THE PARENT EXPERIENCE AND PERSPECTIVE– *CRITICAL PRINCIPLES FOR STUDENT PRIVACY*

The Student Data Minefield

Leonie Haimson, Parent Coalition for Student Privacy

Legislative Office Building, Hartford CT

January 21, 2016

www.studentprivacymatters.org

2014: Parent defeat of InBloom

- inBloom Inc. launched in 2013 with more than $100M in Gates Foundation funding

- Designed to collect personal information of millions of public school students in 9 states and districts, including NY.

- Data to be shared with for-profit data-mining software companies –for operational, research or instructional purposes, w/out parental knowledge or consent.

- Personal data to include student names, addresses, grades, test scores, grades, economic and racial status, disciplinary records, disability information and more.

- All legal liability rested with states and districts and starting in 2015, inBloom was supposed to start charging for its services.

What did we learn from inBloom controversy?

- Parents (and many others) had incorrectly 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 learned how FERPA had been weakened.

- We also became fully aware for 1st time how much collection and sharing of student data was already occurring by schools and districts with vendors and other 3rd parties.

- Without any funding or institutional backing, parent activists across the country protested and in April 2014, inBloom closed its doors.

The inBloom controversy kickstarted a huge debate on student privacy. Results:

- 21 states passed 24 new student privacy laws in 2014
- 15 states passed 28 new student privacy laws in 2015
- 5 student privacy bills have been introduced in Congress
- There is now a voluntary student privacy pledge created by the software industry group and signed onto by 220 companies.
- Yet none of these measures are strong enough & don’t provide the same safeguards for notification and consent as HIPAA – and have insufficient oversight and enforcement provisions.

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 FERPA in case of education records.
- Even so, there have been numerous 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.
- Non-stop breaches off clouds in recent years, including Target breach affected up to 110 million customers.
- US Office of Personnel Management breach affected 21M federal employees.
- Data on 6.4 million children just exposed by breach of toymaker VTech .
- Breaches by school districts also frequent.
- inBloom was going to share the entire NY State student database with ConnectEd; after inBloom closed, the company went bankrupt & information for 20 million students transferred 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 (LSDS) in which personal student data would be combined with health and medical information, juvenile justice, Child services – to track children “cradle to the grave.”

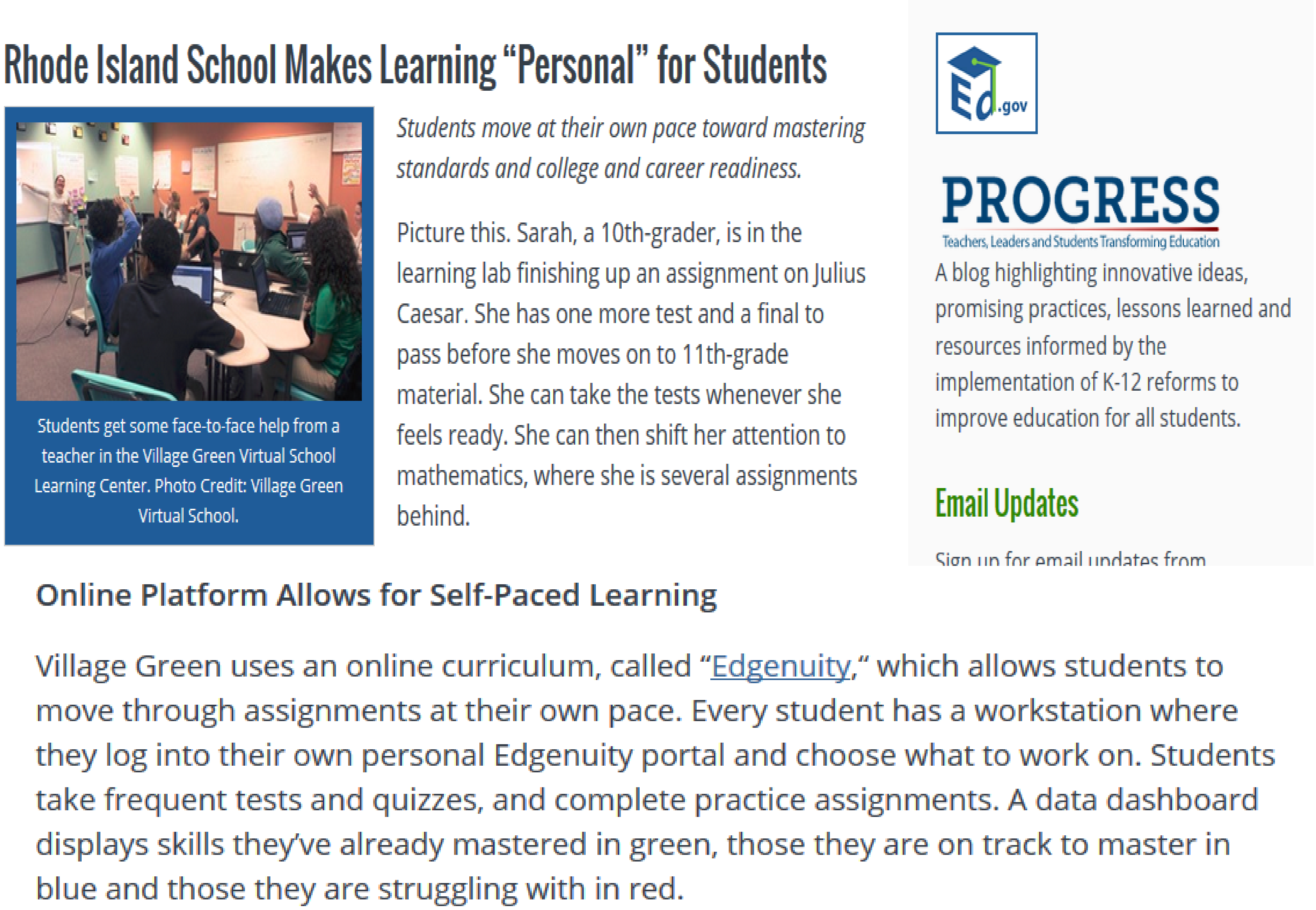
- US ED helped develop Common Education Data Standards, that includes 1500 data pts including health data, early child development info, disciplinary infractions, disabilities, socio-emotional skills, health information, detailed family information & assessment/achievement results.

