Safeguarding your child's personal data: Threat to student privacy from digital learning, Teenspace, College Board, & AI & more

class size matters

Alliance for Quality Education

Parent Coalition for Student Privacy

Student Privacy Briefing

Leonie Haimson, CSM/PCSP & Beth Haroules, NYCLU

Oct. 23, 2024

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 your Wi-Fi network or router;
- Their personal identifier, such as social security number, student ID number, or biometric records;
- Other indirect identifiers, like their date of birth, place of birth, or mother's maiden name;
- Their school-based education and health records, meaning information whether in the form of printed documents, photos, film, audio or video files that could identify them.
- Any other information, including their 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 certain 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.

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

- 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 including NY, and share it with for-profit vendors to build their ed tech tools around.

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

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

- Because of inBloom controversy, parents nationwide realized that federal privac laws not strong enough, so more than 100 new state student privacy laws were passed in 2014-17.

- Yet DOE is still not fully complying with Ed Law §2-d, and now is rewriting Chancellors regs to further weaken their privacy protections.

NYS Education Law 2-d

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

- Ed Law **§ 2-d** Every school vendor with access to student PII must have contract addendum that establishes how that data will be protected & that addendum must be posted on the district website
- ***At least 523 ed tech companies, 55 Related Service Providers, and 50 Research groups have privacy addendums on DOE site, meaning they have access to NYC student PII***
- PII must be encrypted at all times at high level of security 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
- Parents can file complaints to the district and/or State if their children's data has been improperly disclosed
- Vendors can be penalized financially by the state if they don't comply with law &/or barred from future contracts

Despite Ed Law 2-d mandates, DOE's lax security measures have led to repeated breaches

- May 2021 – Microsoft breach, never reported by DOE, exposed 291,955 records containing student names, usernames, district borough numbers, and email addresses

- That same year at least two breaches released student PII from unprotected Google drives, affecting over 3,000 students; first one undisclosed by DOE until the second one occurred.

- Jan. 2022 , Illuminate breach exposed personal data of more than a million current and former NYC students, including dates of birth, ethnicity, academic records, enrollment data; & for some, special ed in and/or free lunch status --possibly the largest student data breach in US history.

- Illuminate privacy addendum not posted until after the breach, & hinted that the data was not always encrypted & though security audits were required, DOE did NOT ask for them

- March 2023, Encore Support Services breached of 50,000 PII records contained in special education billing records; DOE claimed they did not have to notify parents because these pertained to nonpublic school students whose services they were ordered to pay for via impartial hearings

- May 2023, the MoveIt breach released PII for 45,000 students, in addition to DOE staff and related service providers – with no privacy addendum or contract ever posted.

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

- Student PII 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 devasting to their sense of individual freedom

- Their data can also be used by schools for racial profiling 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 lawsuits launched by NYC and State Attorney General

- 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 sexual harassment, abuse or even abduction

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 determined to expand the use of ed tech, AI and online learning in schools throughout the city, multiplying risk of data breaches and misuse of student data.

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

- Chancellors reg A-820 on student privacy hasn’t been updated since 2009

- Proposed revisions would weaken student privacy & are NOT aligned with federal or state law

- Example: DOE would be allowed to share sensitive PII w/o parent consent & w/anyone they please, including student & parent names, emails, home addresses, phone #s, photos, birthdates, & more, by calling this “Directory Information” w/o any protections of Ed Law 2D & only with unreliable parent opt out.

- Yet this ignores that there is NO mention in Ed Law 2D for Directory Information or exemption from its mandated privacy protections, including prohibiting its sale or use for commercial purposes

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

- Their proposed definition ignores DOE own statement on its website that PII like ***home addresses, telephone numbers, and dates of birth are too sensitive to be considered Directory Information.***

- **State guidance** also says that if directory information is to be shared, district must ensure that the release of any information will benefit students and the educational agency;

- Also says that such data "cannot cannot being sold or released for any commercial or marketing purpose, defined as the sale of student data or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly, for advertising purposes, or to develop, improve or market products or services to students.“

- This suggests there must be a written agreement, and yet there is no language in the regs concerning any of these limitations.

