# Privacy & Technology in Schools Today and in the Future

**A talk with Joel Reidenberg**

## I. Students' Privacy Rights

A. Third party vendors
   1. A third party vendors use children's test scores for commercial uses, such as advertising certain educational products based on the child's academic needs.
   2. A majority of school districts use an outside, cloud-based services but only a few actually sign written agreements with those vendors protecting students' educational data.

B. Family Educational Rights and Privacy Act of 1974 (FERPA)
   1. Applies to educational institutions that receive federal funding.
   2. FERPA guarantees parental or guardian access to records and limits disclosure of records to others
   3. At age 18, FERPA rights transfer to the student
   4. Information can be disclosed to school officials who have a "legitimate education interest" in the records. Schools must use "reasonable methods" to make sure that only those records that serve legitimate educational interests are available to administrators.[1]

C. Protection of Pupil Rights Amendment of 1978 (PPRA)[2]
   1. PPRA, or the Hatch Amendment, requires that schools that receive federal funding must get written parental consent before a student may participate in certain surveys or evaluations.
   2. Guardians may also choose to opt their child out of sharing certain information with the school.

D. Children's Online Privacy Protection Act of 1998 (COPPA)
   1. COPPA requires parental consent if a website gathers information directly from children under 13.
   2. In certain circumstances, schools may act *in loco parentis.*
   3. The Federal Trade Commission (FTC) is responsible for regulating and enforcing COPPA.
   4. COPPA has been criticized as ineffective and potentially unconstitutional.
      a. COPPA attacks children's rights to freedom of speech and self-expression.
      b. Age restrictions and the "parental consent" process are easy for children to circumvent. The law does not prevent kids from accessing pornography or lying about their age.

---

[1] Steven J. McDonald, A FEW THINGS ABOUT E-FERPA POLICY SPOTLIGHT, AN EDUCAUSE REVIEW ONLINE BLOG (2013), https://www.educause.edu/blogs/smcdonal/few-things-about-e-ferpa.

[2] Lynn M. Daggett, *Student Privacy and the Protection of Pupil Rights Act as Amended by No Child Left Behind*, 12 UC DAVIS J. JUV. LAW POLICY 51–132 (2008).

c. Parents, not government, should be responsible for protecting children online

E. Children's Internet Protection Act of 2000 (CIPA)
   1. CIPA imposes certain requirements on schools or libraries that receive discounts for internet access through its "e-rate program," which makes certain communications services and products more affordable for eligible schools and libraries.
   2. In 2001, the FCC issued rules implementing CIPA. It provided updates to those rules in 2011.[3]

F. No Child Left Behind Act (NCLB)
   1. Language in Section 1061 of the Act is adopted from the tabled Student Privacy Protection Act of 2001 (Senate Bill 290).
   2. NCLB mandates that local educational institutions and schools must: [4]
      a. Adopt policies giving adult students and parents of minor students the right to inspect any survey created by a third party before it is administered in school
      b. Notify parents and adult students about and allow them to decline to participate in surveys that collect information from students on certain subjects.
      c. Notify parents and adult students about in-school surveys conducted for sales or marketing purposes and allow them to opt out of participation.
      d. Notify parents and adults students about nonemergency, invasive physical examinations and allow them to opt out.
      e. Allow parents to inspect any instructional material used in the classroom.
      f. Provide at minimum yearly notice of the privacy policies that are adopted.

## II. Data

A. Online educational services and student metadata
   1. Online educational services increasingly collect a large amount of metadata. Metadata refers to information that provides meaning and context to other data being collected; for example, information about how long a particular student took to perform an online task has more meaning if the user knows the date and time when the student completed the activity, how many attempts the student made, and how long the student's mouse hovered over an item (potentially indicating indecision).[5]

---

[3] *Children's Internet Protection Act*, https://www.fcc.gov/guides/childrens-internet-protection-act.

[4] EPIC, *No Child Left Behind*, https://epic.org/privacy/student/no-child-left-behind/default.html.

[5] PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES, (2014), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

2. Metadata that has been stripped of all direct and indirect identifiers is not considered protected information under FERPA. Schools and districts need to evaluate the use of online educational services on a case-by case basis to determine if FERPA-protected information is implicated. Schools should consult with professionals to determine how to best "de-identify" information gathered from students.[6]

B. Access to student cell phones
   1. A lawsuit is unfolding in North Carolina after school officials searched a student's phone and found nude images of the student himself. The student is being charged (as an adult) with possessing child pornography.[7]
      a. This case is not unique. Similar cases have unfolded nationwide since at least as early as 2009.[8]

C. Wearable technologies
   1. As smartwatches and fitness trackers become more popular, schools are increasingly banning the devices from classrooms
   2. Schools are concerned students may use the devices to access test answers online or to transmit test information to other students[9]

D. *Robbins v. Lower Merion School District* (2010) and school-issued technologies
   1. School administrators spied on students at home through remotely activated webcams in school-issued laptops. Parents and guardians had not been informed of, nor consented to, this capability.
   2. Ultimately, the school district paid damages in a civil settlement. Criminal charges were not pursued.[10]

E. School access to student technology
   1. School owned technology
      a. Some schools distribute ipads or laptops to its students for educational use. When the school owns the equipment, they generally have the right to access the information on it.
   2. Robbins v. Lower Merion School District
      a. A high school in Pennsylvania activated the webcams on school provided laptops in order to watch students while they were at home.
   3. Internet use

---

[6] PROTECTING PRIVACY IN CONNECTED LEARNING TOOLKIT: CONSIDERATIONS WHEN CHOOSING AN ONLINE SERVICE PROVIDER FOR YOUR SCHOOL SYSTEM, (2014), http://www.cosn.org/sites/default/files/Privacy Toolkit_0319.pdf.

[7] Michael E. Miller, *N.C. just prosecuted a teenage couple for making child porn — of themselves*, THE WASHINGTON POST, September 21, 2015, https://www.washingtonpost.com/news/morning-mix/wp/2015/09/21/n-c-just-prosecuted-a-teenage-couple-for-making-child-porn-of-themselves/.

[8] Clay Calvert, *Sex, Cell Phones, Privacy, and the First Amendment: When Children Become Child Pornographers and the Lolita Effect Undermines the Law*, 18 COMMLAW CONSPEC. J. COMMUN. LAW POLICY 1 (2009).

[9] CNN, *From smartwatch and smartpen... to smartcheat?*, http://www.cnn.com/2014/06/19/business/high-tech-cheating/index.html.

[10] CBSNews, $610K SETTLEMENT IN SCHOOL WEBCAM SPY CASE, http://www.cbsnews.com/news/610k-settlement-in-school-webcam-spy-case/.

   a. Many states have laws requiring schools to monitor and block students' internet activity on school grounds.
4. Social media accounts
   a. Schools may not directly monitor students' social media accounts unless there are threats of bullying or suspicion of an illegal activity.
   b. The Glendale School District in California hired an outside technology firm, Geo Listening, in order to monitor students social media posts. The firm does not specifically state what methods they use to monitor students.
   c. Huntsville City Schools system in Alabama started Students Against Fear (SAFe), an organization where students, teachers, and parents can submit tips about cyber bullying. Once a tip is submitted, the school system would search a student's social media accounts.