HOW IS STUDENT DATA SHARED? HOW IS STUDENT PRIVACY THREATENED?

Parent Action Conference

Leonie Haimson, Parent Coalition for Student Privacy

Nov. 7, 2015

www.studentprivacymatters.org

2014: Parent defeat of InBloom

- inBloom Inc. corporation started with more than $100M in Gates Foundation funds to collect personal information of public school students in 9 states and districts, including NYC.
- Data to be shared with for-profit data-mining software companies – w/out parental knowledge or consent.
- Detailed personal data to include student names, addresses, grades, test scores, detailed disciplinary and disability information.
- Without any funding, parent activists across the country protested and in April 2014, inBloom closed its doors.

What did we learn from inBloom controversy?

- Parents believed federal law protected students' personal identifiable information (PII) in school records by requiring parental notification & consent before disclosure to 3rd parties.
- We were wrong!
- We also had no idea how much collection and sharing of student data was occurring with vendors and other 3rd parties outside school and district.

What about FERPA ?

- *Family Educational Rights and Privacy Act,* federal law passed in 1974 that required parental consent for disclosure of student educational records.
- FERPA regulation weakened by US Dept of Ed in 2008 and 2011.
- In 2008, regulations were rewritten to allow states, districts or schools to share PII data with any third party performing operational services, who could be designated as a "school official."
- This could include "contractors, consultants, volunteers, and other parties to whom an educational agency or institution has outsourced institutional services or functions it would otherwise use employees to perform."

FERPA revision part II

- In 2011, FERPA regulations revised to allow personal student data to be disclosed to “authorized representatives” to conduct studies, evaluations or audits of the effectiveness of an education program.

- Any organization or individual now could be defined as "authorized representative” and get access to student personal data.

- Previously, "authorized representatives" were individuals over which educational authorities had "direct control,” such as an employee or a contractor.

What about health data in student records?

- Often children's education records include detailed disability/health data.
- Same info in medical records couldn't be shared without parental consent with 3rd parties, acc. to HIPAA (*Health Insurance Portability and Accountability Act*) .
- Security provisions in HIPAA require "reasonable methods" including encryption to protect against breaches; NO security protections required in federal law to protect student records.
- HIPAA also requires privacy/security training for all persons handling personal health data – none in case of education records.
- Even so, there have been breaches of health information despite HIPAA.

What about security?

- In survey, 86% of technology experts say they do not trust clouds to hold their organization's "more sensitive" data.* And yet much student information now stored in clouds.
- InBloom had "heartbleed" flaw – critical vulnerability.
- Repeated breaches off clouds include Target breach affected up to 110 million customers. US Office of Personnel Management breach effected 21 M federal employees.
- ConnectED was due to get NYS data from inBloom for data dashboards. Later went bankrupt information for 20 million students transferred anyway to other companies.

**Lieberman Software's 2012 Cloud Security Survey*

Obama administration accelerated state data collection & sharing

- 2009, US Dept. of Education required states to develop longitudinal student data systems combining student data with health and medical information, juvenile justice, Child services – to track children “cradle to the grave.”

- Multi-state databases established, to share personally identifiable student information across state lines, which would have been illegal before FERPA was revised.

- US Dept. of Ed helped develop Common Education Data Standards, 1500 data pts to describe children’s trajectory from birth through college & workforce, including early development, disciplinary infractions, disabilities, socio-emotional skills, health information, & assessment/achievement results.

- NYS developing its own longitudinal system, with unclear restrictions on access or when data will be destroyed.

- During our lawsuit against inBloom, revealed that they would put all this information after 8 years into the state archives.

What else have we learned?

- inBloom tip of the iceberg. Data-mining software companies & their allies in foundation/gov. sectors see huge potential & profit in putting education/assessment online.
- PreK-12 software ed. tech market estimated at $7.9 *billion*, over $90 billion globally.
- Feeds off narrative that our education system is “failing” or “broken”; needs “disruptive” change.
- Ultimate goal to eliminate as many teachers as possible in favor of mechanized instruction.
- Euphemistically called “personalized learning” but really de-personalized learning.

Thousands of data-mining companies working in public schools, often w/o parental knowledge or consent. Examples:

- Clever – in over 18,000 schools, allows vast array of software companies to access PII through school student information systems– using “instant” log-in as in inBloom

- Class Dojo –controversial online behavioral tracking of kids with reward system built-in

- Amplify –division of Murdoch’s NewsCorp, sells tablets pre-installed w/data-mining software, collecting wealth of personal info including student names, SS#s, along w/ learning data which is shared w/ “affiliates” to support “product development”

- Google Apps for Education, pre-installed in Chromebooks or used separately, data-mining personal student data & sued in CA for targeting ads to kids.

