epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

May 16, 2018

Representative Virginia Foxx, Chair
Representative Robert Scott, Ranking Member
Committee on Education and the Workforce
2176 Rayburn House Office Building
Washington, DC 20515

Dear Chairwoman Foxx and Ranking Member Scott:

We write to you regarding the upcoming hearing on "Protecting Privacy, Promoting Data Security: Exploring How Schools and States Keep Data Safe."[1] We appreciate the Committee's interest in the privacy of student records, an issue of paramount concern to American parents and students.

EPIC is a public-interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC is a leading advocate for student privacy rights.[2] EPIC has proposed a Student Privacy Bill of Rights to safeguard student data and security,[3] obtained documents regarding the misuse of education records through the Freedom of Information Act, and repeatedly urged the Federal Trade Commission to establish security standards for student data maintained by state agencies.[4] EPIC also sued the Department of Education regarding changes in an agency regulation that diminished the safeguards set out in

[1] *Protecting Privacy, Promoting Data Security: Exploring How Schools and States Keep Data Safe*, 115th Cong. (2018), H. Comm. on Education and the Workforce, https://edworkforce.house.gov/calendar/eventsingle.aspx?EventID=402711 (May 17, 2018).
[2] *See, e.g., Student Privacy*, EPIC, http://epic.org/privacy/student/; Letter from EPIC et al. to Secretary John B. King, U.S. Department of Education (June 6, 2016), https://epic.org/privacy/student/ED-DataSecurity-Petition.pdf; Comments of EPIC to the Institute of Education Sciences and Department of Education, Privacy Act of 1974; System of Records—"Impact Evaluation of Data-Driven Instruction Professional Development for Teachers", Jan. 4, 2016, available at https://epic.org/privacy/student/EPICComments-ED-Impact-Eval-SORN.pdf; Comments of EPIC to the Department of Education, Notice of New System of Records: "Study of Promising Features of Teacher Preparation Programs", Jul. 30, 2012, available at https://epic.org/privacy/student/EPIC-ED-SORN-Cmts.pdf; Comments of EPIC to the Department of Education, Family Educational Rights and Privacy Act Notice of Proposed Rulemaking, May 2, 2011, available at http://epic.org/privacy/student/EPIC_FERPA_Comments.pdf; The Privacy Coalition to Donald Rumsfeld, Secretary of Defense, DOD Database Campaign Coalition Letter (Oct. 18, 2005), available at http://privacycoalition.org/nododdatabase/letter.html; Br. Amicus Curiae Electronic Privacy Information Center Supp. Apl., *Chicago Tribune Co. v. Bd. of Trustees of Univ. of Illinois*, 680 F.3d 1001 (7th Cir. 2012) (No 11-2066), available at http://epic.org/amicus/tribune/EPIC_brief_Chi_Trib_final.pdf.
[3] EPIC, Student Privacy Bill of Rights, https://epic.org/privacy/student/bill-of-rights.html.
[4] EPIC, *EPIC Uncovers Complaints from Education Department about Misuse of Education Records* (July 18, 2014), https://epic.org/2014/07/epic-uncovers-complaints-from.html.

the Family Educational Rights and Privacy Act.[5] The practical consequence of the FERPA rule change was to make it easier for private parties to get access to sensitive student data.

EPIC has long advocated for privacy and security safeguards for data and the use of privacy enhancing technologies ("PETs") that minimize or eliminate the collection of personally identifiable information.[6] EPIC testified before the Commission on Evidence-Based Policymaking and called for the Commission to adopt innovative privacy safeguards to protect personal data and make informed public policy decisions.[7] And EPIC President Marc Rotenberg and EPIC Advisory Board member Cynthia Dwork served on a panel at the National Academies of Science that recently released a report on how federal data sources can be used for public policy research while protecting privacy.[8]

The Department of Education 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."[9] Yet, the Department "does not believe it is appropriate to regulate specific data security requirements under FERPA."[10] As a consequence, student data is routinely compromised "due to weak or nonexistent data security protocols."[11]

Here are a few examples[12] of weak or nonexistent data security protocols have led to the disclosure of education records in violation of FERPA:

- A University of Maryland database containing 287,580 student, faculty, staff, and personnel records was breached in 2014; the "breached records included name, Social Security number, date of birth, and University identification number." The records go as far back as 1992.[13]
- In 2015, computer criminals hacked the University of Berkeley's Financial System and gained access to Social Security numbers and bank account information for

