limited to the following: name; address; telephone number; e-mail address; photographs; date of birth; grade level; enrollment status; dates of enrollment (but not daily or class period attendance); participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and schools attended*."
- Yet this ignores that there's NO mention in Ed Law 2D of Directory Information nor any exemption from its mandated privacy protections, to ensure that this highly sensitive PII does not fall into the wrong hands to be abused or further redisclosed

NYC DOE's definition of DI is contrary to DOE own advice and NYS guidance

- These revisions ignore DOE statement on its website that "***home addresses, telephone numbers, and dates of birth" are too "sensitive in nature" to be given out as Directory Information.***

- **As DOE says about cybersecurity "***Never give out personally identifiable information (PII) ….including your full birthdate, phone number …or home address."*

- NY Department of State warns that identity theft of minors can occur with only a few items of personal data, like name and birthdate, which could seriously damage their prospects since crimes like identity theft can go undetected for years:

- *"Child identity theft occurs when someone uses a minor's personal information, such as name and birth date…. The damage caused by child identity theft can vary from a single fraudulent bill in collections to a foreclosed mortgage.'*

- Disclosure of this data could also lead to commercial exploitation, sexual victimization, cyber bullying, abduction, and/or government deportation efforts.

No written agreements in regs to ensure data categorized as Directory Info will be protected

- While the proposed Chancellors regs say that Directory Info should not be sold or used by vendors or other third parties for commercial or marketing purposes, they do not require any written agreement to prohibit this.
- So, what does this provision hang on – an unenforceable verbal agreement?
- The proposed regs also do not include any written agreement to prohibit further redisclosures, nor any security protections such as encryptions.
- FERPA's exception to parental consent for Directory information was created when that law was passed in the 1970's, before the use and transmission of electronic data and when student PII was held in written records in file cabinets – before it was easy to put together bits of info to identify, track, and harm students with just a few data elements. There are also no data security protections in FERPA for the same reason.
- In any case, FERPA is the floor on privacy that Ed Law 2D was designed to raise. The fact remains there's NO mention in Ed Law 2D of Directory Information nor any exemptions from its mandated protections, to ensure that this highly sensitive PII does not fall into the wrong hands and be abused or further redisclosed

Health & medical records insufficiently protected

- Sensitive student health & medical records at schools would NOT be protected by these proposed regs if records were made by NYC Dept of Health staff or other officials, working at school-based health & mental health clinics.

- Yet nowhere does ED Law 2D exempt records maintained by schools from any of its protections, whether these records were made by school staff, employees of other city agencies, contractors or CBOs providing Community School services.

- Federal guidance says: *"Health records that directly relate to students and are maintained by a health care provider, such as a third-party contractor…would qualify as education records subject to FERPA regardless of whether the health care provider is employed by the school."*

- We have already seen how student health data can be misused when it is NOT protected by Ed Law 2D, as in the NYC Dept. of Health agreement with Talkspace to provide online mental health services for NYC teens, which has allowed their sensitive mental health data to be exploited for marketing and commercial purposes and shared with social media companies.

Proposed regs for all PII disclosure also omit important security standards required by Ed Law 2D

- Regs merely say "*Protect PII when it is stored or transferred by using encryption, firewalls and password protection, and ensure such safeguards meet industry standards and best practices. "* [and none of this required for Directory Information]

- Yet as we have seen by repeated student data breaches, in NYC & nationwide, current ed tech industry standards are NOT best practices!

- The proposed regs do not mention specific NIST standards required by Ed Law 2D law nor any need for data deletion when its no longer needed to carry out contracted services

