New and emerging threats to student privacy

bbbLeonie Haimson

Co-chair, Parent Coalition for Student Privacy

NPE Conference

info@studentprivacymatters.org

4/30/2022

Parent Coalition for Student Privacy

Privatization comes in many forms – all of them threatening public education as we know it

- More privately run but publicly funded charter schools
- Expansion of vouchers and tax credits going to fund private & religious schools
- Proliferation of ed tech programs, in which personal student data, instruction, assessment and behavior management tools and methods outsourced into hands of private vendors.
- This accelerated during pandemic & school shutdowns.

3 federal laws to protect student privacy all passed before proliferation of ed tech in schools

- 1974: Family Educational Rights and Privacy Act (FERPA), as originally written, prohibited the sharing of personal student data by a school or district with 3rd parties w/o parental consent & enabled parents to access & correct info in their children's files

- 1978: The Protection of Pupil Rights Amendment (PPRA) required parent opt out or consent before surveying students about a certain sensitive information related to sexual & psychological issues; religious or political beliefs: anti-social or criminal activities, and family relationships.

- 1998: the Children's Online Privacy Protection Act, (COPPA) requires operators of online services, websites, games, or mobile applications to obtain permission from parents before collecting personal information online directly from children under 13.

Feds weakened student privacy laws, then inBloom & states stepped in

- To allow for & encourage expanded use of ed tech, online programs & digital learning, US Dept of Education rewrote and weakened FERPA twice through regs, to allow schools/districts to share personal student data w/o parent knowledge of consent. COPPA also weakened through federal guidance

- Parent pushback vs. inBloom - $100M + corporation funded by Gates Foundation to collect personal student data fr/9 states & districts & make it available to private companies to build their tools around it

- inBloom closed in 2014, but controversy it provoked caused at least 43 States to pass 130+ laws student privacy laws to make up for vacuum at federal level

What do these state laws cover?

Many have strong security protections, like requiring encryption for student data (FERPA has none).

Many prohibit the sale or use of student data for marketing purposes.

Many require notifications of breaches

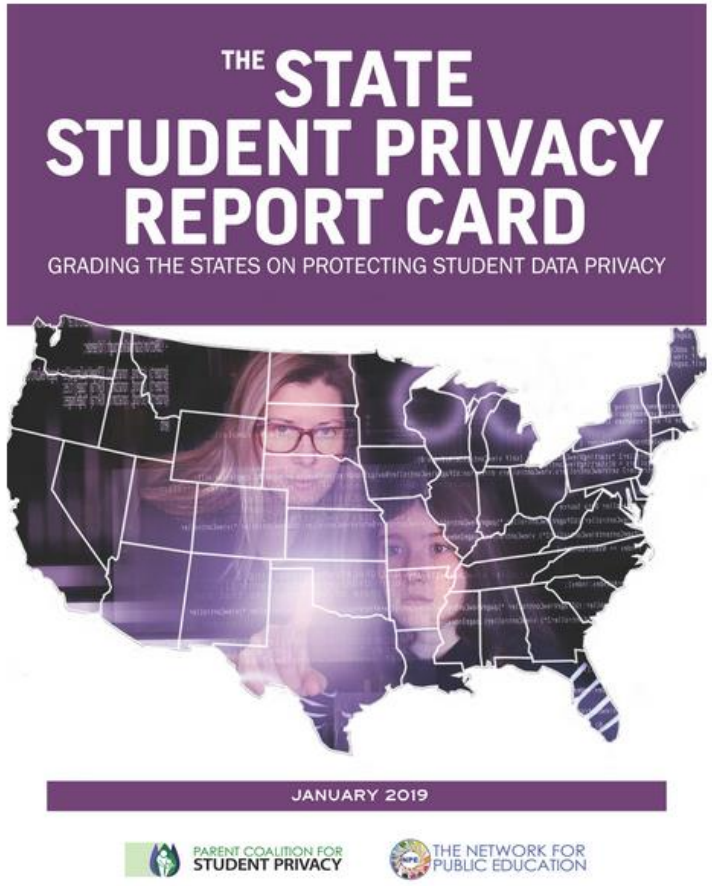
Some require transparency & specific privacy agreements in the contracts with school vendors, & rights for parents to access that data for their kids;

