Concerns with DOE data privacy/security practices and adherence to NYS Student privacy law

Presentation to CEC 15

Leonie Haimson

Executive Director, Class Size Mattes

Co-chair, Parent Coalition for Student Privacy

9/19/23

inBloom controversy led to nearly 100 state student privacy laws being passed including NYS Ed Law §2-d in 2014

- inBloom Inc. launched in February 2013 with more than $100M in Gates Foundation funds, designed to collect and process the 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. NY pulled out when Legislature banned this disclosure in March 2014, and in April 2014, inBloom closed its doors.

- Parents nationwide who had protested inBloom formed the Parent Coalition for Student Privacy in July 2014, having learned how weak federal laws were in protecting student data.

- In 2014, 24 new state student privacy laws were passed in 2014 including in NY; 77 more laws in in 2015 - 2017.

- NYS Legislature passed Ed Law §2-d in March 2014; after much delay, SED finalized the regulations to enforce the law in January 2020.

What does NY student privacy Ed Law §2-d say?

- Every vendor with access to student PII must have a contract with a Parent Bill of Rights (PBOR) that establishes how that data will be protected & these PBORs must be posted on the district website
- Student personally identifiable information (PII) must be encrypted at all times at a high level of encryption (***NIST for National Institute of Standards and Technology***)
- Student PII cannot be sold or used for marketing or commercial purposes
- 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 the vendor & challenge it if inaccurate
- Specific notifications required of vendors & districts w/ families to be informed within 60 days of districts becoming aware of a breach
- Vendors can be penalized financially by the state if they don't comply with law &/or barred from future contracts

SCI has repeatedly urged DOE to institute more privacy-protective measures

- Special Commissioner of Investigation for NYC Schools has repeatedly urged the DOE to establish more privacy protective policies and practices in its formal Policy and Procedure Recommendations (PPRs)

- To prohibit school staff or CBO employees from contacting students using their personal cellphone numbers, social media accounts, and other associated applications, which DOE has refused to do .

- To stop allowing schools to use free products and services, until vetted by trained personnel for privacy/security protections. State law requires this but DOE only starting this recently and very unevenly.

- SCI also noted how after a student data breach occurred in Aug. 2020, they urged DOE to tell staff to stop using unprotected Google drives to store PII; DOE said they would do so but didn't -- and additional breaches from Google drives occurred in January 2021 and March 2021, as a result of the same practice.

- In Jan. 2022 , DOE sent a letter to the SCI, noting that two of its "*most significant corruption hazards [were] in the following areas: (1) the procurement, distribution and safeguarding of air purifiers and (2) data security*"

State Comptroller audit in May 2023

- State Comptroller audit found 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, the city blew past the legal deadline to notify the state of the problem.

- And yet DOE determined to expand the use of ed tech and online learning in schools throughout the city, multiplying risk of more data breaches, including AI bots.

Some DOE vendors with access to student data have no posted Parent Bill of Rights

- Parent Bill of Rights are supposed to be posted on the DOE webpage **Supplemental Information for Parents About DOE Agreements With Outside Entities**

- Yet some have NO contracts or PBORs: Go Guardian is a surveillance/spyware program installed on student computers; can spy into student homes without their knowledge if not properly configured.

- When PEP members asked to see the GoGuardian contract, DOE said there none, but they "***make this product available to all schools through the Enterprise G-Suite/Google Workspace license at no cost to school nor to families,"*** in apparent evasion of the law**.**

- No PBOR posted for **ANY Google product**, including Google Workspace, Google classroom, G-suite for Education, or now renamed Google's Education Fundamentals --

- Other DOE vendors with access to student data, have NO contracts with DOE to this day, including MoveIt, that recently suffered a major breach.

Other ways in which DOE fails to comply with student privacy law

- DOE has not UPDATED the Chancellors regs regarding student privacy since 2009 – though new law passed in 2014
- When there a PBOR is posted, it very rarely is fully compliant with the law .
- Data minimization & deletion rarely occur, and most PBORs posted by DOE do not require this
- Result: Illuminate and MoveIt breaches exposed data from thousands of NYC students who had long graduated and left the system.
- Illuminate contract hinted at fact that data was not encrypted & though it called for independent security audits, it appears that DOE *never* asked for them

College Board – a known violator of state student privacy law

- College Board sells personal student data, including test scores, and its PBORs do not prohibit this practice though it violates the law.

- CB PBOR also says the company, its subcontractors and others with whom it shares this data will NOT encrypt student data "*where data cannot reasonably be encrypted*"

- PBOR for AP exam says it will delete the data only "***when all NYC DOE schools and/or offices cease using College Board's products/services***".

- For the just-posted SAT/PSAT, the PBOR contains no specific date or time when the data will be deleted.

