June 6, 2016

Secretary John B. King
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

**RE: Petition to Amend 34 C.F.R. Part 99 ("Family Educational Rights and Privacy") to Establish a Data Security Rule**

Dear Secretary King:

We, the undersigned student rights, consumer rights, and children's advocates, along with members of the EPIC Advisory Board, petition the United States Department of Education (the "Department") to amend 34 C.F.R. Part 99 ("Family Educational Rights and Privacy") to include a Data Security Rule that would require administrative, physical, and technical safeguards to prevent the unauthorized disclosure of personally identifiable information ("PII") contained in education records, including directory information.[1] Current recordkeeping practices fail to protect student data from unauthorized disclosure and threaten student privacy.[2] The Rule should apply to all educational agencies, institutions and third parties that process personal data subject to FERPA.

## A. The Education Department is Required to Enforce the FERPA

Congress expressly mandated the Education Department to implement and enforce the Family Educational Rights and Privacy Act ("FERPA"), a federal student privacy law applicable to education agencies and institutions receiving federal funds to administer Department programs.[3] FERPA prohibits the unauthorized disclosure of

[1] This is a petition under the Administrative Procedure Act, 5 U.S.C. § 553(e).
[2] *See*, *e.g.*, EPIC, *EPIC Student Privacy Project*, https://epic.org/privacy/student/. *See generally* Pablo G. Molina, *Protecting Data Privacy in Education*, in PRIVACY IN THE MODERN AGE 138-145 (Marc Rotenberg, Julia Horwitz, and Jeramie Scott eds., 2015). *See also Intrusion into UCF Network Involves Personal Data*, DATA SECURITY (Mar. 8, 2016), http://www.ucf.edu/datasecurity/; Steve Ragan, *SNHU Still Investigating Database Leak Exposing Over 140,000 Records*, CSO ONLINE (Jan. 5, 2016, 10:00 AM PT), http://www.csoonline.com/article/3019278/security/snhu-still-investigating-database-leak-exposing-over-140-000-records.html; Megan O'Neil, *Data Breaches Put a Dent in Colleges' Finances as Well as Reputations*, THE CHRONICLE OF HIGHER EDUC. (Mar. 17, 2014), http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/.
[3] 20 U.S.C. §1232g (f) ("The Secretary shall take appropriate actions to enforce this section and to deal with violations of this section [.]"); *see also* 20 U.S.C. § 3474 ("[t]he Secretary is authorized to prescribe such rules and regulations as the Secretary determines necessary or appropriate to administer and manage the functions of the Secretary or the Department."); 20 U.S.C. § 1221e—3 (authorizing the Secretary to "make, promulgate, issue, rescind, and amend rules and regulations governing the manner of operation of, and governing the applicable programs administered by, the Department.").

education records and student personally identifiable information contained in education records.[4] Upon a finding that an education agency or institution has violated FERPA's disclosure prohibitions, the Department may terminate federal funding.[5] The Department, however, must first permit the agency or institution to voluntarily comply with FERPA before terminating federal assistance.[6]

Additionally, FERPA only permits education agencies and institutions to disclose student personal information to contractors, organizations, and other third parties "on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student."[7] If a third party violates FERPA's confidentiality provisions, FERPA prohibits education agencies and institutions from "permitting access to information from education records to that third party for a period of not less than five years."[8] FERPA also imposes conditions directly on third parties receiving education records.[9]

Consequently, the Education Department's FERPA authority not only directly reaches education agencies and institutions, but also third parties to which education agencies and institutions disclose student records.[10]

## B. The Education Department's Recent Changes to FERPA Place at Risk the Personal Information Subject to the Act

Under Education Department rules issued over the last several years, education agencies and institutions increasingly disclose education records to third parties.