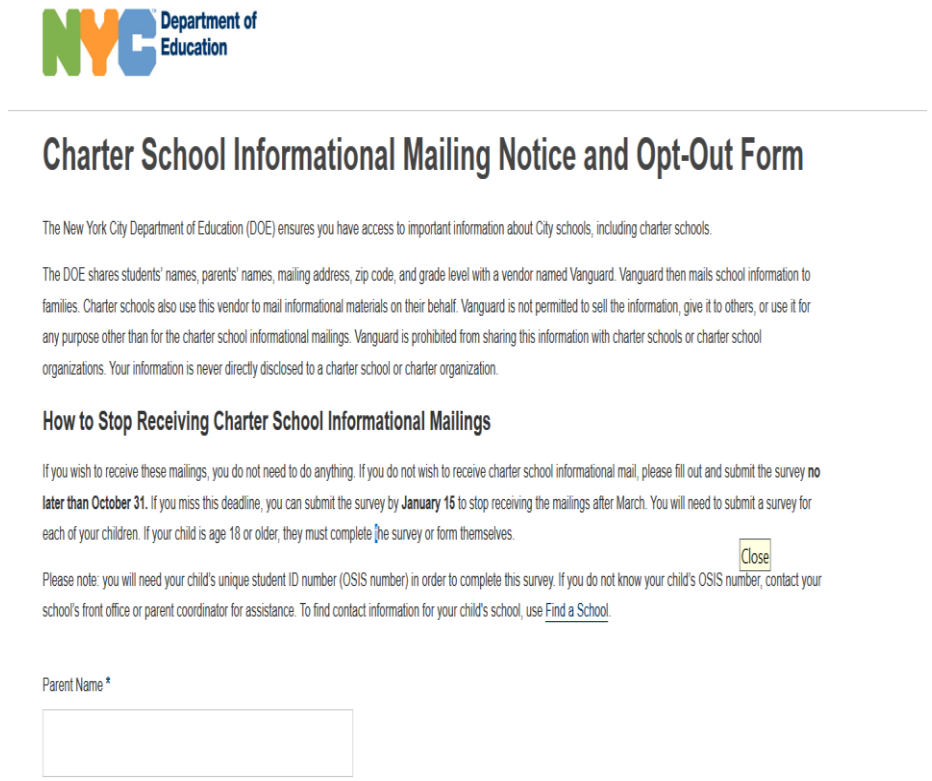
- Illuminate & Moveit breaches exposed info of hundreds of thousands of former NYC students whose data should have been deleted years ago

What about need for schools to hire companies to produce yearbooks, etc?

- NYSED FAQ explains how schools can continue to allow Yearbook companies, photographers and other service providers to collect & use personal student data for the purpose of producing their products.
- Yet as it says, schools should ensure that they have written contracts with these vendors that fully comply with Ed Law § 2-d , including limiting use of the student PII to carry out these services, prohibit further disclosures and delete data when no longer necessary.
- "*While the contract with the vendor must comply with the requirements for third-party contractors found in Education Law § 2-d … the vendor is not prohibited from undertaking activities pursuant to the contract to provide the contracted for service(s). Such activities may include notifying parents of class photograph sessions and yearbook sales, as this would be part of the service it is providing to the educational agency.*"
- Especially important that these agreements should require paywalls and data deletion, as high-quality images can be scraped off the web, by criminals using AI to create deep fake porn or false claims of abduction, putting children at risk of exploitation and harm.

Already, DOE also shares student/parent info with charter schools to help them recruit students

- For years, DOE claimed this is legal as they said they only indirectly provide student and families names, grade levels & addresses etc. through the DOE mailing house
- Yet many parents now report being barraged by phone calls from charter schools as well
- While DOE claims parents can opt out of these mailings, even after parents fill out the opt out form, many say they are still inundated with mailers and phone calls – showing how fallible the opt out process is as proposed by DOE for Directory Info
- NYC only district in country that provides this personal student info voluntarily to charter schools



NYC Department of Education

Charter School Informational Mailing Notice and Opt-Out Form

The New York City Department of Education (DOE) ensures you have access to important information about City schools, including charter schools.

The DOE shares students' names, parents' names, mailing address, zip code, and grade level with a vendor named Vanguard. Vanguard then mails school information to families. Charter schools also use this vendor to mail informational materials on their behalf. Vanguard is not permitted to sell the information, give it to others, or use it for any purpose other than for the charter school informational mailings. Vanguard is prohibited from sharing this information with charter schools or charter school organizations. Your information is never directly disclosed to a charter school or charter organization.

How to Stop Receiving Charter School Informational Mailings

If you wish to receive these mailings, you do not need to do anything. If you do not wish to receive charter school informational mail, please fill out and submit the survey **no later than October 31.** If you miss this deadline, you can submit the survey by **January 15** to stop receiving the mailings after March. You will need to submit a survey for each of your children. If your child is age 18 or older, they must complete the survey or form themselves.

Close

Please note: you will need your child's unique student ID number (OSIS number) in order to complete this survey. If you do not know your child's OSIS number, contact your school's front office or parent coordinator for assistance. To find contact information for your child's school, use Find a School.