Proposed regs include lax security standards

- Ed Law 2D mandates that schools use the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a set of guidelines that helps manage cybersecurity risk.
- DOE revisions never mention this high level of NIST encryption required to protect against breaches
- DOE revisions do not mention need for data deletion by vendors, when info no longer needed to carry out its services
- Yet, Illuminate & Moveit breaches exposed info of hundreds of thousands of former NYC students whose data should have long been expunged
- Instead, proposed regs 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.”*
- Yet as we have seen by repeated student data breaches, in NYC & nationwide, current ed tech industry standards are NOT best practices!

Health & medical records insufficiently protected

- Sensitive health & medical records kept at schools would NOT be protected by Ed Law 2d if made by Dept of Health staff, at school-based health & mental health clinics.

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

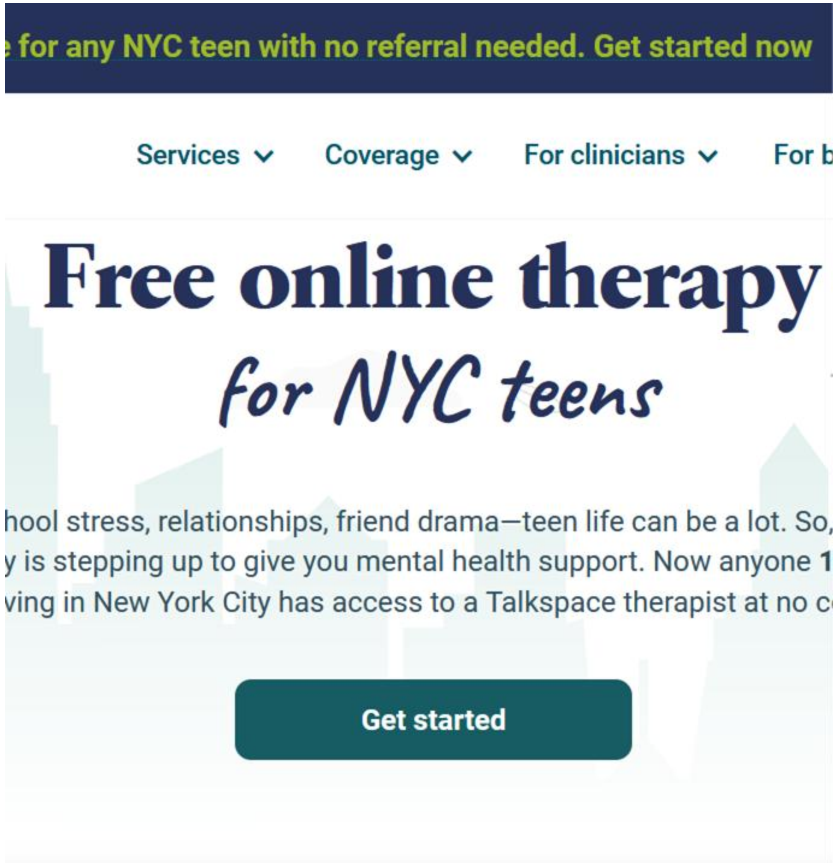
- There is also no exemption in ED Law 2D for any records maintained by schools, whether made by school staff, employees of other city agencies, or CBOs providing Community School services.