[5] *EPIC v. U.S. Dep't of Educ.*, 48 F.Supp. 1 (D.D.C 2014).
[6] EPIC Executive Director Marc Rotenberg, Testimony Before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, Mar. 1, 2001, *Privacy in the Commercial World*, https://epic.org/privacy/testimony_0301.html.
[7] Marc Rotenberg, Commission on Evidence-Based Policymaking: Privacy Perspectives, before the National Academies of Science, Sep. 9, 2016, https://epic.org/privacy/wiretap/RotenbergCEBP-9-16.pdf.
[8] National Academies of Science, "Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy" (2017), https://www.nap.edu/catalog/24652/innovations-in-federalstatistics-combining-data-sources-while-protecting-privacy [hereinafter "Innovations in Federal Statistics"].
[9] Family Educational Rights and Privacy Act Final Reg., 76 Fed. Reg. 75,604, 75,622 (Dec. 2, 2011).
[10] *Id*.
[11] *Id*.
[12] *See, e.g., Chronology of Data Breaches: Security Breaches 2005 – Present,* PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (Select "EDU-Education Institutions)*;* 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; Michael Alison Chandler, *Loudoun Schools Offer Details on Data Breach*, WASHINGTON POST (Jan. 8, 2014), http://www.washingtonpost.com/local/education/loudoun-schools-offer-details-on-data-breach/2014/01/08/d0163b50-78ad-11e3-8963-b4b654bcc9b2_story.html.
[13] UMD Data Breach, UNIVERSITY OF MARYLAND, http://www.umd.edu/datasecurity/.

approximately 80,000 students, vendors, staff, and current and former faculty. By some estimates, the breach affected "approximately 50 percent of current students and 65 percent of active employees."[14]

- D.C. Public Schools recently posted education records of approximately 12,000 public school special needs students online. The information included "each student's identification number, race, age, school, disabilities and any services he or she receives."[15] The information was uploaded to a public D.C. Council Dropbox account. This is at least the second time since 2015 that D.C. Public Schools have publicly posted the private education records of students with special needs.[16]
- Edmodo, the self-described "number one K-12 social learning network in the world" boasting "over 39 million teachers, students, and parents," previously collected student information over an unencrypted connection.[17]
- And, in one of the largest documented school data breaches, the Maricopa County Community College District ("MCCD") experienced a security breach affecting almost 2.5 million students, alumni, vendors and employees.[18] The breach exposed personal information including "names, birth dates, Social Security numbers, and bank account information [.]"[19] This breach followed an earlier 2011 MCCD breach.[20]

The enactment of the Student Privacy Bill of Rights[21] should be a priority for this Congress. The Student Privacy Bill of Rights would provide students with the following rights:

---

[14] Janet Gilmore, *Campus Alerting 80,000 Individuals to Cyberattack*, BERKELEY NEWS (Feb. 26, 2016), http://news.berkeley.edu/2016/02/26/campus-alerting-80000-individuals-to-cyberattack/

[15] Perry Stein, *D.C. Accidentally Uploads Private Data of 12,000 Students*, WASHINGTON POST (Feb. 11, 2016), https://www.washingtonpost.com/local/education/dc-accidentally-uploads-private-information-of-12000-students/2016/02/11/7618c698-d0ff-11e5-abc9-ea152f0b9561_story.html.

[16] John Templon and Katie J.M. Baker, *D.C. Public Schools Website Exposed Confidential Info About Students With Disabilities*, BUZZFEED (Feb. 3, 2015, 1:02 PM), http://www.buzzfeed.com/johntemplon/dc-public-schools-website-exposed-confidential-info.

[17] 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.

[18] *Maricopa Community Colleges Notifies 2.5M After Data Security Breach*, PHOENIX BUSINESS JOURNAL (Nov 27, 2013, 11:58 AM MST), http://www.bizjournals.com/phoenix/news/2013/11/27/mcccd-notifies-25m-about-exposed.html?page=all.

[19] *Id*.

[20] Mary Beth Faller, *Failure to Address 2011 Hacking Tied to '13 Breach*, THE ARIZONA REPUBLIC (Feb. 2014, 10:36 AM), http://www.azcentral.com/community/phoenix/articles/20140318arizona-mcccd-failure-address-hacking-tied-breach.html. *See also* EPIC, *In the Matter of Maricopa County Community College District* (Sept. 29, 2014), https://epic.org/privacy/student/EPIC-Safeguards-Rule-Complaint.pdf.

[21] In 2015, President Obama rightly proposed legislation to safeguard student privacy. The Student Digital Privacy Act would have "prevent[ed] 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." 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.

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.
2. **Focused collection:** Students have the right to reasonably limit student data that companies and schools collect and retain.
3. **Respect for Context:** Students have the right to expect that companies and schools will collect, use, and disclose student information solely in ways compatible with the context in which students provide data.
4. **Security:** Students have the right to secure and responsible data practices.
5. **Transparency:** Students have the right to clear and accessible information privacy and security practices.
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.

As school districts and companies that market services and products to students increasingly collect and use student data, the ability for students to have access to and control of that data will be increasingly important. Also important is the use of Privacy Enhancing Techniques (PETs) that minimize or eliminate the collection of personal information.[22]

Conclusion

Students today face unprecedented threats to their personal privacy. New technology is routinely deployed in classrooms without meaningful accountability. Student communications, interests, location, and learning experiences are routinely logged, compiled, and analyzed. Personal data flows from schools to consultants and private corporations. Schools simply fail to safeguard the student data they collect. We urge you to enact a Student Privacy Bill of Rights to safeguard student data.

We ask that this statement be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

[22] *See* Comments of EPIC, *On the Privacy and Security Implications of the Internet of Things*, FTC File No. ___ (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.