epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Khaliah Barnes
Director, EPIC Student Privacy Project
Electronic Privacy Information Center

on

Ensuring Student Privacy in the Digital Age

before the

Education Committee and Select Committee on Privacy
California State Assembly

May 14, 2014

Assembly Member Buchanan, Assembly Member Chau, and Members of the Education Committee and Select Committee on Privacy, thank you for the opportunity to participate in today's joint hearing on "Ensuring Student Privacy in the Digital Age." My name is Khaliah Barnes and I am the Director of the EPIC Student Privacy Project at the Electronic Privacy Information Center ("EPIC").

EPIC is a non-partisan research organization in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] We work with a distinguished panel of advisors in the fields of law, technology, and public policy.[2] EPIC has a particular interest in protecting student privacy and has worked in this field for many years.[3] For example, in 2005, EPIC, joined by more than 100 local, state, and national organizations, urged then Secretary of Defense Donald Rumsfeld to end the "Joint Advertising and Market Research Studies" military Recruiting Databases because it did not have sufficient privacy protections.[4] This massive database contains troves of information, including student information (*e.g.*, grade point average, graduation date), date of birth, address, and ethnicity.[5] Because of EPIC's efforts, the Defense Department granted individuals the right to opt-out of the database.[6]

In 2011, EPIC filed an *amicus* brief in *Chicago Tribune v. University of Illinois*, a case involving student privacy rights protected by FERPA.[7] EPIC's brief argues that Congress intended to protect student records, including admissions files, from unauthorized release and that Illinois' open government law must yield to the federal privacy law.

In 2012, EPIC and other privacy organizations issued a position paper calling for moratorium on RFID tracking in schools.[8] The position paper warned that RFID tracking in schools compromised student privacy, civil liberties, and First Amendment rights.

---

[1] *About EPIC*, EPIC, http://epic.org/epic/about.html (last visited May 13, 2014).
[2] *EPIC Advisory Board*, EPIC, http://epic.org/epic/advisory_board.html (last visited May 13, 2014).
[3] *Student Privacy*, EPIC, http://epic.org/privacy/student/ (last visited May 13, 2014).
[4] Letter from Privacy Coalition to the Hon. Donald H. Rumsfeld (Oct. 18, 2005), *available at* http://privacycoalition.org/nododdatabase/letter.html.
[5] *Defense Privacy and Civil Liberties Office—Privacy—System of Records Notices (SORNs)—DoD Wide Notices—DHRA 04*, DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE, http://dpclo.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/6839/dhra-04.aspx (last visited May 13, 2014).
[6] *Id*.
[7] *Chicago Tribune v. University of Illinois*, EPIC, http://epic.org/amicus/tribune/ (last visited May 15, 2013.
[8] CONSUMERS AGAINST SUPERMARKET PRIVACY INVASION AND NUMBERING (CASPIAN), ELEC. PRIVACY INFO. CTR. (EPIC), AND PRIVACY RIGHTS CLEARINGHOUSE, POSITION PAPER ON THE USE OF RFID IN SCHOOLS (Aug. 21, 2012), *available at* http://www.spychips.com/school/RFIDSchoolPositionPaper.pdf

Earlier this year, EPIC held a public panel featuring prominent student privacy experts discussing the current state of student privacy.[9] At the event, Senator Ed Markey (D-MA) announced his intentions to introduce new student privacy legislation.

We appreciate the Assembly's interest in protecting student privacy. In my statement today, I will: (1) describe how the current regulatory framework encourages mass collection of student records; (2) discuss the privacy risks that students today face; (3) underscore the need for data security safeguards; and (4) recommend that California adopt the Student Privacy Bill of Rights to ensure student privacy in the digital age.

