epic.org

February 11, 2015

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

Representative Todd Rokita, Chairman
Subcommittee on Early Childhood, Elementary, and Secondary Education
Education and the Workforce Committee
2181 Rayburn House Office Building
Washington, D.C. 20515

Representative Marcia L. Fudge, Ranking Member
Subcommittee on Early Childhood, Elementary, and Secondary Education
Education and the Workforce Committee
2181 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Rokita and Ranking Member Fudge:

We write today in anticipation of your upcoming hearing, "How Emerging Technology Affects Student Privacy." We understand that the hearing "will provide members an opportunity to learn more about the role new technology is playing in classrooms and school accountability, its impact on student privacy, and the need to advance reforms that will strengthen student privacy protections."[1]

As described below, new technology is routinely deployed in classrooms without meaningful accountability, oversight, and transparency. More than ever, students experience routine and pervasive surveillance that threatens fundamental privacy and intellectual freedom rights. And schools and companies fail to adequately safeguard the student data they collect.[2] We write to urge you to pursue effective measures that

[1] Press Release, House Comm. on Educ. & the Workforce, Rokita to Hold Hearings on Student Privacy (Feb. 10, 2015), http://edworkforce.house.gov/news/documentsingle.aspx?DocumentID=398345.

[2] *See, e.g.*, Natasha Singer, *Uncovering Security Flaws in Digital Education Products for School Children*, N.Y. TIMES, Feb. 8, 2015, at B1, *available at* http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html?ref=topics&_r=0; *D.C. Special-Education Students' Confidential Info Was Publicly Accessible for Years*, WTOP (Feb. 4, 2015, 5:15 AM), http://wtop.com/dc/2015/02/d-c-special-education-students-confidential-info-publicly-accessible-years/; Benjamin Herold, *Danger Posed by Student-Data Breaches Prompts Action*, EDUCATION WEEK (Jan. 22, 2014), http://www.edweek.org/ew/articles/2014/01/22/18dataharm_ep.h33.html; 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?pagewanted=all.

meaningfully safeguard student data. We appreciate your work and the work of other Committee Members to address an issue of paramount concern to American parents and students.

The Electronic Privacy Information Center ("EPIC") is a non-partisan research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has a particular interest in safeguarding student records and has worked in this field for many years.[3] In 2013, we urged Congress to investigate student privacy practices and to strengthen the Family Educational Rights and Privacy Act ("FERPA").[4] Last year, EPIC wrote the Student Privacy Bill of Rights, an enforceable student privacy and data security framework.[5] The Student Privacy Bill of Rights is in line with President Obama's Consumer Privacy Bill of Rights, which is largely based on the well-established Fair Information Practices ("FIPs").

Meaningful, effective outcomes that protect student privacy are long overdue. Schools and companies collect students' location, health, discipline, social media information, and other sensitive data with no accountability.[6] Last month, President Obama made an important commitment to fixing the current problems plaguing student

---

[3] *See Student Privacy*, EPIC, https://epic.org/privacy/student/. *See also*, Khaliah Barnes, EPIC Student Privacy Project Director, *Testimony and Statement for the Record on "Ensuring Student Privacy in the Digital Age" before the California State Assembly* (May 14, 2014), *available at* https://epic.org/privacy/student/EPIC-CA-Asmbly-Hearing-Stu-Priv-5-14.pdf; Khaliah Barnes, EPIC Administrative Law Counsel, *Testimony and Statement for the Record on "Study Session regarding inBloom, Inc." before the Colorado State Board of Education* (May 16, 2013), https://epic.org/privacy/student/EPIC-Stmnt-CO-Study-5-13.pdf; *Failing Grade: Education Records and Student Privacy*, EPIC, http://epic.org/events/student-privacy14/; Khaliah Barnes and Marc Rotenberg, *Amassing Student Data and Dissipating Privacy Rights*, EDUCAUSE REVIEW ONLINE (Jan. 28, 2013), http://www.educause.edu/ero/article/amassing-student-data-and-dissipating-privacy-rights. *See also* Khaliah Barnes and Marc Rotenberg, *Students and Data Privacy*, N.Y. TIMES (May 3, 2014), www.nytimes.com/2014/05/04/business/students-and-data-privacy.html; Letter from Privacy Coalition to the Hon. Donald H. Rumsfeld (Oct. 18, 2005), *available at* http://privacycoalition.org/nododdatabase/letter.html; *Chicago Tribune v. University of Illinois*, EPIC, http://epic.org/amicus/tribune/.