Parent Name *

Despite Ed Law 2-d mandates, DOE's lax security & contracting processes already led to breaches

- ***As of Dec. 2024, at least 523 ed tech companies, 55 Related Service Providers, and 50 Research groups had privacy addendums on DOE site, meaning they have access to NYC student PII***
- Yet many companies w/access to student PII have no privacy agreements posted on DOE website–as required by law -- including some that suffered breaches
- Also, many of the privacy agreements that ARE posted do NOT fully align with law
- Example: In Jan. 2022 , Illuminate breach exposed personal data of more than million current and former NYC students, including dates of birth, ethnicity, academic records, special ed and/or free lunch status -- including thousands of former students.
- The privacy agreement was NEVER posted on the DOE website until after the breach. When it was, it suggested that PII was NOT always encrypted. Though security audits were offered, no indication that DOE ever asked for them
- May 2023, MoveIt breach released PII for 45,000 students, in addition to DOE staff and related service providers – with no privacy agreementever posted.

State Comptroller found DOE had inadequate breach notification

- State Comptroller reported that 80% of DOE cybersecurity incident reports lacked enough detail to tell if students and teachers were informed within the legally required 60-day timeline.
- In more than half of incidents, NYC DOE blew past the legal deadline to notify NYSED of the problem.
- And yet NYC DOE still is expanding use of ed tech and online learning, including risky AI programs, multiplying risk of data breaches and misuse of student data – without necessary guardrails & now proposing to weaken Chancellor A-820 privacy regs.

Lax response to PowerSchool breach in Dec. 2024

- Jan. 9, 2025, PowerSchool announced that their Student Info System had been hacked, exposing student PII nationwide, and began informing schools & districts of the breach

- Among data released, depending on school and district: student names, contact info, date of birth, grades, test scores, special ed status, mental health details, disciplinary notes, parental restraining orders and more – as well as teacher PII in some districts.

- When asked, DOE initially told reporters that no NYC schools were affected.

- On Feb. 3, 2025, I learned DOE had told NYSED at least four NYC schools that enroll about 3,000 students were likely affected; yet DOE refused to confirm names of schools when asked by reporters & only alerted parents at these schools after Daily News reported this

- As of Feb. 26, 2025, DOE had still said nothing publicly and posted no alert on its website, despite NYSED guidance this should be done "***to capture as wide an audience as possible***" especially as former students may also have been affected & PowerSchool offering free ID theft insurance & credit monitoring.

- DOE website finally updated by March 2 – more than 2 months after the breach --but without disclosing names of schools or which data was affected – though parents were told at PTA meeting that former students may also have had their data breached

DOE's privacy agreement with PowerSchool defective and does NOT conform to law.

- PowerSchool is now facing numerous state lawsuits for lax privacy practices including failure to use double authentication – standard procedure to protect security of PII.

- But as we pointed out months ago, PowerSchool's privacy agreement w/DOE says the company will "*Review data security and privacy policy and practices to ensure they are in conformance with all applicable federal, state, and local laws & the terms of this DSPP [Data Security Privacy Plan].…*

- *… In the event Processor's policy and practices are not in conformance, Processor will implement commercially reasonable efforts to ensure such compliance."*

- In other words, PowerSchool **will only comply with federal and state privacy laws when it doesn't unduly affect their bottom line.**

STILL DOE authorizes schools to use 17 data hungry PowerSchool products – including Naviance that commercializes student data

- Naviance, a college/career planning program, is used in many NYC HS, which collects a huge amount of student PII & sends targeted ads to students, disguised as objective recommendations, in violation of State law. The company has been shown to allow colleges to discriminate by targeting ads to white students only.

- Other PowerSchool programs DOE allows NYC schools to use that collect student PII: *Enrollment, Enrollment Express, Performance Matters Advanced Reporting; Performance Matters Assessment;* and *PowerSchool SIS*

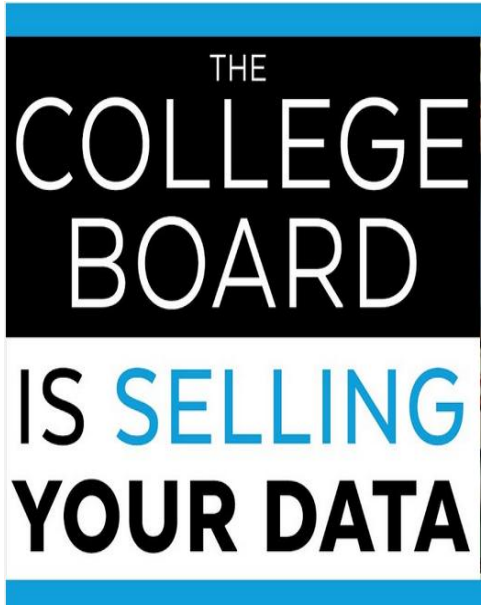
- Student and teacher data: *Unified Talent Employee Records; Unified Classroom Schoology Learning; Unified Classroom Curriculum and Instruction*