- NY state officials are planning to put student data in the SLDS into the state archives – potentially forever, with no clear rules or restrictions on access.

Also big push towards online learning which weakens student privacy

- The Alliance for Excellent Education Gates-funded organization that leads Future Ready Schools with US Department of Education
- About 2000 district Superintendents have taken the “Future ready” pledge to transition to digital learning
- “*Future Ready Schools is a comprehensive effort to maximize digital learning opportunities and help school districts move quickly toward preparing students for success in college, a career, and citizenship*.”
- “How much time will it take for the district to complete the transition to digital learning?
- ***The truthful answer to this question is that a district will probably never be “finished.”***

US ED hawking digital learning products



Rhode Island School Makes Learning "Personal" for Students

Students get some face-to-face help from a teacher in the Village Green Virtual School Learning Center. Photo Credit: Village Green Virtual School.

Students move at their own pace toward mastering standards and college and career readiness.

Picture this. Sarah, a 10th-grader, is in the learning lab finishing up an assignment on Julius Caesar. She has one more test and a final to pass before she moves on to 11th-grade material. She can take the tests whenever she feels ready. She can then shift her attention to mathematics, where she is several assignments behind.

Ed.gov

PROGRESS

Teachers, Leaders and Students Transforming Education

A blog highlighting innovative ideas, promising practices, lessons learned and resources informed by the implementation of K-12 reforms to improve education for all students.