- We have already seen how student data can be abused when it is NOT protected by Ed Law 2D, as in the NYC Dept. of Health deflection of problems w/ Teenspace

- ***Please send a message now, urging them to revise these proposed regs and postpone the Oct. 30 PEP vote at https://tinyurl.com/emailDOEregs***

Dept of Health has $26M contract with Talkspace/Teenspace for online mental health services for students

- Use of Teenspace relentlessly promoted by Mayor, Health Commissioner, & Chancellor Banks
- Teenspace online Privacy Policy says personal info can be used for marketing purposes & disclosed to unnamed partners, which would be barred by Ed Law 2D if contract was w/DOE
- Talkspace has been sued in CA for sharing personal mental health info with TikTok, including that of minors.
- PCSP, NYCLU and AI for Families sent letter to Mayor, Health Commissioner and Chancellor, expressing our concerns



e for any NYC teen with no referral needed. Get started now

Free online therapy

for NYC teens

hool stress, relationships, friend drama—teen life can be a lot. So, y is stepping up to give you mental health support. Now anyone 1 ving in New York City has access to a Talkspace therapist at no c

Dept. of Health response inadequate

- They said they don’t have to abide by Ed Law 2D as they are not an education agency, but that their contract protects student privacy, which references the application of HIPAA, NY state mental health law and the NYC Identifying Information Act

- Yet unclear if these law pertains to Teenspace & other online mental health providers &/or their contract applies when students visit the Teenspace website before they’ve signed up for services

- Website has a survey asking many highly sensitive questions about student mental health, drug use, family relationship and gender identity before they’ve signed up for services.

- We discovered that when a student visits the Teenspace website on their phone, their personal info shared is with 15 ad trackers and 34 cookies, as well as Facebook, Amazon, Meta, Google, and Microsoft among other companies, which we saw from using the Blacklight privacy audit tool. These findings were later confirmed by a security company .

- Ironically, the city & AG office are now suing these companies for undermining children’s mental health and designing their platforms to be addictive to maximize their revenues via targeted advertising.

- We asked for a meeting with DOH officials, for the Teenspace website to be immediately taken down, and families of students whose personal info has been compromised to be notified.

- So far none of this has occurred.

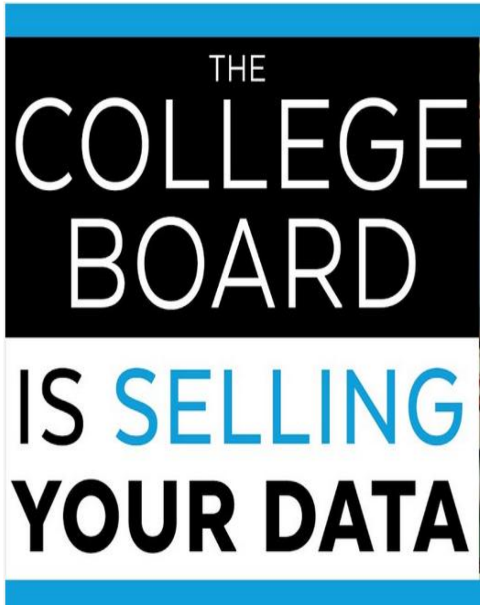
College Board – a known violator of state student privacy law

- College Board makes more than $100 million per year selling personal student data collected from students during testing in school and when they sign up for accounts.

- This includes their names, addresses, race/ethnicity, income and test scores, even though this sale violates student privacy law in NY and about 19 other states

- We protested this practice to DOE and State Ed for nearly ten years, and in February 2024, NY Attorney General Letitia James negotiated a consent agreement with College Board & they agreed to stop this practice and pay a fine of $750,000.

- But we have no idea how this will be enforced or monitored – especially as ***DOE has had no current contract with College Board since June 2023*** – even though hundreds of thousands of NYC HS students took AP, PSAT and SAT exams last year in school & DOE paid them millions for those tests!



THE COLLEGE BOARD IS SELLING YOUR DATA

College Board – other privacy issues

- CB Privacy addendum posted on DOE website from past contract says the company, its subcontractors will NOT encrypt student data “***where data cannot reasonably be encrypted***”

- Addendum to AP contract 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.

- Recently, bill has been introduced to create a loophole in the law and allow the College Board to continue monetizing student data

- A9967/ S9597 would allow CB to send ads to student phones, based on their PII, test scores & other data – as long as a student opts in, though we have found that College Board often uses deceptive language to persuade students to do this that doesn’t benefit their prospects.