- CB supposedly in negotiations with NY AG office to halt its illegal practices, but DOE just signed a new CB contract with a PBOR that is non-compliant with the law

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

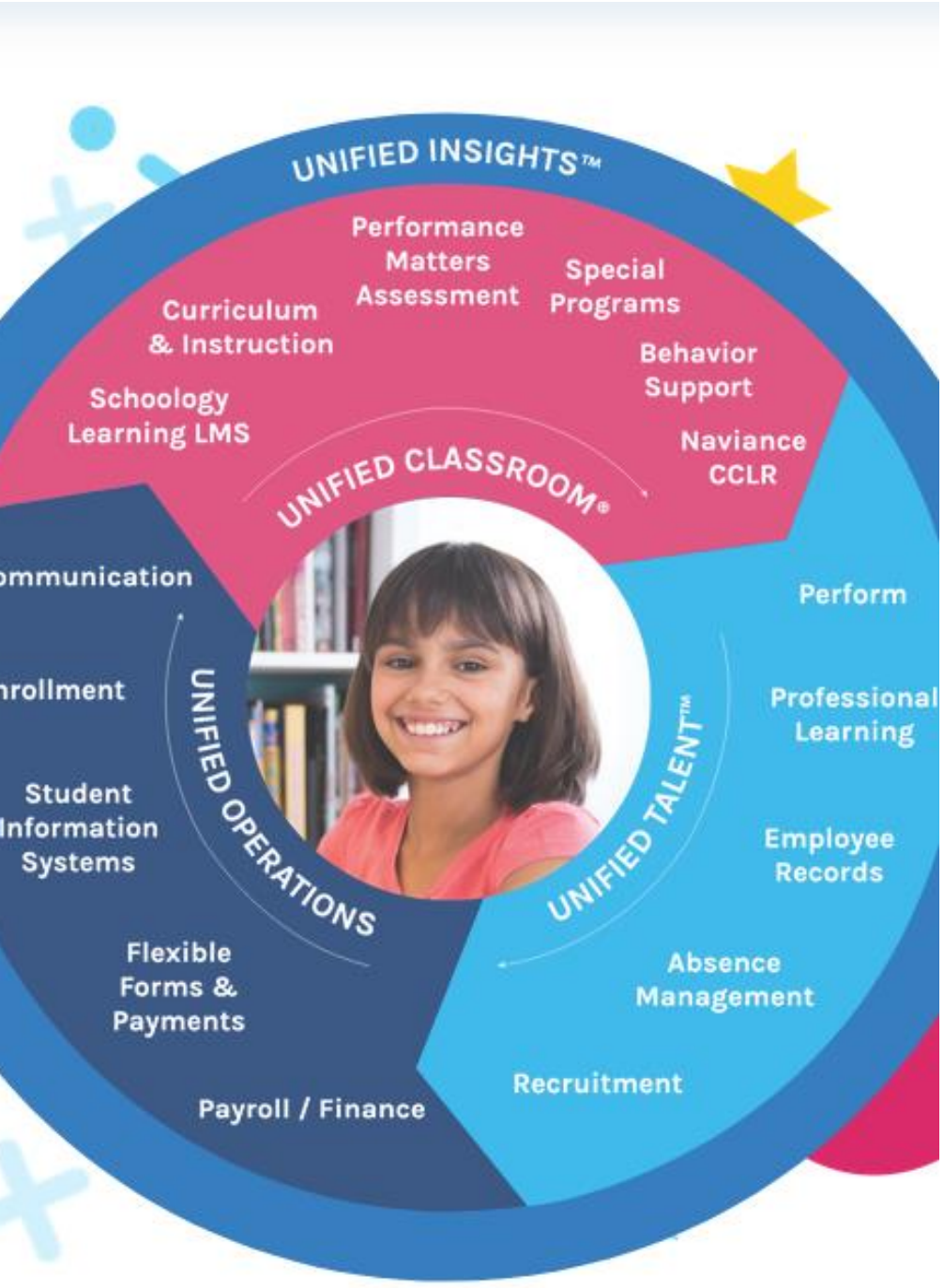
- Naviance, a college and career planning program, had no PBOR posted until last week, though DOE has paid $1.7M on Naviance since 2020.

- Naviance, now owned by PowerBook, collects huge amount of personal student data & profits by selling ad space within its student-facing platform to colleges, disguised as objective recommendations

- Naviance allows colleges to target ads to students by their race, including targeting ads only to white students.

- NEW DOE PBOR 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 & even the contract itself when they feel it won't unduly affect their bottom line.



This deficient PBOR now pertains to 17 different privacy-invasive PowerSchool programs –with additional programs added daily. 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!***

What should DOE contracts/PBORs require?

- No vendor should be able to access ANY student data without a legally-compliant contract and a PBOR posted on the DOE website.

- Contracts/PBORs should specify what data elements can be accessed by the vendor and for what specific purposes; too often DOE has no idea what data is being collected and transmitted by their vendors.

- Contracts/PBORs should require strong encryption (NIST) level & independent privacy & security audits -- and DOE should ask for those audits!

- Contracts/PBORs should require AT MINIMUM that the vendor delete the data when students graduate or move out of district, and optimally at the end of every school year.

- Contracts/PBORs need to clearly prohibit the sale or the commercial, marketing use of student data under all conditions.

NYC Comptroller has a role to play as well

- NYC Comptroller has the authority to refuse to certify any DOE contract that doesn't comply with the law, and he should do so in the case of vendors with access to personal student data.

- He should also audit already certified NYC DOE contracts with vendors, to see that those with access to student PII include PBORs that fully comply with the law, and that these PBORs are posted on the DOE website;

- He should also use his bully pulpit to propose what changes are needed in the state law, enforcement or policy to ensure that personal student data is better secured and protected from breaches, commercial use, or abuse.

NYC chapter of Parent Coalition for Student Privacy

- *We are looking for NYC parents interested in these issues to help us advocate for stronger student data privacy and security.*

- *If you have questions or are interested in joining us, please email us at: info@studentprivacymatters.org thanks!*