STUDENT PRIVACY 101

Rachael Stickland, co-chair of Parent Coalition for Student Privacy

The Promise and Pitfalls of EdTech
Chicago, October 26, 2017
What we’ll cover tonight

• What technology is used in schools

• What data is being collected

• Why this should concern parents

• What laws exist to protect student privacy

• What parents can do
WHAT TECHNOLOGY is used in schools
The world’s most valuable resource is no longer oil, but **DATA**.

*(The Economist, May 6, 2017)*
Who’s cashing in?

*Education technology is becoming a global phenomenon, and as distribution and platforms scale internationally, the market is projected to grow at 17.0% per annum, to $252 billion by 2020.*

EdTechXGlobal: connects the global EdTech community through insight, investment and annual thought leadership events in London and Singapore. (May 2016 Report)
Implications for Business in ESSA

- **Title I, $15B**: New program flexibilities + fiscal flexibilities including a radically different supplement not supplant rule.
- **Title II, $2B**: New focus on embedded + personalized career development
- **Title III, $756M** Eng. Language Leaners: New focus on "effective" language instructional programming;
- **Title IV, up to $1.6B** to support Title I and invest in the effective uses of technologies.
- **Evidence based programming**: The law emphasizes evidence-based decision making to procure and review products.
- **Assessment Innovation.** ESSA allows for “innovative assessment” pilots
- **Direct Student Services**: New optional state set aside for tutoring programs and direct programming for students.
- **“Pay for success” program** allow private investment in ed.

* Congress has yet to pass Fiscal Year 2017, so the figure are not yet known. There is a lot of politics to play out.
Case Study

- Colorado student privacy law HB16-1423
- Requires schools to inventory EdTech usage
- Poudre School District in northern Colorado
The list below shows Contract Service Providers with current Poudre School District contracts.

<table>
<thead>
<tr>
<th>Title</th>
<th>View Contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accelerated Math</td>
<td>View Contract</td>
</tr>
<tr>
<td>Accelerated Reading</td>
<td>View Contract</td>
</tr>
<tr>
<td>Aimsweb</td>
<td>View Contract</td>
</tr>
<tr>
<td>Albert</td>
<td>View Contract</td>
</tr>
<tr>
<td>Amplify</td>
<td>View Contract</td>
</tr>
<tr>
<td>Big Ideas Learning</td>
<td>View Contract</td>
</tr>
<tr>
<td>Career Cruising</td>
<td>View Contract</td>
</tr>
<tr>
<td>ChildPlus</td>
<td>View Contract</td>
</tr>
<tr>
<td>Cognitive Abilities Test</td>
<td>View Contract</td>
</tr>
<tr>
<td>College Physics: A Strategic Approach AP</td>
<td>View Contract</td>
</tr>
<tr>
<td>Destiny Discovery</td>
<td>View Contract</td>
</tr>
<tr>
<td>Digital Science Techbook</td>
<td>View Contract</td>
</tr>
<tr>
<td>Dreambox</td>
<td>View Contract</td>
</tr>
<tr>
<td>Engrade</td>
<td>View Contract</td>
</tr>
<tr>
<td>Enrich</td>
<td>View Contract</td>
</tr>
<tr>
<td>enVision Math 2.0</td>
<td>View Contract</td>
</tr>
</tbody>
</table>
### On-Demand Service Providers

The list below shows On Demand Service Providers identified for use within the district.