I. The Current Student Privacy Regulatory Framework Encourages Mass Collection of Student Records

The Family Educational Rights and Privacy Act ("FERPA") is a federal student privacy that grants students the right to control who has access to their information.[10] FERPA also permits students to access and amend their records.[11] In enacting FERPA, it was Congress's intent that "parents and students may properly begin to exercise their rights under the law, and the protection of their privacy may be assured."[12] Congress enacted FERPA in response to "the growing evidence of the abuse of student records across the nation."[13] Senator James Buckley, one of FERPA's principal sponsors, emphasized the "larger problem of the violation of privacy and other rights of children and their parents that increasingly pervades our schools."[14] FERPA's purpose is to "affirm the privacy and rights of children and their parents," ensure parental access to student information, and extend the "personal shield for every American against all invasions of privacy" to students.[15]

As it was originally adopted, FERPA provided the necessary safeguards to protect students from harm. Over the last several years, however, the Education Department has issued regulations interpreting FERPA that have significantly diminished students' control over their education records. These regulations, issued in 2008 and 2011, grant companies, government agencies outside of the education space, and other third party entities access to sensitive student information.[16]

---

[9] *Failing Grade: Education Records and Student Privacy*, EPIC, http://epic.org/events/student-privacy14/ (last visited May 13, 2014).
[10] 20 U.S.C. § 1232g.
[11] Id. § (a)(1)-(2).
[12] 120 Cong. Rec. 39,863 (1974).
[13] 121 Cong. Rec. 7,974 (daily ed. May 13, 1975) (remarks of Senator Buckley).
[14] 120 Cong. Rec. at 13,951-52.
[15] *Id*.
[16] Family Educational Rights and Privacy Act Final Regulations, 73 Fed. Reg. 74,806 (Dec. 9, 2008); Family Educational Rights and Privacy Act Final Regulations, 76 Fed. Reg. 75,604 (Dec. 2, 2011).

In 2012, EPIC sued the Education Department over its 2011 FERPA regulations.[17] The regulations removed limitations prohibiting educational institutions and agencies from disclosing student personally identifiable information without first obtaining student or parental consent. Specifically, the Education Department's regulations reinterpreted FERPA statutory terms "authorized representative," "education program," and "directory information."[18] This reinterpretation gives non-governmental actors increased access to student personal data. In our lawsuit, we argued that under the Administrative Procedure Act, the Department's 2011 regulations amending FERPA exceed the agency's statutory authority and are contrary to law. EPIC's lawsuit followed detailed comments we submitted to the agency, explaining the purpose of FERPA, the importance of student privacy, and the growing privacy risks that third parties present when granted access to intimate student information.[19] We urged the agency to withdraw its proposed changes. It was only after the agency failed to act on our recommendations that we chose to file the lawsuit.

In September of last year, the Court dismissed the case on procedural grounds. Importantly, the court never reached the substantive issue as to whether the Education Department had the legal authority to change the student privacy law.

By removing FERPA's well-established limitations on student record dissemination, the Education Department permitted and encouraged third party access to student records. And in response, there has been an overwhelming demand for private student information.

II. Big Data's Mass Sensitive Student Data Collection Presents Big Risks for Student Privacy

Pursuant to the Education Department's regulations, schools, private companies, and government agencies collect personal student information on an unprecedented scale. Student data collection is no longer limited to test scores and attendance records. The current Big Data environment increasingly demands personal student data. For example, statewide longitudinal databases, which track students from prekindergarten into the workforce, collect a range of student information, including:

- Name
- Date of Birth
- Gender
- Parents' name, address
- Where they attended preschool or Head Start
- Early assessments and interventions

[17] *Elec. Privacy Info. Ctr. v. U.S. Dep't of Educ.*, CV 12-0327 (ABJ), 2014 WL 449031 (D.D.C. Feb. 5, 2014).
[18] 2011 regulations, *supra* note 16.
[19] *Comments of the Elec. Privacy Info. Ctr. to the Dep't of Educ., Notice of Proposed Rulemaking, RIN 1880-AA86*, May 23, 2011, *available at* http://epic.org/privacy/student/EPIC_FERPA_Comments.pdf.

- Suspension, expulsion
- Kindergarten readiness
- School(s) attended: state test scores & percentiles, enrollment, etc
- Economically Disadvantaged
- Race/Ethnicity; English Language Learner
- Migrant
- Remedial
- Promoted/Retained (held back)
- Gifted/Talented
- Special Education: dates of eligibility determinations and individualized education plan review.
- Annual state test scores and percentiles starting in 3rd grade
- Identities of teachers
- Grades, attendance, suspension/expulsion, grade promotion
- Specific courses taken, including AP, and grades earned
- Did you graduate on time?
- Why did you leave school? Aged out; Expelled; Court order; Arrested; Incarcerated; Pregnant
- If you left school, where did you go? Transfer/Dropout/Home school/GED
- Did you go to college?
- If so, was it in-state/public? Which one? (Some states share with private and for-profit colleges too)
- If In-state/public, did you need remediation? In Math or English or both?
- Did you graduate college?[20]