[4] Letter from Marc Rotenberg & Khaliah Barnes, EPIC, to Senate Comm. on Health, Educ., Labor & Pensions & House Educ. & the Workforce Comm. (Oct. 9, 2013), https://epic.org/apa/ferpa/EPIC-ED-Student-Privacy-Letter.pdf.

[5] *Student Privacy Bill of Rights*, EPIC, https://epic.org/privacy/student/bill-of-rights.html. *See also* 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/.

[6] Khaliah Barnes, *Student Data Collection Is Out of Control*, N.Y. TIMES (Sept. 25, 2014), http://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/student-data-collection-is-out-of-control.

privacy. The President will work with Congress to implement the "Student Digital Privacy Act"—common sense, pragmatic student privacy legislation to "ensur[e] that data collected in the educational context is used only for education purposes."[7] To meaningfully implement the Student Digital Privacy Act, Congress must enact strong baseline measures, including the Student Privacy Bill of Rights and Privacy Enhancing Techniques.[8] The Student Digital Privacy Act should also include a private right of action for students and parents against companies' unlawful disclosure of student information. This enforcement mechanism is essential to protecting student privacy.

As described by the President, the Student Digital Privacy Act "would prevent companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school."[9] While President Obama's proposal focuses on limiting companies' use of student data, more privacy-protective initiatives include the mandatory use of Privacy Enhancing Techniques ("PETs"), which minimize or eliminate the collection of students' personally identifiable information. Simply put, schools and companies cannot abuse student information to which they do not have access. PETs can help facilitate anonymous research to improve student learning without jeopardizing student privacy. Anonymous and de-identified information can protect student personally identifiable information if the anonymization techniques are robust, scaleable, and independently evaluated.

The Student Digital Privacy Act should also incorporate the Student Privacy Bill of Rights.[10] In line with President Obama's Consumer Privacy Bill of Rights, the Student Privacy Bill of Rights is an information privacy and security framework for schools, districts, and companies that collect student information:

> 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.
>
> - Schools, companies, government agencies, and other entities that collect any student data should provide students access to their information. This includes access to any automated decision-making rule-based systems (*i.e*, personalized learning algorithms) and behavioral information.

[7] Press Release, White House Office of the Press Secretary, Fact Sheet: Safeguarding American Consumers & Families (Jan. 12, 2015), http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.
[8] *See* EPIC, Comments on National Privacy Research Strategy 6 (Oct. 17, 2014), https://www.epic.org/apa/comments/EPIC-NITRD-Privacy-Research-Strategy.pdf (discussing privacy safeguards and defining Privacy Enhancing Techniques as technologies and practices that "minimize or eliminate the collection of personally identifiable information.").
[9] *Supra* note 7.
[10] *Supra* note 5.

2. **Focused collection**: Students have the right to reasonably limit student data that companies and schools collect and retain.

- Companies should collect only as much student data as they need to complete specified purposes. "Educational purposes" and " improving educational quality" are frequent examples of broad and fluid purposes that grant EdTech companies 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 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 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 Consumer Privacy Bill of Rights. Companies should immediately notify schools, students, and appropriate law enforcement of any breach. 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.

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. 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.

Concerning accountability, current enforcement mechanisms have failed to protect student information. The Education Department is responsible for enforcing student data protection under FERPA. In 2008 and 2011, the Department issued controversial FERPA rules that fostered the current environment of educational data flowing nearly unrestricted from schools to third parties.[11] Practically speaking, the institutions entrusted to teach students are rarely the custodians of the majority of student records. Consequently, students and schools have necessarily lost substantial control of student information. Currently, FERPA does not provide a private right of action. Under FERPA, the Education Department may remove federal funding from schools that violate the law, but the Department may only do so after permitting schools to voluntarily comply with FERPA.[12] To date, the Education Department has never removed federal funding. Pursuant to the Freedom of Information Act, EPIC sought records detailing the Education Department's investigations into possible FERPA violations.[13] The documents that EPIC has received thus far reveal that schools and districts have disclosed students' personal records without consent, possibly in violation of FERPA. The documents also reveal that the Education Department failed to investigate many FERPA complaints and that some parents even wrote to members of Congress seeking assistance over alleged FERPA violations.[14]

The Federal Trade Commission ("FTC") has a broad mandate to protect consumers. EPIC frequently files complaints with the FTC on behalf of student consumers, but the FTC has not meaningfully exercised its enforcement powers to protect student consumers. In 2009, EPIC filed a complaint with the FTC against Echometrix, the developer of parental control software that monitored children's online activity.[15] Echometrix analyzed the information collected from children and sold the data to third parties for market-intelligence research. EPIC alleged that Echometrix engaged in unfair and deceptive trade practices by representing that the software protects children online