<table>
<thead>
<tr>
<th>Title</th>
<th>Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Manufacturing Products</td>
<td>Approved With Restrictions</td>
</tr>
<tr>
<td>ACT WorkKeys</td>
<td>Approved</td>
</tr>
<tr>
<td>ALEKS</td>
<td>Approved</td>
</tr>
<tr>
<td>BookFix</td>
<td>Approved</td>
</tr>
<tr>
<td>BrainPOP</td>
<td>Approved</td>
</tr>
<tr>
<td>Breathe, Think, Do with Sesame</td>
<td>Approved</td>
</tr>
<tr>
<td>Conjuguemos</td>
<td>Approved</td>
</tr>
<tr>
<td>Connect for Kapoor, Personal Finance</td>
<td>Approved</td>
</tr>
<tr>
<td>EasyCBM</td>
<td>Approved</td>
</tr>
<tr>
<td>EBSCO</td>
<td>Approved</td>
</tr>
<tr>
<td>Edulastic</td>
<td>Approved</td>
</tr>
<tr>
<td>ESGI</td>
<td>Approved</td>
</tr>
<tr>
<td>GoSwim</td>
<td>Approved</td>
</tr>
<tr>
<td>International Baccalaureate Organization</td>
<td>Approved</td>
</tr>
<tr>
<td>Khan Academy</td>
<td>Approved</td>
</tr>
<tr>
<td>LiveSchool</td>
<td>Approved</td>
</tr>
</tbody>
</table>
“Before I write my name on the board, I’ll need to know how you’re planning to use that data.”

WHAT STUDENT DATA is collected?
Traditional student information

Name, date of birth, grades, test scores, health information (e.g. immunizations, prescribed medicines, disabilities), free- and reduced-lunch status, etc.

Before he starts kindergarten, Tommy’s parents must provide his school with his personal information including name; gender; date of birth; social security number; health information (e.g., immunizations, prescribed medications, disabilities, allergies, etc.); and family income information to see if he qualifies for free or reduced-priced lunch.

Tommy’s information is then uploaded into the district’s online database — which is likely maintained by an out-of-state company such as InfiniteCampus and stores all data in the “cloud” — and provided to school administrators, teachers, and parents via a digital “data dashboard.”

The school will send much of the information electronically to the state department of education to track Tommy’s progress through school in the statewide longitudinal data system (SLDS). Researchers and policymakers often use this information for accountability and evaluation purposes.
Student information, including biometrics, for operational systems

Fingerprints used for cafeteria services, health data collected by heart monitors used in gym class, books checked out from the library, location trackers in bus ID badges, etc.

3. On his way to school, Tommy’s location and internet activity are tracked by technology installed on his school bus.

A radio frequency identification (RFID) chip in Tommy’s ID card allows the school to track his whereabouts.

5. In the cafeteria, Tommy provides his fingerprint, name, or student number to the lunchroom aide, who then records his food selections in his online account, which may become a part of his permanent digital record.

6. During gym class, Tommy wears a heart rate monitor to record his workout intensity as part of his grade. An app analyzes the results and sends a report via email to the teacher’s Dropbox account. It’s unclear what happens to Tommy’s digital health information at the end of the school year.
Digital information for “educational” purposes

Email addresses, user IDs, IP addresses, passwords, behavioral events, internet search histories, videos watched, papers submitted online, voice recordings, etc.

2. Before Tommy arrives in the classroom for his first day, his personal information is shared with various companies that provide services to the school and district. The district creates Tommy’s school bus and online lunch account and ID card, and signs him up with Google’s G Suite for Education.

4. While in class, if Tommy speaks without raising his hand, his teacher records the event in his Class Dojo account — an online behavior management tool. The system emits an audible “BONG” for the entire class to hear and adds a demerit to his online profile. Daily and weekly updates are sent to Tommy’s parents via a phone app, text, or email.

7. At home and school, Tommy receives “personalized learning” lessons online. Whether he’s solving math problems via a video game or taking quizzes after reading a story, for-profit technology companies — not his teachers — determine the content and difficulty level of the activity by collecting data and using proprietary algorithms to analyze his abilities, profile his interests, and predict outcomes. This process is known as “data mining.”

14. In high school, Tommy registers for an online course or instructional app in addition to his traditional classes. Some online courses, like those offered by a company called Knewton, collect millions of data points on each student per day. Information Tommy provides online companies may be used to advertise products or programs to him or his parents, based on his personal data.
Sensitive information from surveys

Questions about “school climate,” personal beliefs, political views, social and emotional skills, personal goals, ambitions, interest areas, perceived weaknesses, etc.