Plans are already underway to include personalized learning analytics and information detailing whether students ends up on welfare or in jail after high school.[21]

Schools in California and other states are foregoing traditional roll calls and replacing them with GPS and RFID trackers to monitor students, in real time, throughout the day.[22] This type of enhanced tracking not only reveals a student's presence at school, but also her personal

[20] Anya Kamenetz, *What Parents Need to Know About Big Data and Student Privacy*, NPR: ALL TECH CONSIDERED (Apr. 28, 2014, 11:58AM), http://www.npr.org/blogs/alltechconsidered/2014/04/28/305715935/what-parents-need-to-know-about-big-data-and-student-privacy.

[21] *Id.*

[22] Eric Carpenter, *Kids Who Skip School are Tracked by GPS*, ORANGE COUNTY REGISTER (Aug. 21, 2013, 1:17 PM), http://www.ocregister.com/articles/school-288730-students-program.html; *Texas School District Uses GPS to Track Students Who Skip Classes*, THE ASSOCIATED PRESS (Jan. 6, 2013, 12:38PM), http://www.oregonlive.com/today/index.ssf/2013/01/texas_school_district_uses_gps.html.

comings and goings, like to the school nurse or psychologist. Schools also collect biometric data –fingerprints, palm and iris scans— and Social Security numbers with little oversight.[23]

Private companies, too, have an insatiable appetite for student information. For example, last year, EPIC filed a complaint with the Federal Trade Commission concerning Scholarships.com, a popular website among high school students researching college scholarships.[24] The website encouraged students to share intimidate details, including religious affiliation, and health information, including whether the student has ADD/ADHD, hepatitis, cancer related medical issues, digestive or mental impairments, and whether the student is clinically depressed or overweight.[25] The website also encouraged students to divulge whether they have current alcohol addictions or are recovering alcoholics; have parents who are illegal immigrants; are domestic abuse victims; have drug addictions or convictions; are lesbian, gay, bisexual, transgender ("LGBT") or have an LGBT parent; and are political activists.[26] The website did not disclose that it would provide this student data to its business partner for general advertising purposes.[27]

More recently, Google, whose services are used in many California schools, has been under fire for illegally reading student emails for commercial purposes.[28] Google has since stated that it has "permanently removed all ads scanning in Gmail for Apps for Education" which, according to Google, means that it cannot "collect or use student data in Apps for Education services for advertising purposes."[29] These are just a handful of examples in the growing trend of mass student data collection.

This type of unbounded intimate data collection greatly increases the risks that students will be stigmatized, and that transgressions and shortcomings from the classroom will follow students for the rest of their lives. In fact, concerns about the long lasting implications of student data collection galvanized Congress to pass FERPA. FERPA's legislative history discusses *Merriken v. Cressman*, a federal case analyzing the privacy implications of a school program designed to identify potential eighth grade drug abusers.[30] Although the case is over forty years

---

[23] Brian Heaton, *State Legislatures Grapple with Biometrics Use in Schools,* GOVERNMENT TECHNOLOGY (Apr. 17, 2014), http://www.govtech.com/State-Legislatures-Grappling-with-Biometrics-Use-in-Schools.html; *Social Security Number Privacy*, UNIVERSITY OF FLORIDA, http://privacy.ufl.edu/privacy/social-security-number-privacy/ (last visited May 13, 2014).
[24] *In the Matter of Scholarships.com, LLC* (Dec. 12, 2013), *available at* http://epic.org/privacy/student/EPIC-FTC-Compl-Scholarships.com.pdf.
[25] *Id*.
[26] *Id*.
[27] *Id*.
[28] Benjamin Herold, *Google Under Fire for Data-Mining Student Email Messages*, EDUCATION WEEK (Mar. 26, 2014), http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html.
[29] *Protecting Students with Google Apps for Education*, GOOGLE (Apr. 30, 2014), http://googleenterprise.blogspot.co.uk/2014/04/protecting-students-with-google-apps.html.
[30] *Merriken v. Cressman*, 364 F. Supp. 913, 915 (E.D. Pa. 1973).

