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

Leonie Haimson, Exec Director, Class Size Matters

& Co-chair, Parent Coalition for Student Privacy

May 2025

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

- Chancellor's regulation A-820 on student privacy hadn't been updated since 2009; though in 2014 NY Ed Law 2D passed, significantly strengthening protections for student data.

- DOE's proposed revisions would severely jeopardize student privacy & in our view, are NOT aligned with state law

- Example: DOE &/or individual schools could now share a huge range of sensitive PII without parent consent & w/any company, individual or organization they believe would benefit them or students, by calling it Directory Info, & with only an unreliable parent opt out method to prevent its disclosure

DOE now set to revise their student privacy regulation: Chancellor regulation A-820

- 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, as did NYC Education Chair Rita Joseph and CMs Shekar Krishnan and Alexa Aviles, pointing out the dangers to student privacy and safety, including immigrant students, 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. That group held two meetings since Feb. 2025. Yet insufficient changes have been made to these regs and now up for a vote of the PEP on May 28.

What student data could be shared without parent consent according to these regs?

- Within the school community, schools could share student and parent names, telephone numbers, emails, physical address, plus student's grade level, enrollment status, schools attended, dates of enrollment, images of the student, degrees, honors, awards, and information about their participation in sports and activities, including weight, and height of team members.

- Outside the school community, DOE could share any and all information including the above and more, **only excluding**: SS #, OSIS#, grades, test scores, daily attendance, race, ethnicity or other demographic info, special ed or multilingual status and disciplinary history – which are barred by FERPA without consent.

- The one significant concession made so far by the DOE is these disclosures will require a written agreement that bars its further redisclosure and sets out the same security protections as in Ed Law 2D.

- Yet this ignores that even with these protections, too often student data has been breached and used for commercial purposes contrary to the Ed Law 2D, with inadequate oversight and enforcement.

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…are too "sensitive in nature" to be given out as Directory Information.***
- **As DOE itself 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, which if they fell into the wrong hands 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….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 efforts to deport immigrant students***

Whole notion of Directory information being harmless if released widely is out of date

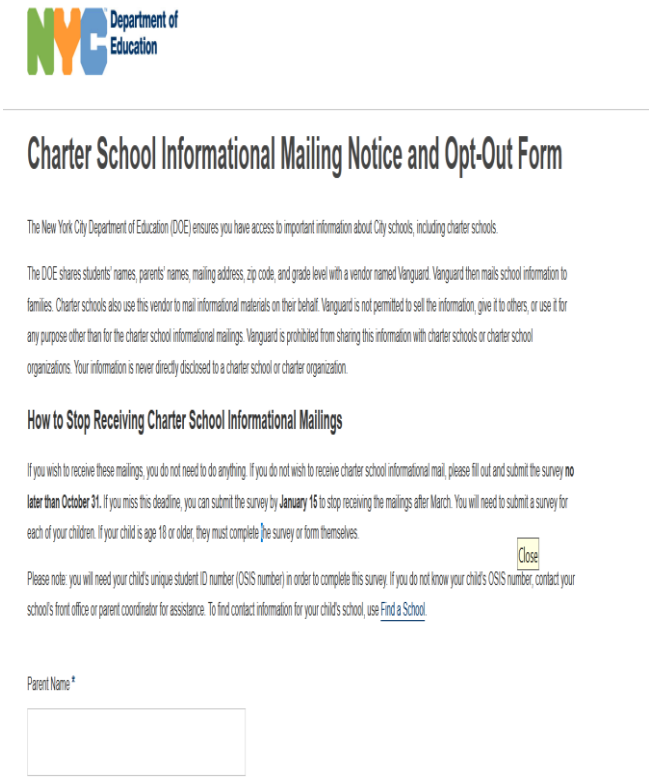
- FERPA's exception to parental consent for Directory information was created when the law was passed in the 1970's, before the use and transmission of electronic data, including biometric data, when student PII was held in written records in file cabinets – before it was easy to put together bits of info to identify, track, and harm students with just a few data elements.

- Yet the latest proposed version of the regulations would exacerbate this risk and is due to be voted upon at the May 28, 2025 meeting of the Panel for Educational Policy.

- The draft regulations are posted on a DOE SharePoint Folder – you can also find them at a link on the agenda for the May 28 meeting.

Already, DOE 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 through the DOE mailing house, called Vanguard.
- 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 the sole protective measured proposed in the amended regs.
- These regs if adopted would allow charter schools to even more aggressively solicit students by providing them with student phone nos. and emails and allow them to differentially recruit those who are high performers, either academically or athletically.
- ***As it is, NYC only district in country that provides this personal student info voluntarily to charters .***



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 *

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 student safety, leading to cyberbullying, sexual harassment, abuse, abduction or deportation

Parent Coalition for Student Privacy

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