Email Updates

Sign up for email updates from

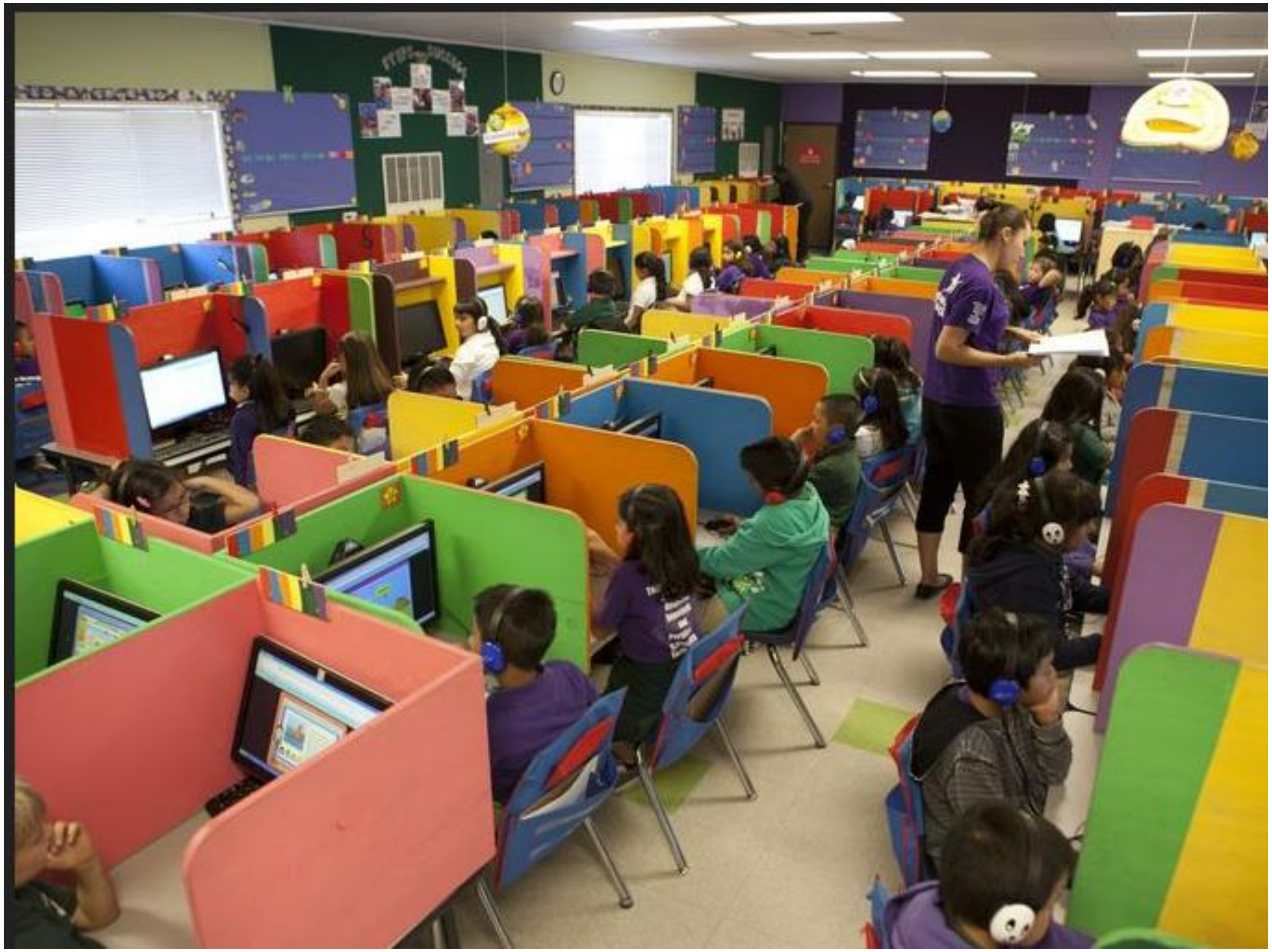
Online Platform Allows for Self-Paced Learning

Village Green uses an online curriculum, called "Edgenuity," which allows students to move through assignments at their own pace. Every student has a workstation where they log into their own personal Edgenuity portal and choose what to work on. Students take frequent tests and quizzes, and complete practice assignments. A data dashboard displays skills they've already mastered in green, those they are on track to master in blue and those they are struggling with in red.

Student review: Edgenuity is a waste of time, not an effective learning tool –

- In several of my high school classes, the corporation Edgenuity's products have been used to replace teachers completely.
- Edgenuity is NOT an adequate replacement, and it has effectively wasted my time, left me frustrated and unhappy, and given me very little substantial knowledge. My first and biggest complaint is the content and the way it is taught.
- Every lesson has a collection of videos- about 10 videos that are 3-4 minutes long in length, interrupted by 2 or 3 questions. The videos feature a teacher and a slide. The teacher reads off the slide, offers a little extra information, and presses the "next" button. The information on the slide is vague, poorly worded, and often biased or completely untrue.
- A prime example? When learning about the origins of religion, my World History class taught me that it was a historical fact that Jesus came back to life 3 days after his death.

Is this the goal of US ED, Gates Foundation & software industry?



Online learning: does it work?

- NO evidence that online learning works to improve student achievement or outcomes in K12– and underlying goal of many is to lessen need for teachers and outsource instruction to private vendors.

- OECD study released in September: "*Students who use computers very frequently at school do a lot worse in most learning outcomes, even after accounting for social background and student demographics*."