Naviance: another program widely used by NYC schools that commercializes student data

- Naviance, a college and career planning program, is used in many schools; DOE has paid more than $1.7M for its services since 2020.

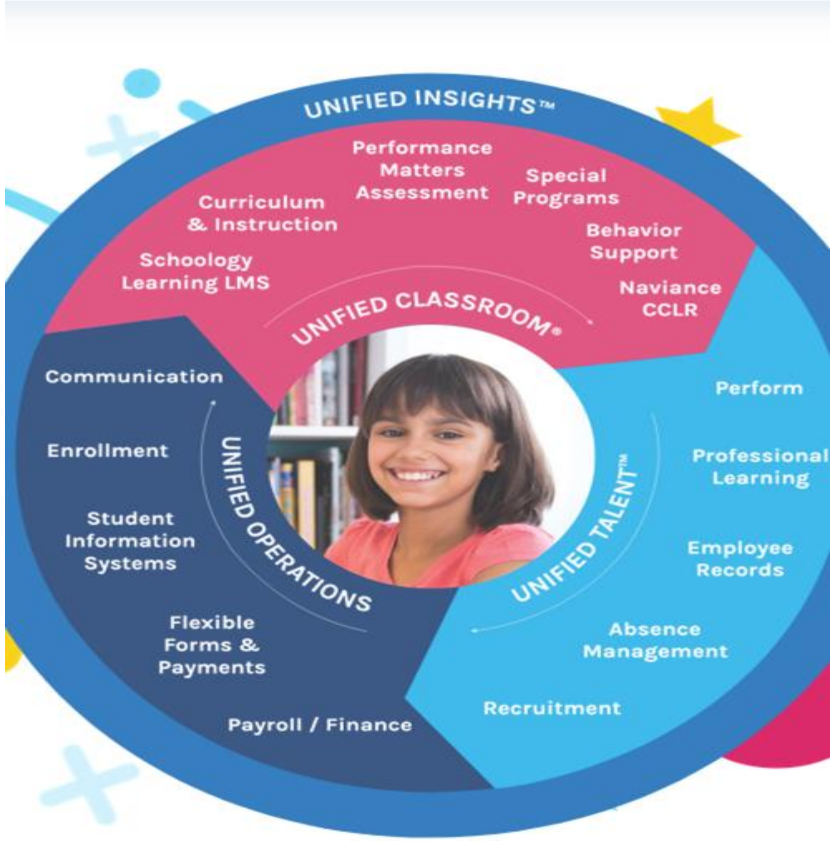
- Now owned by PowerBook, they collect a huge amount of personal student data & profits by selling ad space within its student-facing platform to colleges, disguised as objective recommendations

- Naviance has been shown to allow colleges to target ads to students by their race, including showing ads only to white students.

- DOE addendum for Naviance and 16 other data-hungry PowerBook products say this: 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 won't unduly affect their bottom line.**

DOE plans to use up to 17 different privacy-invasive PowerSchool programs. A sample:



- Student data: *Naviance, 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*