- Special education, SEL and behavior data: *Unified Classroom Special Programs; Unified Classroom Behavior Support,* plus six more***!***

- ***None of these programs should be trusted given PowerSchool sloppy privacy practices and inherent weakness of the DOE contract.***

College Board – a known violator of state privacy law

- For years, College Board made more than $100 million annually selling personal student data collected from students during testing in school and when they sign up for accounts.
- This includes student names, addresses, race/ethnicity, grades, income and test score ranges, even though this sale has violated student privacy law in NY since 2014
- We protested this practice to DOE & they did nothing to stop it.
- Finally, in February 2024, NY Attorney General negotiated a consent agreement with College Board & they agreed to stop selling student data and paid a fine of $750,000.
- But ***DOE has had no contract with College Board since June 2023*** – even as hundreds of thousands of NYC HS students took AP, PSAT and SAT exams last year in school & DOE paid them $9.9 million for those tests!
- Meanwhile, College Board is STILL violating the law by asking NYC students to sing up for their “Connections” program which allows colleges to target ads to students based on their personal data – including their test scores.



College Board – another weak DOE privacy agreement

- CB Privacy agreement posted on DOE website says the company, its subcontractors will NOT encrypt student data "***where data cannot reasonably be encrypted***"
- Also says it will delete the data only "***when all NYC DOE schools and/or offices cease using College Board's products/services***".
- For the SAT/PSAT, the PBOR contains ***no specific date or time*** when the data will be deleted – both are contrary to the law.
- Recently, bill has been introduced to create a loophole in the Ed Law 2D to allow the College Board to continue monetizing student data
- A9967/ S9597 would allow CB to send targeted ads to student phones, paid for by colleges and other companies, based on their data, including their grades, test scores, race and ethnicity – but as we have seen they are doing this already!

What's the harm of breaches or disclosing student PII without restrictions?

- Student PII is very valuable for identity theft as most minors do not already have credit ratings
- Excessive monitoring of student's internet use by schools can be devastating to their sense of individual freedom
- Their data can also be used by schools for racial profiling, law enforcement, and other discriminatory actions
- Student PII can be used by ad tech and social media companies for marketing, bombarding them with ads, & even undermining their mental health, as noted in recent NYC & state lawsuits vs these companies
- Negative info about a student can affect their future opportunities, including jobs, college admission, medical insurance, etc.
- Student data can also be used to threaten their safety, leading to cyberbullying, sexual harassment, abuse, abduction or deportation

Some NYC schools also surveille students without alerting parents

- Oct. 2021, Bloomberg News reported that NYC DOE signed a contract with GoGuardian that sells surveillance/spyware installed on computers used by students and that could spy into their homes and their family members without their knowledge if not properly configured.
- When a PEP member asked to see this contract in Nov. 2021, DOE said there was none, but that they were "***able to Centrally make this product available to all schools through the Enterprise G-Suite/Google Workspace license at no cost to school nor to families***"
- More recently, the DOE posted a GoGuardian privacy agreement online, for a contract that they say started in Aug. 2021, but it lacks sufficient detail and says that it lapsed in August 2024.
- According to GoGuardian, best practice is to inform parents beforehand that this program is being used and installed on their children's computers, and allow for parent opt out, but we do not know if this has been done in NYC schools***.***

Expansion of AI likely to further undermine student privacy

- DOE encouraging principals and teachers to expand use of AI without guidance, though most Generative AI programs harvest personal data to improve their products as pointed out Center for Artificial Intelligence and Digital Policy FTC complaint.
- Open AI admits that "Chat ***GPT-4 has the potential to be used …to identify private individuals when augmented with outside data***" and that its use could "***reinforce & reproduce specific biases & worldviews, including harmful stereotypical & demeaning associations for certain marginalized groups***."
- Their official policy says no child under 13 should be using Chat GPT, and no student aged 13-17 without parent consent. Other AI programs have similar age-linked restrictions which are ignored by many families and schools.
- Yet DOE has put out NO guidance or guardrails to ensure that student data is not monetized or abused via use of AI in classrooms and schools. Once its shared with AI, impossible to check to see if it wasn't improperly mined.
- HMH Writeable, authorized to be used in NYC schools, says they use student data for "***Product improvement"*** in their Privacy Policy– and their privacy agreement w/DOE does not prohibit this.

For a briefing or for more information, contact Parent Coalition for Student Privacy at info@studentprivacymatters.org

Or check out our website at www.parentcoalitionforstudentprivacy.org

A Spanish translation of this presentation is available at https://studentprivacymatters.org/wp-content/uploads/2025/03/Spanish-Privacy-briefing-updated-2.26.pdf