old, it bears many similarities to today's environment where mass student data collection is espoused, but rarely vetted. The court found that

> letters to the parents were 'selling devices' aimed at gaining consent without giving negative information that would make the parents completely aware of 'the relevant circumstances and likely consequences' of the Program . . . the letter to the parents gave only one side of the test picture. There were no statements to the parents concerning the self-fulfilling prophecy, scapegoating of those children who opted not to participate or the ultimate use of the data as it would effect their children and law authorities who might find it necessary to use that information . . .[31]

The court ultimately held that this invasive student data collection violated students' and parents' "right to privacy inherent in the penumbras of the Bill of Rights of the Untied States Constitution."[32] *Merriken v. Cressman* illustrates "the potential harm that can result from poorly regulated testing, inadequate provisions for the safeguarding of personal information, and ill-devised or administered behavior modifications programs."[33]

Through FERPA, Congress aimed to ward against the problems that currently plague student privacy. But, as discussed above, the Education Department's regulations substantially set student privacy back.

III. There are No Adequate Data Security Safeguards to Protect Against Unauthorized Access to Student Records

Despite removing FERPA's privacy safeguards, the Education Department has declined to ensure student data protection. The Department itself has recognized that data security is an "essential part of complying with FERPA as violations of the law can occur due to weak or nonexistent data security protocols."[34] Yet, the Department "does not believe it is appropriate to regulate specific data security requirements under FERPA."[35] Students have had their information continuously compromised "due to weak or nonexistent data security protocols."[36]

For example, in 2009, Fordham Law School's Center on Law and Information Policy conducted a study on the privacy protections in statewide K-12 longitudinal databases.[37] The study underscores the current problems with student data security. Among its other findings,

---

[31] *Id*. at 919.
[32] *Id*. at 922.
[33] 120 Cong. Rec. 14,581.
[34] 2011 regulations, *supra* note 16, at 75,622.
[35] *Id*.
[36] *Id*.
[37] FORDHAM LAW SCHOOL CTR. ON LAW AND INFO. POLICY, CHILDREN'S EDUCATIONAL RECORDS AND PRIVACY: A STUDY OF ELEMENTARY AND SECONDARY SCHOOL STATE REPORTING SYSTEMS (2009).

Fordham found that "most states collected information in excess of what is needed" for government reporting requirements," student databases "generally had weak privacy protections," "many states do not have clear access and use rules regarding the longitudinal database," most states "fail to have data retention policies," and "several states . . . outsource the data warehouse without any protections for privacy in the vendor contract."[38]

Additionally, recent large-scale security breaches at educational institutions have compromised student (and faculty) privacy. In February of this year, a University of Maryland ("UMD") database containing 309,079 student, faculty, staff, and personnel records was breached; the "breached records included name, Social Security number, date of birth, and University identification number" and included records covering a span of 20 years.[39] The university acknowledged that it could have implemented privacy enhancing techniques by purging some of those records "long before the breach."[40] Soon after the UMD breach, Indiana University reported that it had stored names, addresses, and Social Security numbers for "approximately 146,000 students and recent graduates" in an "insecure location" for almost a year, thus potentially exposing students to identity theft and other forms of fraud.[41] More recently in California, the San Juan School District "discovered that certain data files containing sensitive personal information were exposed to online access for approximately two weeks."[42] Private companies have also failed to adequately safeguard student information. Scholarships.com, the aforementioned company that collected sensitive student information, was unencrypted. And last year Edmodo, a popular online learning system was also under fire for not encrypting its system.[43]

[38] FORDHAM LAW SCHOOL CTR. ON LAW AND INFO. POLICY, CHILDREN'S EDUCATIONAL RECORDS AND PRIVACY: A STUDY OF ELEMENTARY AND SECONDARY SCHOOL STATE REPORTING SYSTEMS EXECUTIVE SUMMARY (2009).
[39] Letter from Brian D. Voss concerning UMD Data Breach, Feb. 21, 2014, http://www.umd.edu/datasecurity/.
[40] Mark Albert, *UMD Testifies to Congress on Massive Data Breach*, WUSA 9, Mar. 27, 2014, http://www.wusa9.com/story/news/local/2014/03/26/university-of-maryland-congress-data-breach/6942023/.
[41] Press Release, Indiana University, Indiana University Reports Potential Data Exposure (Feb. 25, 2014), news.iu.edu/releases/iu/2014/02/data-exposure-disclosure.shtml.
[42] *Frequently Asked Questions*, CSID, http://www.csid.com/sanjuan/ (last visited May 13, 2014).
[43] Natasha Singer, *Data Security Is a Classroom Worry, Too*, N.Y. TIMES, June 22, 2013, at BU1, *available at* http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html?_r=0.