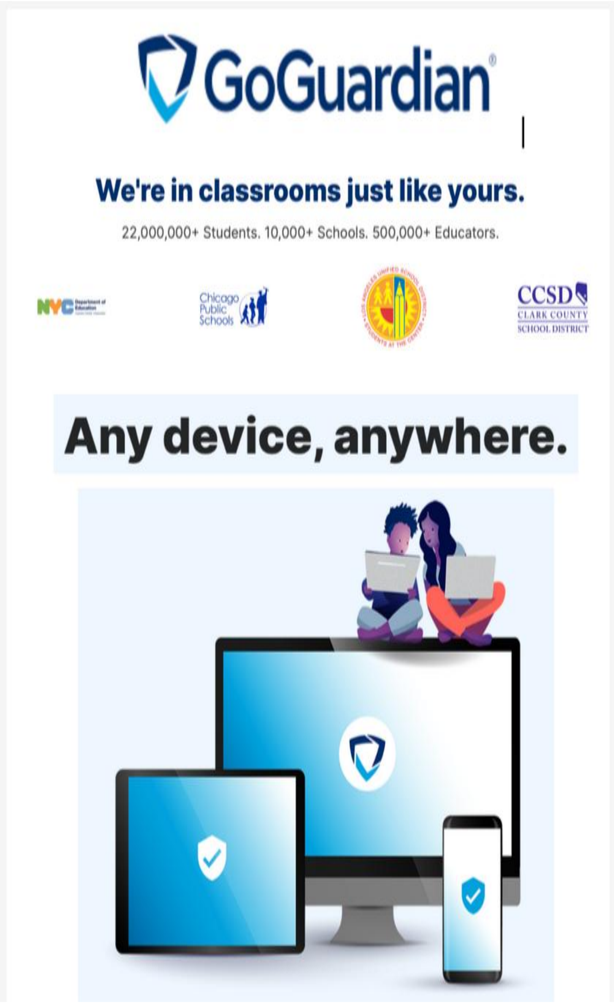
- Special education data: *Unified Classroom Special Programs ;* SEL and behavior data: *Unified Classroom Behavior Support*

- ***Plus, six more!***

Expansion of online learning & AI room likely to further undermine privacy as well as quality of instruction

- DOE encouraging principals and teachers to expand use of AI while putting more data in the hands of for-profit companies where it may be breached, used for commercial purposes or in ways that are racially- or gender biased.
- Yet DOE has put out NO guidance or guardrails to ensure that student data is not monetized or abused.
- Most every AI program gathers huge amounts of personal data without consent, as pointed out by FTC complaint filed by Center for Artificial Intelligence and Digital Policy (CAIDP).
- 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 being ignored by DOE.

NYC schools also surveille students without alerting parents


GoGuardian
We're in classrooms just like yours.
22,000,000+ Students. 10,000+ Schools. 500,000+ Educators.
NYC
Chicago Public Schools
CCSD CLARK COUNTY SCHOOL DISTRICT
Any device, anywhere.

- 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 can spy into their homes 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 addendum online, for a contract that they say started in Aug. 2021, but it lacked 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 these guidelines have not been followed by DOE.

More concerning AI tools used in NYC schools

- One example that NYC teachers are already encouraged to use to help students with their writing is HMH Writeable.

- A brief statement on the HMH website says their products including Writeable "*is compliant with Educational Law Section 2-D*"; but their general privacy policy states that "***we may use and disclose the Personal Information we collect for the following purposes…[including] Product improvement"***

- Yet Ed Law 2D regs make clear that PII should not be used for commercial purposes, including "using the data ***to develop, improve or market products or services to students."***

