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 2, 2017

The Honorable Jason Chaffetz, Chairman
The Honorable Elijah Cummings, Ranking Member
House Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Chaffetz and Ranking Member Cummings:

We write to you regarding the upcoming hearing on "Reviewing the FAFSA Data Breach."[1] We thank you for your interest in this issue and urge you to support a Student Privacy Bill of Rights. American students face unprecedented privacy and security threats. The increasing commercialization of personal data has led to staggering increases in identity theft, security breaches, and financial fraud in the United States. The Department of Education collects extremely sensitive personal information such as Social Security Numbers, and has an obligation to protect that data, but has failed to do so.

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

[1] *Reviewing the FAFSA Data Breach*, 115th Cong. (2017), H. Comm. on Oversight and Gov't Reform, https://oversight.house.gov/hearing/reviewing-fafsa-data-breach/ (March 22, 2017).
[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-Data-Security-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/EPIC-Comments-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.

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 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.

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."[6] Yet, the Department "does not believe it is appropriate to regulate specific data security requirements under FERPA."[7] As a consequence, student data is routinely compromised "due to weak or nonexistent data security protocols."[8]

Here are a few examples[9] 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.[10]
- In 2015, computer criminals hacked the University of Berkeley's Financial System and gained access to Social Security numbers and bank account information for approximately 80,000 students, vendors, staff, and current and former faculty. By some estimates, the breach impacted "approximately 50 percent of current students and 65 percent of active employees."[11]
- 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.[12]

---

[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.
[5] *EPIC v. U.S. Dep't of Educ.*, 48 F.Supp. 1 (D.D.C 2014).
[6] Family Educational Rights and Privacy Act Final Reg., 76 Fed. Reg. 75,604, 75,622 (Dec. 2, 2011).
[7] *Id*.
[8] *Id*.
[9] *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.
[10] UMD Data Breach, UNIVERSITY OF MARYLAND, http://www.umd.edu/datasecurity/.
[11] 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/
[12] 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.

The enactment of the Student Privacy Bill of Rights[13] should be a priority for this Congress. The Student Privacy Bill of Rights would provide students with the following rights:

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 that are 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. [14]

Far more needs to be done to safeguard the personal information of students at American educational institutions.

We ask that this letter 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

[13] 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.

[14] *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.