DEVELOPMENTS IN STUDENT PRIVACY
BEGINNING WITH INBLOOM INC.

NYSED/ DPAC Presentation

Leonie Haimson

Co-chair Parent Coalition for Student Privacy

6.15.22

www.studentprivacymatters.org

Life and death of inBloom Inc. (2013-2014)

- inBloom Inc. launched in February 2013 with more than $100M in Gates Foundation funding
- Designed to collect personal information of millions of public-school students, starting in nine states and districts, including NY.
- Data to be systematized and shared with for-profit data-mining software companies to build their “tools” around, w/out parental knowledge or consent.
- Data to include student names, addresses, grades, test scores, grades, economic and racial status, disciplinary records, disability information and much else.
- In their contracts with NYSED, Gates Foundation and inBloom disclaimed all legal responsibility if data breached, and they said would start charging districts for their “services.” in 2015.
- Parents, educators and district leaders vehemently protested, and one by one, every state and district pulled out. In April 2014, inBloom closed its doors.

With inBloom defeated, what did we learn?

- Parents & many others had incorrectly believed FERPA protected students' personal identifiable information (PII) in school records by requiring parental notification & consent before disclosure to 3rd parties.

- Instead, we learned that FERPA had been weakened twice by US Dept of Ed, through regulations that created vast loopholes to enable ed agencies to disclose student PII with organizations and vendors for many reasons without parental knowledge or consent

- We also became fully aware for 1st time how much collection and sharing of student data was ALREADY occurring without our knowledge.

The inBloom controversy kick-started a huge debate on student privacy that continues:

- In 2014, the NY Legislature passed a strong student privacy law, NYS Ed Law 2D that also banned inBloom & led to its demise.
- Same year we formed the Parent Coalition for Student Privacy to represent parents' right to protect their children's education data.
- 38 states have passed at least 98 student privacy laws since then, to try to make up for weaknesses in FERPA.
- And yet few of these laws have been properly complied with and enforced, including Ed Law 2D.

Sloppy & illegal practices in NYC and elsewhere

- NYC schools are still encouraged to use hundreds of apps & programs w/o proper screening and without posting their contractual Parent Bill of Rights
- NYC DOE still doesn't notify parents of many of their privacy rights under federal law, including COPPA, PPRA and their Directory Information policy.
- Data minimization & deletion doesn't occur, and many of the PBORs posted by DOE do not require this.
- Example: Illuminate breach included all sorts of data that it didn't need --like PII of students who had long graduated.
- Illuminate also had expansive access to many categories of data it didn't need – unclear if DOE ever attempted to restrict it.
- Illuminate contract required independent security audits – unclear if DOE ever asked for them

DOE contract with Illuminate shows profound misunderstanding of federal law

- "*Vendor understands that under FERPA it must limit access to PII to those who need to know the Confidential Information for Vendor to perform its duties under its contract, and to destroy all copies of PII, or to*
- *return PII to the DOE, when no longer needed or at the expiration of any contract. "*

- Yet under FERPA and ED Law 2D, these are **the district's** obligations– not vendors, and it appears that DOE did none of this.

Many other problematic vendors used by DOE & other NY districts.

- Go Guardian – students surveillance/spyware that schools use to protect against cheating and check to see if students are engaged; can spy into student homes if not properly configured. When members of NYC school board asked for contract, DOE said it didn't exist.

- College Board continues to sell student data collected before AP/PSAT/SAT exams and online and sells it directly to colleges and other third parties, including student score ranges– in violation of 2D and law in many other states.

- Naviance – makes $ by surveying students without parent knowledge, collecting their data, and allowing colleges to target ads to students based upon that data in discriminatory ways.

- Kinsa thermometer that schools encouraged families to use during pandemic captures student health data remotely; company uses that data to market products to families & unclear if data is encrypted.

What needs to be done

- Prohibit teachers using unscreened & likely illegal clickwrap agreements or “freemium”
- Disallow use of any programs/apps not screened for privacy/security protections & post EVERY Parent bill of rights for EVERY vendor accessing personal data
- Require & enforce strong encryption & independent privacy & security audits -- and ask for proof that this is done!
- Limit vendor access ONLY to data that they absolutely need to provide specific services – and maintain control over this!
- Require vendor to delete student data every year & at minimum, when students graduate or move out of district

For more information…

- We have privacy fact sheets & toolkits for parents and teachers as well as opt out forms available at www.studentprivacymatters.org
- You can also ask us questions at info@studentprivacymatters.org
- Sign up for our newsletter for updates at our website at www.studentprivacymatters.org
- Join our Facebook page and follow us on Twitter *@parents4privacy*