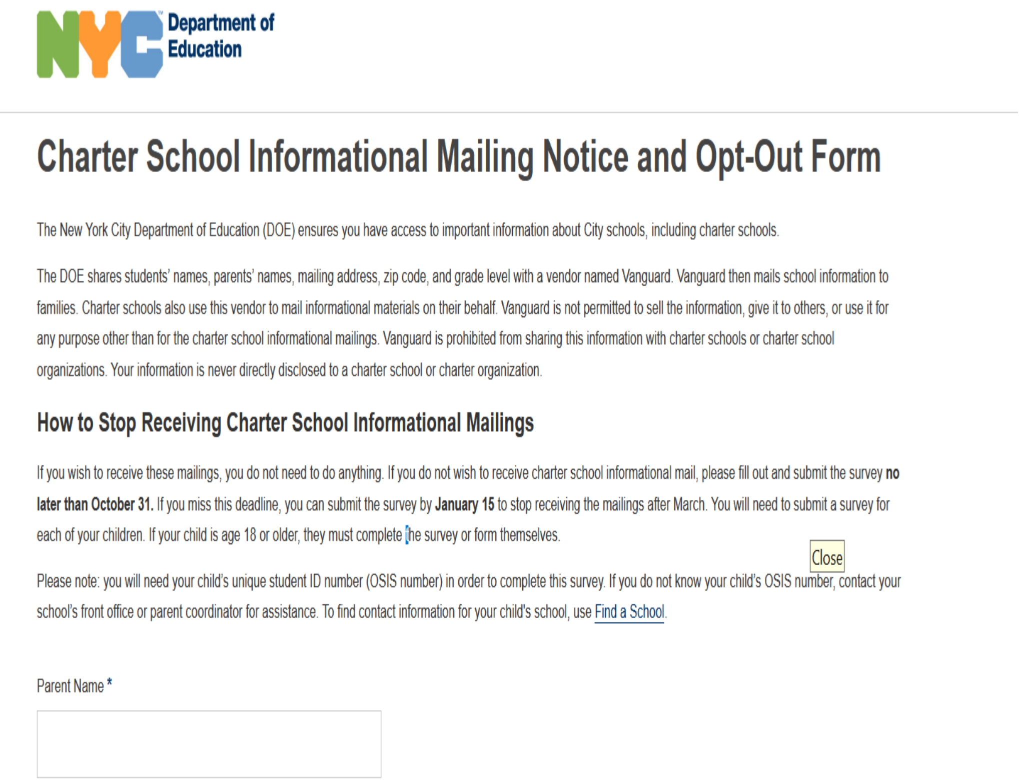
- Amira is another AI tutoring app used in NYC schools that we have heard is collecting voice from students in grades k-5 without parental knowledge or consent.

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

- DOE claimed this is legal as they only indirectly provide addresses etc. through their mailing house

- Yet many parents now report being barraged by phone calls from charter schools as well

- Also, DOE says that parents can opt out of these mailings but when parents fill out the form, they still inundated with mailers and phone calls



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.

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 *

NYC Kids Rise college saving program

https://nyckidsrise.org/get-started/

- DOE says more than 200,000 NYC students are enrolled, though how many parents are aware is unclear as no consent is given

- DOE shares student names, birthdates, home addresses, parent names, email addresses, cell phone numbers, and unique student and parent ID numbers. Why so much PII is being shared unclear.

- Both NYC Kids RISE and VistaShare, a data management company, receive the data and say they use it only for this purpose though no contract is posted.

- The initial opt-out period is Nov. 4 – Dec. 4; the DOE form is hard to find but available here. https://infohub.nyced.org/docs/default-source/default-document-library/district-opt-out-notice-and-form.pdf

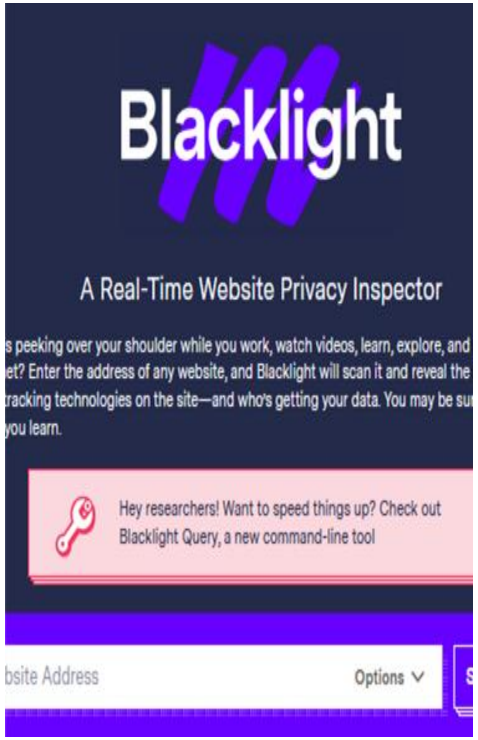
- After this opt-out period ends, you can still opt out on your NYC Schools Account. After logging in, click on the "Forms" tile, then on the "view" button on the next page next to "NYC Kids RISE Save for College Program." After that, you can review program information and see your opt out options available towards the bottom of the page.