9. Sometime during elementary school, Tommy may be asked to complete “school climate” and other surveys measuring his personal beliefs, his political views, or social and emotional skills, often using an online account with his name or other personal information attached to it.

13. By the time Tommy is in middle school, he is encouraged or required to use an online program like Naviance to complete surveys and set personal and academic goals to plan for college. Once in high school, he will be required to use much of the information stored in Naviance to apply for college.
Data from various assessments

Interim assessments, annual standardized exams, College Board’s AP and/or PSAT/SAT, ACT (“voluntary questions” including race and citizenship), Armed Services Vocational Aptitude Battery (ASVAB), etc.

15. In high school, Tommy takes College Board Advanced Placement (AP) courses and exams, the PSAT, SAT, and/or the ACT, before which he will be asked a series of personal questions. The College Board or ACT may then sell his student profile to colleges to help them decide whether to recruit and admit him or not, if he unknowingly gives his consent.

16. When Tommy is a sophomore or junior, his private information may be shared with military recruiters unless his parents revoke their permission in writing. Regardless, his school may administer the Armed Services Vocational Aptitude Battery (ASVAB) exam and release his results to recruiters.

8. Starting as early as Kindergarten, Tommy is assigned interim assessments or test prep to meet district and state requirements. In grades 3 through 8, he takes annual standardized exams in math and English Language Arts (ELA) as required by federal law. He may also be subjected to various local and periodic standardized assessments in these and other subjects. Companies administering these tests often collect an array of sensitive personal information from students, as well as metadata like the amount of time they spend answering a specific question. Essays are often scored by machines rather than people.
Metadata

- Data about other data – including keystrokes, and time spent on a task or test item – especially used in “personalized learning” platforms in 1:1 programs.

11. When Tommy reaches sixth grade or even sooner, his district may implement a 1:1 program. District-provided devices will be issued to each student with default settings that allow companies like Google to track and mine student data, including internet sites visited and search terms used, books and articles read online, videos watched on YouTube, and passwords. Tommy uses this device until he graduates, amassing millions of data points that can be mined to diagnose his learning issues, steer him towards certain courses or careers, or generate a consumer profile that can be sold by data brokers.
WHY PARENTS should be concerned
Data security threats
Data security threats – Federal level

- No specific security provisions in federal law to secure student data.
- 2015 audit by U.S. Department of Education’s Inspector General
  - Found significant weaknesses in 4 out of the 5 security categories.
  - Staff in the Inspector's office hacked into the Dept’s main IT system and gained access to personal data without anyone noticing.
- 2016 government scorecard
  - Created to assess how well federal agencies were implementing data security measures.
  - Awarded the Education Department an overall grade of D.
- 2017 hack of the Free Application for Federal Student Aid (FAFSA) web-based “data retrieval tool”
  - Affected at least 100,000 taxpayers.
Oops.

Ummm ...

We’ll offer ONE member of your family a year of credit monitoring service with Equifax.
Data security threats – Higher education

• Ransomware attacks:
  • In 2016 alone, 13% of "all higher education institutions" experienced a ransomware attack — "where a hacker takes control of the victim’s information systems and encrypts data, preventing the owner from accessing it until the victim pays a sum of money."