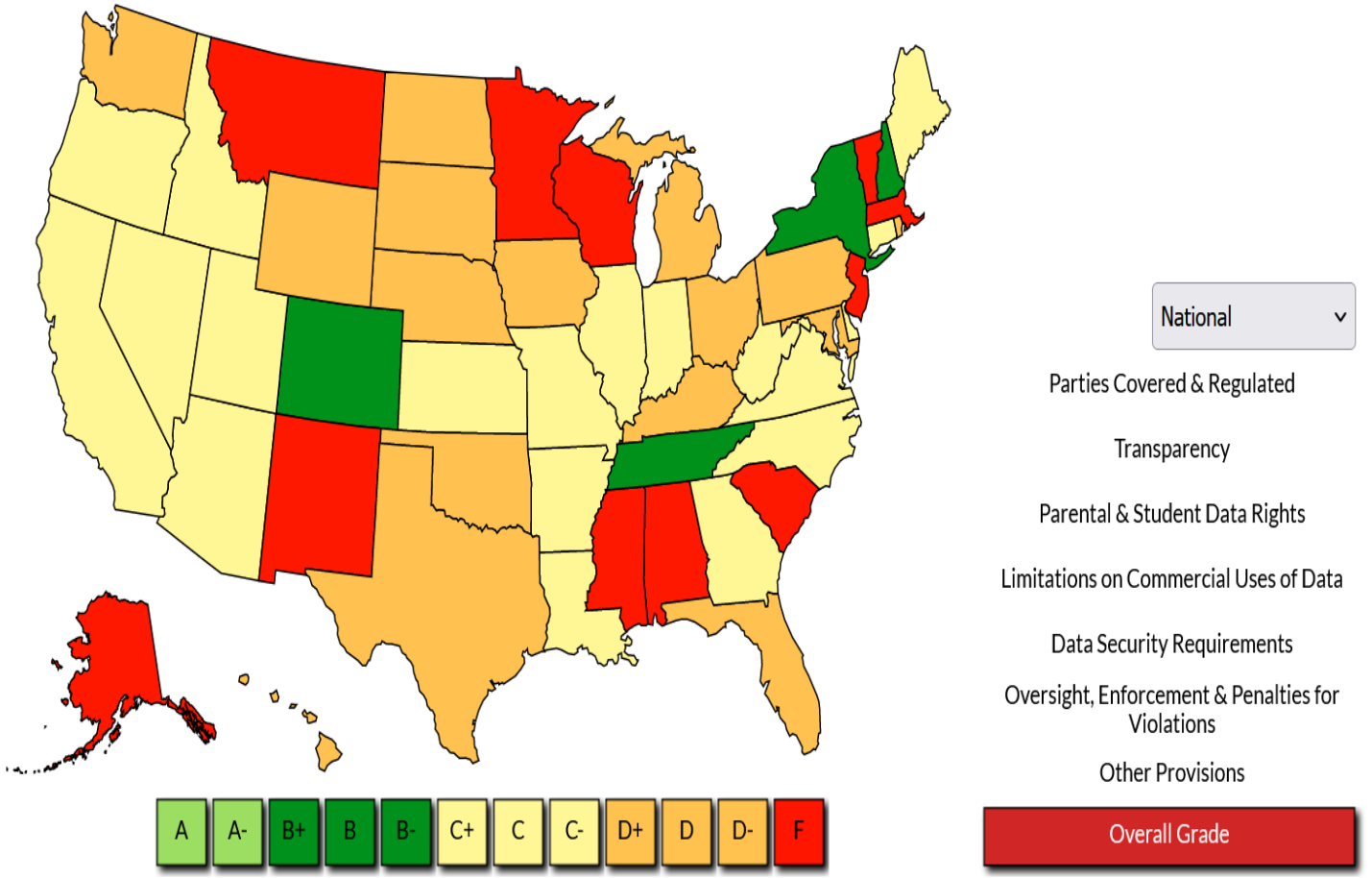
Some call for data minimization & deletion

Many call for penalties & fines for vendors & other third parties who violate privacy/security protections in their contracts

A few deal with protecting teacher data

PCSP & NPE state student report card graded state student privacy laws





And yet there are serious problems with even the strongest of these state laws

- Transparency promised & parent right of access to data rarely provided
- Data minimization & deletions rarely happens either
- No private right of action as in FERPA – parents & students cannot sue if districts or vendors violate the law
- State Ed Depts and State AGs have refused to enforce them

Just some of the controversial vendors used in many districts

- Go Guardian – students surveillance/spyware that many schools use to protect against cheating and check to see if students are engaged; can spy into student homes if not properly configured.
- College Board continues to sell student data collected via AP/PSAT/SAT including student score ranges to colleges – in violation of law in many states, including CA, NY and IL.
- Naviance – makes $ by allowing colleges by surveying students without parent knowledge, collecting their data, and sells access to colleges to market to families in discriminatory ways.
- Kinsa thermometer that parents in many districts encouraged to use during pandemic captures student health data remotely; uses that data to market products to families & unclear if data is encrypted.

Also: proliferation of surveys called “social emotional screeners”

- These are regulated by PPRA if they asks about certain sensitive topics and require parental consent if they are mandatory
- And yet by calling them “screeners” vs. surveys, districts are claiming they aren’t subject to these restrictions
- Some screeners including ones we’ve seen from WA state ask incredibly intrusive questions about family relationships, parent or child use of alcohol & drugs, sexual & gender identity etc.