For example, under FERPA's 2008 regulations, schools may disclose education records to a "contractor, consultant, volunteer, or other party" performing "an institutional service or function for which the agency or institution would otherwise use employees."[11] Education institutions and agencies traditionally used this "school official" exception to the FERPA consent requirement to disclose education records to teachers, but now routinely use this exception to disclose student records to Google, Pearson, Khan

---

[4] 20 U.S.C. § 1232g (b).
[5] *Id.* § 1232g (f). *See also* 34 C.F.R. § 99.66 (c); 34 C.F.R. § 99.67 (a).
[6] 20 U.S.C. § 1232g (f). *See also* 34 C.F.R. § 99.66 (c)-(d).
[7] 20 USC § 1232g (b)(4)(B).
[8] *Id. See also* 34 C.F.R. § 99.67 (c) – (e).
[9] *See*, *e.g.*, 20 U.S.C. § 1232g (b)(1)(F); 34 C.F.R. § 99.31(a)(6) (iii)(B) (requiring organizations conducting studies to destroy student PII "when no longer needed for the purpose for which the study was conducted."). *See also* 34 C.F.R. § 99.31 (b)(permitting third parties to release de-identified student data for education research by attaching "a code to each record that may allow the recipient to match information received from the same source," provided that the third party does not release information "that would allow a recipient to identify a student based on a record code [.]")
[10] *See also* 34 C.F.R. § 99.66 (d) (describing the Department's enforcement process for third parties outside of an educational agency or institution that have disclosed records in violation of FERPA).
[11] 34 C.F.R. § 99.31(a) (1)(i)(B)(1).

Academy, and countless other ed tech providers.[12] The Department requires these outside contractors and consultants to be under the "direct control" of the education agency or institution.[13] Importantly, FERPA does not require written agreements to disclose student information to school officials.[14] Education agencies and institutions are only required to use "reasonable methods" to ensure that school officials have access only to those "education records in which they have legitimate educational interests."[15] The Department's failure to require written agreements for outside contractors and consultants has resulted in schools giving away student records without any meaningful privacy and data security safeguards.[16]

In 2011, the Department again revised key FERPA definitions that once limited to whom education agencies and institutions could disclose education records.[17] The 2011 regulations defined one term – "authorized representative" – so broadly that the term can entail state politicians having access to student records, as long as they comply with basic FERPA confidentiality rules.[18]

### C. Poor Data Security Has Led to the Unauthorized Disclosure of Student Records Subject to FERPA

Following the Department's 2008 and 2011 FERPA rules permitting the widespread disclosure of education records, data breaches routinely plague K-12 and higher education institutions. As the Education Department notes, 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."[19] Yet to date, there are no baseline data security

---

[12] Natasha Singer, *Privacy Pitfalls as Education Apps Spread Haphazardly*, N.Y. TIMES, Mar. 11, 2015, at B1, *available at* http://www.nytimes.com/2015/03/12/technology/learning-apps-outstrip-school-oversight-and-student-privacy-is-among-the-risks.html.

[13] *Id.* § 99.31(a) (1)(i)(B)(2).

[14] *Id*. § 99.31. *See also* PRIVACY TECH. ASSISTANCE CTR., DEP'T OF EDUC., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES 4 (2014), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

[15] 34 C.F.R. § 99.31 (a)(1)(ii).

[16] Joel Reidenberg, N.Cameron Russell, Jordan Kovnot, Thomas B. Norton, Ryan Cloutier, and Daniela Alvarado, *Privacy and Cloud Computing in Public Schools*, CTR. ON LAW AND INFO. POLICY (2013), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip.

[17] *See* EPIC, *EPIC v. U.S. Department of Education*, https://epic.org/apa/ferpa/.

[18] Family Educational Rights and Privacy Final Regulations, 76 Fed. Reg. 75,604, 75,616 (Dec. 2, 2011)("While nothing in the final regulations specifically prohibits a State politician or private company, for example, from being designated as an authorized representative, the full requirements under FERPA must be met before PII from education records may be disclosed to any party."). *See also* 34 C.F.R. § 99.35.

[19] *Id*. at 75,622. *See also* Christine Borgman, Kent Wada, and James F. Davis, *New Models of Privacy for the University*, in PRIVACY IN THE MODERN AGE 34-35 (Marc Rotenberg, Julia Horwitz, and Jeramie Scott eds., 2015) ("*Information security*, as distinct from privacy, supports the protection of information resources from unauthorized access that could compromise their confidentiality, integrity, and availability.").

rules to prevent the unauthorized disclosure of education records. In 2011, the Department stated that it "does not believe it is appropriate to regulate specific data security requirements under FERPA."[20] But amid the current backdrop of data breaches that compromise the education records of millions of students, the Department's belief is arbitrary and capricious.

