Keeping our children’s educational data private and secure in an era of big data

Ubiquitous use of computers and digital devices in public schools means **ever larger amounts of data are being collected about and from students**. Parents are concerned that current state and federal statutes are inadequate to ensuring that student privacy is protected and that all children have access to a free and appropriate public education—regardless of the digital divide that many families in our state still face.

- In CPS, schools are **monitoring student website history usage even at home, off school grounds and outside of school hours** via the cps.edu login on Chrome browsers. This is a blatant violation of student and family privacy. This tracking has been publicly confirmed by at least one CPS principal. Parents and students are not notified of or granted consent for this tracking.

- A new software system developed by Facebook, Summit Personalized Learning Platform, collects comprehensive data about students: grades, test scores, assignments, possibly keystrokes and web history. Previously Summit asked for parental consent for participation, but no longer do so. **Students have no alternative for instruction if parents object to data collection** and storage because the system replaces core coursework and instruction entirely. Summit is being used in at least 13 public schools in IL.

- Parents in south suburb were told that their kindergartener had **no alternatives other than private or home-schooling to their child’s participation in Pearson AIMSweb testing** which required providing child’s PII to be shared with and stored by Pearson. Ultimately, after parents secured legal assistance, district compromised and let them use pseudonym for child and attach no personally-identifiable information to the Pearson account.

- CPS elementary school is **surveying children about sensitive social-emotional issues via an unsecured Google form** attached to their cps.edu account. Parents were not notified about survey (in violation of federal law) and when questioned, school would only agree to remove individual student data.

- CPS has data security and privacy constraints for paid vendors with district-level contracts, but **freeware providers are unmonitored and unconstrained**. Countless sites and apps are in use, but parents are rarely if ever notified about such programs, much less asked for consent; terms of service often simply say that responsibility for consent lies with teachers and administrators. For example, one CPS school shared student test score data with Khan Academy without parental notification; parents only heard about this in passing at Local School Council meeting.

- Programs like ClassDoJo store and share **large amounts of highly sensitive behavioral data about students**, including things like bathroom usage or harsh negative evaluations (“disrespectful”, “uncooperative”, “lack of persistence”). But as a free site, they aren’t constrained by same oversight that paid vendors with district-level contracts receive.

- **Ransomware** incidents in IL, where public school district data is hacked and then offered back to a district for thousands of dollars, include one in Oct 2017 in Crab Orchard (IL House 17) and one in Pekin (IL House 91) in April 2017. Additional **school data hacking** incidents in Illinois since Jan 2016: Urbana (IL House 103), Morton (IL House 88) and Abingdon (IL House 93).

- In schools with 1-to1 device programs, families and students, including elementary-aged students, are asked to sign agreements for **financial responsibility for devices regardless of their ability to pay**. Students may be required to do homework online even if they have limited access to high-speed internet and computers outside of school hours.