Breaches proliferate including largest ever for single district in NYC

- In late March, NYC Dept of Ed reported that the personal data of about 820,000 NYC students who attended public schools going back to year 2016 had breached.
- Apps called Skedula/Io classroom/Pupil path/ that teachers use to access student PII & communicate w/parents/students.
- Programs owned by Illuminate Edu; since then, breaches of these programs reported in CO, CT, and NYS outside of NYC
- Seems to have occurred during the program's extended shutdown in January, caused by hackers and perhaps when data being transferred from Google to Amazon cloud

How to improve security/privacy practices

- Prohibit teachers using clickwrap agreements or “freemium”
- Disallow use of any programs/apps not screened for privacy/security protections
- Require strong encryption & independent privacy & security audits
- Minimize vendor access to data they absolutely need to provide specific services
- Require vendor to delete data as soon as possible & certainly when student graduates or moves out of district

College Transparency Act

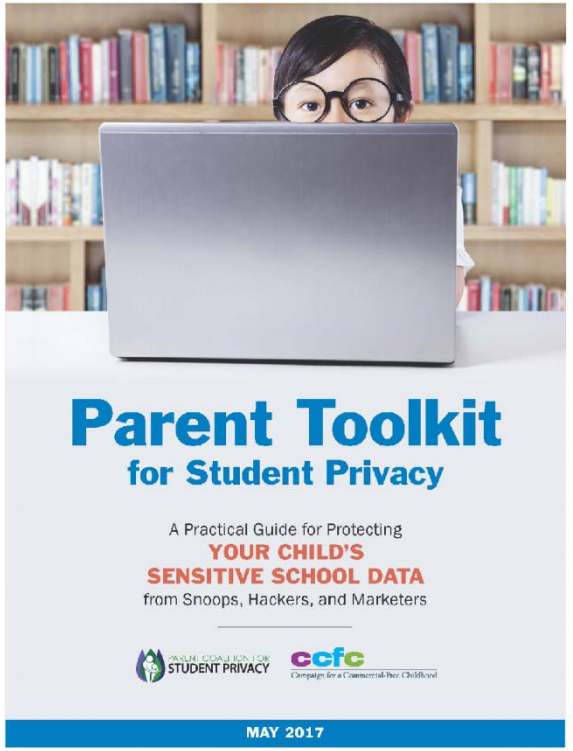
- Bill now being considered in Congress to authorize feds to track every student enrolled in college through life
- Information to include their names, age, grades, test scores, attendance, race and ethnicity, gender, and economic status, collected directly from their colleges, along with their disabilities and/or “status as a confined or incarcerated individual.”
- As students move through life, this data could be “matched” with their personal data from the other federal agencies, including the Census Bureau, the DoD, Social Security Admin & perhaps others.
- NO ability for students to opt out or ever have data deleted.
- You can send a message to Congress opposing this bill from our website at https://tinyurl.com/No2CTA

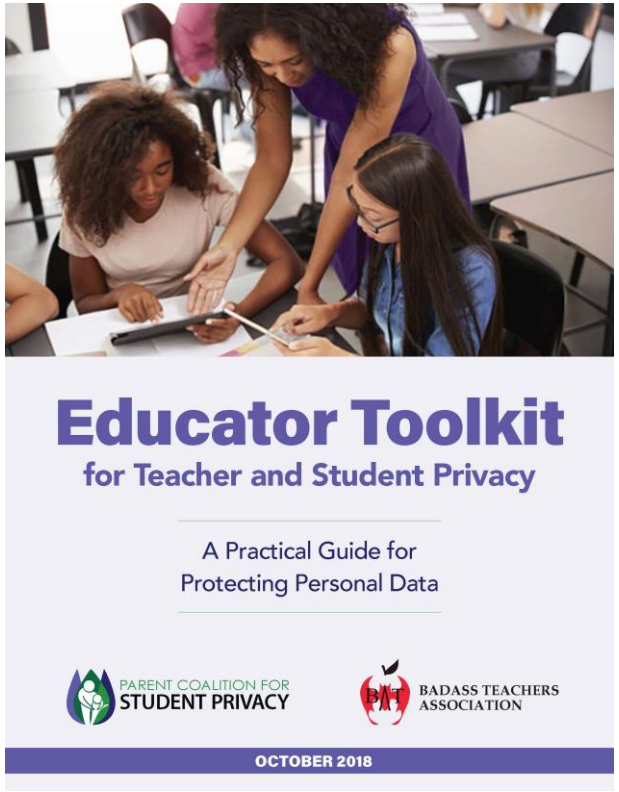
For more info, visit the Parent Coalition for Student Privacy

www.studentprivacymatters.org

Email us at:
Info@studentprivacymatters.org

Follow us @parents4privacy





Download free copies