What should DOE be doing instead?

- Naveed Hasan is a computer scientist, with a focus in artificial intelligence and technology systems design, and a member of the Panel for Education Policy
- NYC DOE has a $39 billion annual budget and size that would allow them to use their market power to demand information technology serve students in a manner that protects the security and privacy of their data.
- DOE should be hosting their server-side software in data centers that they own and operate, with vendors providing the software to run in-house. That way, no PII would exit the DOE to be shared with private companies, and instead could be accessed by schools, including staff, teachers and students over a private intranet.
- Students would also be able to connect from home to these tools via virtual private network links.
- ***All major corporations use this type of infrastructure for data security and the NYC school system should behave in a manner that befits their size and responsibility to our children.***

Meanwhile, here are ways you & your child can better protect their data

- Ask your school for its policies regarding data privacy and a list of apps that are being used by the school and/or assigned to your child to use at home or in the classroom. Ask to opt out of any that you do not trust
- Also ask your child to log into any ed tech program they use in school, then copy the URL into the Blacklight tool at https://themarkup.org/blacklight to see what companies can access their personal info
- You can also enter the name of the ed tech program into https://appmicroscope.org/ or Commonsense Media to see its privacy ratings
- Tell your kids never to be logged into Facebook, Instagram, TikTok or any social media platform while using ed tech, as this makes it easier for their data to be accessed by those companies.
- Use Foxfire as a browser, Duck Duck Go as a search engine, and install Privacy Badger, which alerts users to ad tech & other invasive trackers.



Blacklight

A Real-Time Website Privacy Inspector

s peeking over your shoulder while you work, watch videos, learn, explore, and
et? Enter the address of any website, and Blacklight will scan it and reveal the
racking technologies on the site—and who's getting your data. You may be su
you learn.

Hey researchers! Want to speed things up? Check out Blacklight Query, a new command-line tool

Other ways to protect your child’s privacy

- Set up a Google alert to give you real-time updates on news related to breaches in your school, city, or specific to an app or service your school is using.
- Teach your children data minimization, such as providing as little information as possible when setting up and using apps, and use fake but memorable answers for password retrieval such as “what city were you born in.”
- If you or your child haven’t used an app or service for more than 6 months, be sure to demand for it to be “closed and your personal information deleted.” Unsubscribing to updates is not enough.

Other ways to protect your child’s data privacy *(cont.)*

- Turn off Wi-Fi on your phone when not in use, such as when walking around outside, unless you or your child require location tracking. Otherwise, apps can match you to in-store content and ads.
- Utilize built-in parental control features on devices to manage app access and monitor usage. For instance, Apple's Screen Time allows you to set limits on app usage and content restrictions.
- Try to clear cookies often and open different browsers for social media versus other platforms or apps

Also, more immediate steps you can take!

- Email DOE opposing these new regs at https://tinyurl.com/emailDOEregs or by using QR code at right.
- Attend PEP meeting where they are supposed to be voted on – Wed. Oct 30 6 PM at M.S. 131 at 100 Hester St.
- Opt out of all directory information sharing now at https://tinyurl.com/DOEoptoutforms ***Deadline for opting out of Charter school mailings is Oct 30!***
- Military recruitment deadline Oct. 18, but you should try now anyway - & point out that you weren't notified in time. Copy us!
- National Student Clearing House deadline says Jan. 10, 2020 [assume they mean 2024]

Other steps to help us help you!

- Ask your child if they've visited the Teenspace website and/or signed up for their services. If so, let us know! If not, warn them that if they do, their data may be monetized and misused.
- If they took a College Board exam in a NYC public school last year, either PSAT, SAT or AP, and you're concerned that their PII including their scores may have been illegally disclosed, let us know.
- Warn them not to sign up for the College Board Student Search, Connections or Big Future programs if they don't want their PII, including test scores, to be sold or used for targeted advertising
- If you've opted out of charter school disclosures, but were contacted by a charter school anyway, let us know.
- Email the DOE Chief Privacy Officer at studentprivacy@schools.nyc.gov to ask him what companies have access to your child's data -- & copy us!