• Data breaches:
  • February 2016, University of Central Florida – 63,000 students/staff affected.
  • November 2016, Michigan State University – 400,000 student/staff records affected.
  • June 2017, Oklahoma University – Thousands of student records exposed.
Data security threats – K-12

Schools
• As of October 26, 225 cybersecurity-related incidents have been reported in U.S. K-12 public schools since January 2016. (EdTech Strategies)

Vendors
• Dark Overlord hackers targeted Johnston School District in Iowa – student names, addresses, student ID numbers, grade levels, and the names of students’ child care centers were posted online. Threatening phone calls and texts to students and their families followed. District confirms the data was hacked from a “vendor.”
• Study by Carnegie Mellon researchers found that Ed-tech startups say they “do not prioritize” student data privacy protections in devising their products. Why? Investors don’t show a “meaningful interest” in the issue.
• Edmodo, in which 77 million accounts were compromised and user information allegedly for sale on the dark web.
Hello,

Safeguarding the trust and security of our users is of the utmost importance to Edmodo. We are reaching out to you because Edmodo recently learned about a security incident potentially affecting the accounts of Edmodo users. We promptly retained leading information security experts to investigate this incident and reported the incident to law enforcement.

Our investigation has now confirmed that user names, email addresses, and hashed passwords were acquired by an unauthorized third party. The passwords were “hashed” (or encrypted) using the strong and robust bcrypt algorithm, and they were also “salted,” which adds an additional layer of security.

We have no indication at this time that any user passwords have been compromised, but we strongly recommend that all users reset their passwords as soon as possible.

To reset your password:
1. Go to the Edmodo website and log in to your account.
2. Click on the “Password Reset” link in the notice at the top of the page.
3. Enter your current password, and then create a new password.

If you used the same password on any other site, we encourage you to change your password there as well.

Thank you for your understanding as we work through this issue together. Protecting the security of our users is critical to Edmodo, and we are committed to providing a safe and secure experience for our users. Please know that we are taking additional steps to increase the security of our platform.

If you have any questions or need assistance resetting your password, please visit the Edmodo website and go to our Support Help Center.

Thanks again for making Edmodo such an amazing community and resource to help all of us on our common goal: Helping all learners reach their full potential.

Sincerely,
The Edmodo Team
Data security threats = Identity theft

“High school kids, almost all of them have a very clean slate when it comes to credit scoring. So they’re trying to gain access to a large volume of teenagers’ [information] that can help them down the road,” he said. “These guys have time. They’re willing to wait a year, two years before they can actually monetize that data.”

Professor Yair Levy, a cybersecurity researcher at Nova Southeastern University
Privacy threats
What is privacy?

pri·va·cy
[prahy-vuh-see; British also priv-uh-see]
noun

1. the state of being apart from other people or concealed from their view; solitude; seclusion.
2. the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone.
3. freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one’s personal data or information, as by a government, corporation, or individual.
4. the state of being concealed; secrecy.
Privacy threats – That we can see

• Security cameras, Radio Frequency ID (RFID) badges, etc.
• Social media monitoring systems used by schools and others.
  • In 2010, a Philadelphia district remotely activated webcams in school-provided laptops to view students in their homes. Over 50,000 screenshots were taken.
  • In 2015, Pearson used student data to monitor social media accounts to identify students who might be leaking test questions or other exam information.
• 1:1 or online “personalized learning” programs with policies that often “require students and parents to acknowledge they have no expectation of privacy whatsoever regarding the device at any time – even if students are allowed to use it for non-school reasons and parents are encouraged to use it too.” (ACLU – Rhode Island)
Privacy threats – Secret predictive analytics

• “Education is the most data-minable industry by far, and it’s not even close.”
• Netflix & Amazon = 1 data point/user/day
• Google & Facebook = 10 data points/user/day
• Knewton = 5,000,000 - 10,000,000 actionable data points/user/day

How is this data used? “Predictive analytics … is used to make predictions about unknown future events. Predictive analytics uses many techniques from data mining, statistics, modeling, machine learning, and artificial intelligence to analyze current data to make predictions about future.”

https://www.youtube.com/watch?v=Lr7Z7ysDluQ
Privacy threats – Secret algorithms

“Algorithms … sort and separate the winners from the losers.”

“We’re being scored with secret formulas that we don’t understand, that often don’t have systems of appeal.”

“Algorithms are opinions embedded in code.”