- Evidence growing that online learning actually widens the achievement gap between racial and ethnic groups.

- Many studies show that strong and ongoing personal interaction and support from teachers necessary for learning and engagement – especially for disadvantaged students.

- This is why class size reduction – real personalized learning– is especially effective in narrowing achievement gap.

What 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.

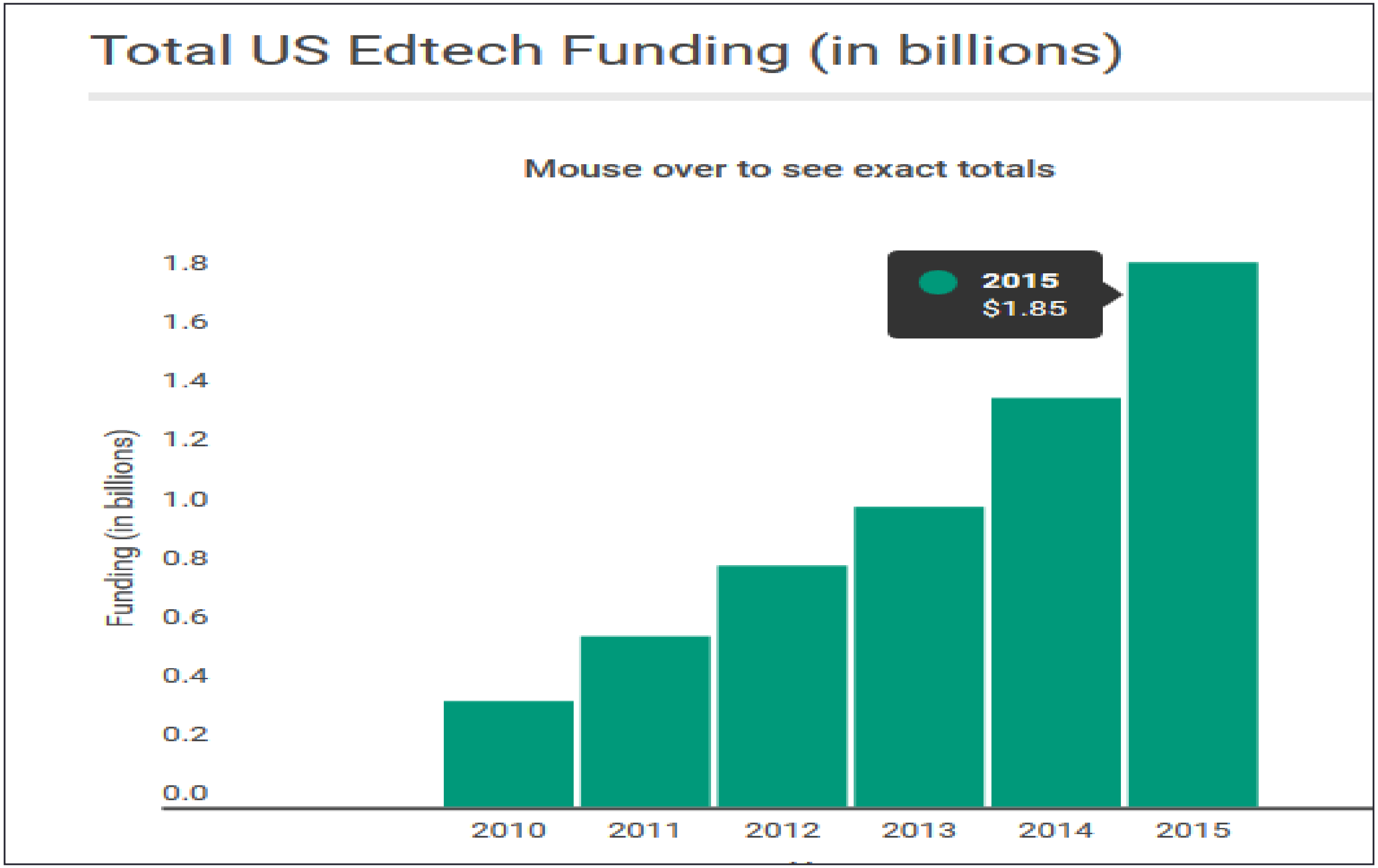
- PreK-12 software ed. tech market estimated at $7.9 *billion*, over $90 billion globally.

- 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.