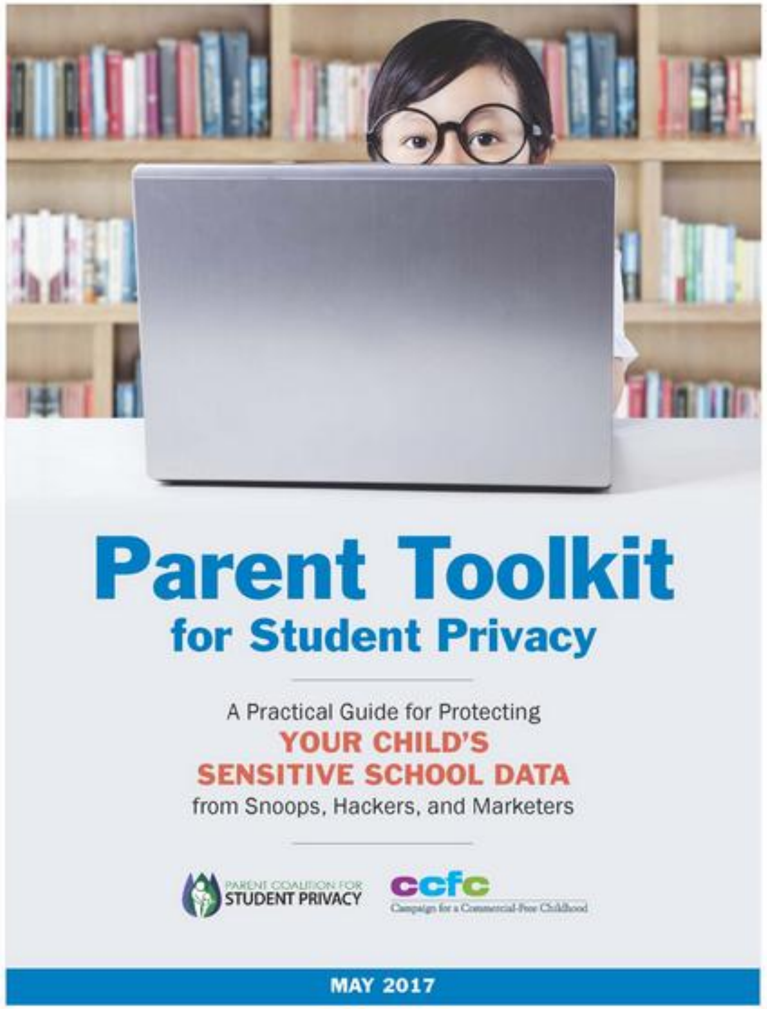
For more tips on how to protect your child's privacy…

Check out our Parent Toolkit for Student Privacy

Co-sponsored with Fairplay for Kids (formerly Campaign for Commercial Free Childhood)

Available on our website in English
http://bit.ly/ParentToolkitStudentPrivacy

and Spanish
http://bit.ly/ParentToolkitStudentPrivacySpanish



Parent Toolkit
for Student Privacy

A Practical Guide for Protecting
YOUR CHILD'S
SENSITIVE SCHOOL DATA
from Snoops, Hackers, and Marketers

PARENT COALITION FOR STUDENT PRIVACY

ccfc
Campaign for a Commercial-Free Childhood

MAY 2017

Any questions or if you want help

- Fill out our brief survey here: https://tinyurl.com/helpwithprivacy

- We are also here to support parents who believe their child’s personal data may have been breached or improperly disclosed, & to discuss whether they’d like to file a privacy complaint

- Contact us at Parent Coalition for Student Privacy at info@studentprivacymatters.org
-
- More info including this presentation is available on our website at www.parentcoalitionforstudentprivacy.org