“We think algorithms are objective, true and scientific … that’s a marketing trick.”

“A lot can go wrong when we put blind faith in big data.”

“Algorithms decide who gets a loan, who gets a job interview, who gets insurance and much more -- but they don't automatically make things fair. Mathematician and data scientist Cathy O'Neil coined a term for algorithms that are secret, important and harmful: "weapons of math destruction."

Privacy threats = Surveillance culture

“We’ve arranged a civilization in which most crucial elements … profoundly depend on science and technology. We have also arranged things so that almost no one understands science and technology. This is a prescription for disaster. We might get away with it for a while, but sooner or later this combustible mixture of ignorance and power is going to blow up in our faces.”

Carl Sagan, 1994
WHAT LAWS EXIST to protect student privacy
Federal laws

FERPA – (Family Educational Rights and Privacy Act, passed in 1974) protects education records collected & maintained by schools (and some of their vendors)

IDEA – (Individuals with Disabilities Education Act, passed in 1975) protects the privacy of children with disabilities

NSLA – (National School Lunch Act, passed in 1946) protects confidential income information used by schools to determine whether child qualifies for Free- or Reduced Priced lunch

PPRA – (Protection of Pupil Rights Amendment, passed in 1978) allows parents to see surveys given at school in advance that asks sensitive questions; & allows them to opt out

COPPA – (Children’s Online Privacy Protection Act, passed in 1998) gives parents some control over information collected online directly from children under 13 in & out of school
Illinois state laws

• **105 ILCS 10/2**
  - Illinois School Student Records Act

• **HB 3527**
  - Passed in 2016
  - Right to Privacy in the School Setting
  - Protects students’ social media passwords and access

• **SB 1796**
  - Passed in 2017
  - Student Online Personal Protection Act
  - Modeled after the California’s 2014 landmark Student Online Personal Information Act (SOPIPA). Bars selling, “targeted advertising” but includes several exceptions
WHAT PARENTS CAN DO
to combat risks to student privacy
Be informed.
Parent Toolkit for Student Privacy

- Introduction: Why should parents be concerned?
- Table of Contents
- Section I: What is student data?
- Section II: Parents’ rights under federal law to protect their children’s privacy
- Section III: Tips for parents looking to protect their children’s privacy
- Section IV: Student privacy best practices for states, districts, schools, and teachers
- Section V: Talking to teachers, schools, and districts about student privacy
- Section VI: Advocating for student privacy in schools, districts, and beyond
- Section VII: Student privacy FAQs
- Appendix A: Request to inspect education records held by the school, district or state
- Appendix B: Sample letter to opt out of disclosure of directory information
- Appendix C: Sample letter to opt out of military recruitment
- Appendix D: Additional questions to ask your teacher or principal
- Appendix E: Sample petition
- Appendix F: Tips for media outreach and sample press materials
- Additional resources

Download your copy at www.studentprivacymatters.org
Section III: Simple tips

At home

• Resist the urge to “sharent” (oversharing your child’s information on social media)
• Consider how a “free app” might be using your child’s information before signing up
• Create usernames and passwords without identifying information
• Place a sticky note over your webcams

At school

• Ask your teachers which classroom apps & online programs your child will be using
• Ask if student accounts can be created with limited identifying information
• If your child was assigned a Gmail account through school, be sure to log out before surfing the net (while at home or at school)
Section VI: Talking to teachers

- How many hours per day will my child be expected to use an electronic device?
- Have programs and apps been vetted for data privacy?
- What data is being collected about my child?
- How can I access the data for my child?
- What data does the school or device provider (e.g., Microsoft, Apple, Google, etc.) have access to when my child is using a school-provided device?
- Additional questions can be found in the toolkit.
THANK YOU!

Contact information:
Rachael Stickland
Parent Coalition for Student Privacy
rachael@studentprivacymatters.org
www.studentprivacymatters.org
@parents4privacy