Ed Tech is big business and is growing fast and in the United States



Data source: <u>EdSurge</u>, 12/21/15

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

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

- Google Apps for Education – pre-installed in Chromebooks or used separately, data-mining personal student data & sued in CA for targeting ads to kids. New FTC complaint for violating student privacy pledge.

- College Board and ACT – sell student data to colleges etc., not just test scores but also lots of personal info that they obtain through online surveys upon registering and before the test administration.

Data collection through PARCC and SBAC exams also threaten student privacy

- After inBloom controversy erupted, PARCC released a very weak privacy policy that allowsfor unlimited redisclosures of personal student data without parental knowledge or consent.
- SBAC has refused to release any privacy policy at all, despite being asked for it by parents in many different states.

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 a strengthened federal student privacy law.
- 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 at every level – including as members of oversight boards for state SLDS .

Parent Coalition for Student Privacy

- We have formed a 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 protections.
- We have fact sheets on the rights parents have under federal law to protect their kids' privacy
- We also help parents write FERPA complaints
- We are now creating parent and teacher privacy toolkits.
- We have developed five privacy principles that every school and district should uphold

Five principles to protect student privacy

- **1. Transparency**: Parents must be notified by their children’s school or district in advance of any disclosure of personally identifiable info to any third parties outside of the school or district.

- All disclosures should require publicly available contracts and privacy policies that specify which data are disclosed for what purposes, and provide a date certain when the data will be destroyed.

- **2. No commercial uses**: Selling of personal student data and; or use for marketing purposes should be banned. ***NO advertising should be allowed on instructional software or websites*** assigned to students by their schools, since ads are a distraction from learning and serve no legitimate educational purpose.

- While some of the current federal and state bills ban “targeted” ads, others ban targeted ads except for those derived from a student’s one- time internet use.   But how can any parent know whether an ad displayed to their children was based on data-mining, either a single time or over a longer period?

Security and enforcement

- **3. Security protections**: At minimum, encryption of personal data at motion and at rest should be required
- Training for all individuals with access to personal student data, audit logs, and security audits by an independent auditor.
- Passwords should be protected in the same manner as all other personal student information.
- There must be notification to parents of all breaches, and indemnification of the same.
- No “anonymized” or “de-identified” student information should be disclosed without verifiable safeguards to ensure data cannot be easily re-identified.
- **4. Enforcement**: The law should specify fines if the school, district or third party violates the law, their contracts and/or privacy policies; with parents able to sue on behalf of their children’s rights as well.
- Without strong enforcement provisions, any law or policy protecting student privacy is likely to be ignored.

Parental and student rights

- **5. Parental/Student rights**: NO re-disclosures by vendors or any other third parties to individuals, sub-contractors, or organizations should be allowed without parental notification and consent (or students, if they are 18 or older).

- Parents must be allowed to see any data collected directly from their child by a school or a vendor delete the data if it is in error or is nonessential to the child’s transcript, and opt out of further collection.

- Any data-mining for purpose of creating student profiles, even for educational purposes, must be done with full parental knowledge.

- Parental consent must be required for disclosure of personal data, especially for highly sensitive information such as their child’s disabilities, health and disciplinary information.

Our toolkits will also share best practices

- No teacher or school should sign up with company that receives personal student data without 1st consulting district and/or state.
- Why? Given complexity of federal laws (not just FERPA, but also COPPA and PPRA) and myriad new state laws, they will likely not have ability to analyze whether vendor’s privacy policy complies with law.
- Difficult w/o expertise to gauge if security protections sufficient.
- Best practice: Ask vendor to adopt full liability for breaches.
- Best practice: whenever possible, ask parents for consent before sharing personal student data, especially sensitive information like disability or disciplinary data.

For more information…

- We have fact sheets on parental rights under FERPA, COPPA, and PPRA as well as 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 & follow us on Twitter @parents4privacy

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 – including in the SLDS.

- 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 Children's Online Privacy Protection Act (COPPA)

- If your child participates in online services at home or school, COPPA applies, regulated by FTC.
- Your school should be providing you with a list of all the online programs that your child participates that gains access your child's personal information, according to FTC "best practice."
- If your child is under-13 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..

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; religious affiliations and beliefs;
- Sexual behavior and attitudes; illegal anti-social, self-incriminating or demeaning behavior;
- Critical appraisals of individuals with whom respondents have close family relationships;
- Privileged relationships, with lawyers, physicians, and ministers;
- 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.
- **3.** In either case, schools and/or their contractors must make these materials or surveys available for inspection by parents ahead of time.