[11] 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).
[12] 34 C.F.R. § 99.67.
[13] *EPIC Student Privacy Freedom of Information Act Request: Department of Education's FERPA Enforcement*, EPIC, http://epic.org/foia/ed/ferpa/default.html.
[14] *Id*.
[15] EPIC, *In the Matter of Echometrix, Inc.* (Sept. 25, 2009), https://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.

while simultaneously collecting and disclosing information about children's online activity. The complaint further alleged that Echometrix's practices violate the Children's Online Privacy Protection Act ("COPPA") by collecting and disclosing information from children under the age of 13. EPIC asked the FTC to stop Echometrix's practices, seek compensation for victims, and ensure that Echometrix's collection and disclosure practices comply with COPPA. It took the FTC over a year after EPIC filed its complaint to act. Under the settlement with the FTC, Echometrix agreed not to share any data and to destroy the information it had collected in its marketing database, but was not required to pay any fines.[16] In contrast to the FTC's actions, the Defense Department quickly canceled a contract with Echometrix following EPIC's complaint, and the New York Attorney General filed charges against the company, which resulted in Echometrix paying a $100,000 penalty to the state of New York.[17]

More recently, EPIC filed an extensive complaint with the FTC concerning the business practices of Scholarships.com.[18] The company encouraged students to divulge sensitive medical, sexual, and religious information to obtain financial aid information. The company claimed that it used this information to locate scholarships and financial aid. Scholarships.com, however, transferred the data to a business affiliate that in turn sold the data for general marketing purposes. EPIC alleged that Scholarships.com's actions were unfair and deceptive trade practices. EPIC also alleged that Scholarships.com's failure to use reasonable security practices was an unfair trade practices. EPIC has asked the FTC to require the company to change its business practices. Following EPIC's complaint, the company improved security on its website. But the FTC failed to act on EPIC's complaint.

EPIC also filed an FTC complaint concerning the loss of personal information of almost 2.5 million current and former students, employees, and vendors in Maricopa County Community College District.[19] We alleged that the District's failure to maintain a comprehensive information security program led to a "massive breach of names, addresses, phone numbers, e-mail addresses, Social Security numbers, dates of birth,

---

[16] Press Release, Federal Trade Commission, FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers (Nov. 30, 2010), http://www.ftc.gov/news-events/press-releases/2010/11/ftc-settles-company-failed-tell-parents-childrens-information.

[17] EPIC, *Defense Department Pulls Parental Control Software Product Following EPIC Complaint*, Dec. 4, 2009, https://epic.org/2009/12/defense-department-pulls-paren.html; Press Release, New York Attorney General, Cuomo Announces Agreement Stopping Software Company "echometrix" From Selling Children's Private Online Conversations to Marketers (Sept. 15, 2010), http://www.ag.ny.gov/press-release/cuomo-announces-agreement-stopping-software-company-echometrix-selling-childrens.

[18] EPIC, *In the Matter of Scholarships.com, LLC* (Dec. 12, 2013), http://epic.org/privacy/student/EPIC-FTC-Compl-Scholarships.com.pdf.

[19] EPIC, *In the Matter of Maricopa County Community College District* (Sept. 29, 2014), https://www.epic.org/privacy/student/EPIC-Safeguards-Rule-Complaint.pdf.

certain demographical information, and enrollment, academic, and financial aid information."[20] This breach occurred after repeated warnings from the Arizona Auditor General that Maricopa County Community College District lacked adequate security measures. We alleged that the District violated the FTC's Safeguards Rule by failing to protect students' financial information. The FTC has yet to act on EPIC's complaint.

The Education Department and the Federal Trade Commission could and should do more to protect student privacy. But because they have not, meaningful legislation will provide a private right of action for students and their parents against private companies that unlawfully disclose student information.

It is within the Committee's jurisdiction to address the growing privacy threats to American students.

EPIC looks forward to working with your staff on this matter.

Sincerely,

Marc Rotenberg
EPIC President

Khaliah Barnes
Director, EPIC Student Privacy Project

CC: Representative Jared Polis;
Representative Luke Messer

Attorney General Jim Hood (MS), President, National Association of Attorneys General (NAAG);
Attorney General Marty Jackley (SD), President-Elect, NAAG

[20] *Id*.