Data tracking can lead to profiling – *even if there are no privacy violations*

- Minor incidents –even those years earlier— now enter into a student's permanent record and be easily accessible to teachers and admins through the dashboards.
- "Pygmalion" or "Golem effect": studies show that teachers and administrators tend to stereotype students based on prior knowledge.
- When teachers told a student is problematic, this can become self-fulfilling prophecy.
- If dashboards reveal negative academic or disciplinary history before teachers have even met a student can lead to negative expectations that seriously impair their prospects.

Lessons from inBloom fiasco

- FERPA as revised does not protect kids' privacy; we need federal law strengthened.
- Data is powerful, and can be used for good or for ill.
- If collected, personal student data must be used – and shared – with great caution.
- Parents must be informed and involved in the decision-making.

Parental rights under FERPA

- Right for your child's educational records NOT to be disclosed publicly (except for operational, educational, research, or evaluation exceptions.)
- Right to inspect the information in your child's education records, held by school, district or state & correct data if it's erroneous.
- Right to be informed of school/district's criteria to determine who constitutes a "school official" with whom PII can be shared without parental consent.
- Right to opt out of the child's "directory information" being shared–including name, address, email, telephone number, date & place of birth etc. –as long as the school/district has no agreement with the vendor to share data for exceptions noted above.
- Right to opt out of having their child's name, address and telephone provided to military recruiters.
- Right to be informed of their FERPA rights each year by their school or district.

Parental rights under the Protection of Pupil Rights Amendment (PPRA)

- 1. Right of parental consent before child is required to participate in federally funded survey, analysis or evaluation dealing with information concerning:

- Political affiliations;
- Mental or psychological problems potentially embarrassing to the student or family;
- Religious affiliations and beliefs;
- Sexual behavior and attitudes;
- Illegal, anti-social, self-incriminating and demeaning behavior;
- Critical appraisals of individuals with whom respondents have close family relationships;
- Privileged relationships, with lawyers, physicians, and ministers; or
- Income (other than that required by law to determine eligibility for a program).

- 2. If the survey or evaluation is not federally funded, written consent not required but parents must be notified in advance & have the right to opt their children out of participating.

- 3. In either case, schools and/or their contractors must make instructional materials or surveys available for inspection by parents ahead of time, to allow them to decide whether to consent or opt out.

Parental rights under Children's Online Privacy Protection Act (COPPA)

- COPPA applies to any operators of websites or online services that your child is participates in at school or home, including testing, programs or "apps" that collect, use, or disclose children's personal information.
- Your school should be providing you with a list of all the online programs that your child participates collecting your child's personal information, according to FTC "best practice."
- If your under-13 child is participating in an online program collecting personal information, whether for instruction, testing, or other purposes, the school and/or vendor or operator must provide you with a clear and prominent privacy policy , including the following information:
- The name, address, telephone number, and email address of the vendors collecting or maintaining personal information through the site or service;
- The types of personal information the operator is collecting, how the data is being used and with whom it may be shared;
- That you can review or have deleted the child's personal information;
- That you can refuse to permit its further collection or use..

NYS privacy law passed in 2014

- Called for end of inBloom.
- Appointment of chief privacy officer who will develop an expanded Parent Bill of Rights with input from parents w/deadline July 31, 2014:
- Still today, we have not permanent CPO & no expanded Bill of rights
- Interim CPO Tina Sciochetti refuses to meet with parents or to strengthen Parent bill of rights
- Gives out FALSE information, including as to whether parents have to pay to access their child's data in the state longitudinal data system.

What are we doing?

- We have formed national organization **Parent Coalition for Student Privacy** w/ some of our allies in the inBloom fight.
- We are working to pass a stronger federal student privacy law in Congress
- We are also focused on alerting parents to the rights they still have to protect their kids' privacy
- We are helping parents write FERPA complaints

For more information…

- We have fact sheets and opt out forms available at www.studentprivacymatters.org
- You can also ask us questions at info@studentprivacymatters.org
- Sign up for updates at our website at www.studentprivacymatters.org
- Join our Parent Coalition for Student Privacy Facebook page