IV. California Should Adopt the Student Privacy Bill of Rights, an Enforceable Student Privacy and Data Security Framework

Earlier this year in the *Washington Post*, EPIC unveiled the Student Privacy Bill of Rights, an enforceable student privacy and data security framework.[44] In line with the President's Consumer Privacy Bill of Rights, which is based largely based on the well-established Fair Information Practices ("FIPs"), schools, districts, and EdTech and other cloud-based service providers should adhere to the following practices when collecting student data. These rights should transfer from parents or legal guardians to students once the student is eighteen or attending college.

1. Access and Amendment: Students have the right to access and amend their erroneous, misleading, or otherwise inappropriate records, regardless of who collects or maintains the information.
    - There are gaps in current laws and proposed frameworks concerning students' access and amendment to their data. Schools, companies, government agencies, and other entities that collect any student information should provide student access to this information. This includes access to any automated decision-making rule-based systems (*i.e*, personalized learning algorithms) and behavioral information.

2. Focused collection: Students have the right to reasonably limit student data that companies and schools collect and retain.
    - EdTech companies should collect only as much student data as they need to complete specified purposes. "Educational purposes" and "educational quality" are frequent examples of broad and fluid purposes that grant EdTech carte blanche to collect troves of student data. A more focused collection would, for example, specify that the collection is necessary to "improve fifth grade reading skills" or "enhance college-level physics courses." In focusing student data collection for specific purposes, schools and companies should consider the sensitivity of the data and the associated privacy risks.

3. Respect for Context: Students have the right to expect that companies and schools will collect, use, and disclose student information solely in ways that are compatible with the context in which students provide data.
    - Schools and companies should never repurpose student data without express written student consent. This includes using student data to serve generalized or targeted advertisements. The Education Department's guidance states that federal student privacy laws do no prohibit schools or districts "from allowing a provider acting as a school official from serving ads to all students in email or other online

[44] Valerie Strauss, *Why a 'Student Privacy Bill of Rights' is Desperately Needed*, THE WASHINGTON POST ANSWER SHEET BLOG (Mar. 6, 2014, 3:30 PM), http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.

services." This allows service providers to repurpose the information. Schools provide private companies access to student data to help enhance education quality. When companies use this access for general marketing purposes, they have repurposed the student data and turned the classroom into a marketplace.

4. Security: Students have the right to secure and responsible data practices.
    - Amid recent, large-scale student data breaches, schools and companies must increase their data safeguards to ward against "unauthorized access, use, destruction, or modification; and improper disclosure" as described in the CPBR. Companies should immediately notify schools, students, and appropriate law enforcement of any breach. And schools should immediately notify students when there is a breach. Schools should refrain from collecting information if they cannot adequately protect it. Securing student information also entails deleting and de-identifying information after it has been used for its initial and primary purposes (no secondary uses allowed!).

5. Transparency: Students have the right to clear and accessible information privacy and security practices
    - Schools and companies should publish the types of information they collect, the purposes for which the information will be used, and the security practices in place. Schools and companies should also publish algorithms behind their decision-making.

6. Accountability: Students should have the right to hold schools and private companies handling student data accountable for adhering to the Student Privacy Bill of Rights
    - Schools and companies should be accountable to enforcement authorities and students for violating these practices.

Conclusion

The sweeping increase of student data collection must be met with increased privacy protections. State and local legislation and oversight can help safeguard student privacy.

In light of (1) how the current regulatory framework encourages mass collection of student records; (2) the privacy risks that students today face; and (3) the need for data security safeguards, California should adopt the Student Privacy Bill of Rights to ensure student privacy in the digital age.

Thank you for the opportunity to participate in today's hearing. I will be pleased to answer your questions.