What follows below is a small sample of examples[21] where weak or nonexistent data security protocols have led to the unauthorized disclosure of education records and student information 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."[22] The breached records included records going as far back as 1992.[23]

- In 2015, unauthorized individuals gained access to 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.[24] By some estimates, the breach impacted "approximately 50 percent of current students and 65 percent of active employees."[25]

- 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.[26]

- D.C. Public Schools recently posted education records of approximately 12,000 public school special needs students online. The information included "each

---

[20] Family Educational Rights and Privacy Final Regulations *supra* note 18 at 75,622.
[21] *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?tkn=YLPFtDc0755TK%2Fu34U8t0wAM665xk%2Bw7tQWZ&cmp=clp-edweekhttp://www.edweek.org/ew/articles/2014/01/22/18dataharm_ep.h33.html?tkn=YLPFtDc0755TK%2Fu34U8t0wAM665xk%2Bw7tQWZ&cmp=clp-edweek; 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.
[22] UMD Data Breach, UNIVERSITY OF MARYLAND, http://www.umd.edu/datasecurity/.
[23] *Id*.
[24] 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/
[25] *Id*.
[26] 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.

student's identification number, race, age, school, disabilities and any services he or she receives."[27] 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.[28]

- Last year, Harvard University reported a data breach that "may have compromised email login information" for an unspecified number of students attending several Harvard schools.[29]

- In 2014, Indiana University also 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.[30]

- Iowa State reported a breach in 2014 that compromised the Social Security numbers of 29,780 students covering a seventeen-year span.[31]

- That same year, Butler University announced that the personal information of nearly 200,000 people including former, current, and prospective students, had been compromised in a hacking "incident."[32] Butler's compromised records included names, birthdates, Social Security numbers, and academic records.[33] The hack affected former students going back as far as the 1980s.[34]According Butler University, the security breach arose from "unauthorized hacking into Butler University's computer network between November 2013 and May 2014."[35].

---

[27] 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.

[28]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?utm_term=.nbEnL7Vw1#.lsVe5BZd9.

[29] Melanie Y. Fu, *Harvard Investigates IT Security Breach*, THE HARVARD CRIMSON (Jul. 2, 2015) http://www.thecrimson.com/article/2015/7/2/harvard-it-security-breach/.

[30] Indiana University Reports Potential Data Exposure, INDIANA UNIVERSITY, Feb. 25, 2014, http://news.iu.edu/releases/iu/2014/02/data-exposure-disclosure.shtml.

[31] *Iowa State IT Staff Discover Unauthorized Access to Servers*, IOWA STATE UNIVERSITY (Apr. 22, 2014, 9:20 AM), http://www.news.iastate.edu/news/2014/04/22/serverbreach.

[32] Vanessa McClure, *Butler Alumni, Current and Prospective Students Warned of Data Breach*, FOX 59 (June 30, 2014, 9:39 AM), http://fox59.com/2014/06/30/butler-university-alumni-current-students-warned-of-data-breach/. *See also* June 26, 2014 Butler University letter, *available at* https://tribwxin.files.wordpress.com/2014/06/butlerletter2.pdf.

[33] June 26, 2014 Butler University letter.

[34] *Supra* note 32.

[35] *Supra* note 33.

- 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.[36] The breach exposed personal information including "names, birth dates, Social Security numbers, and bank account information [.]"[37] This breach followed an earlier 2011 MCCD breach.[38]

Equally disturbing as schools and their vendors failing to protect student privacy is the poor data security of statewide longitudinal databases. Designed to "capture, analyze, and use student data from preschool to high school, college, and the workforce," statewide longitudinal databases security practices also pose risks to student privacy. [39] In a 2009 study, the Fordham Law School's Center on Law and Information Policy uncovered that many statewide longitudinal 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."[40]

Congress has introduced several bills that would mandate basic data security protections for education records.[41]

## D. The Education Department Should Adopt a Data Security Rule to Protect Education Records

Weak or nonexistent data security procedures have directly led to the unauthorized disclosure of education records in violation of FERPA. Accordingly, the undersigned organizations and privacy experts petition the Education Department to

---

[36] *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.

[37] *Id*.

[38] 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.

[39] *Statewide Longitudinal Data Systems*, U.S. DEP'T OF EDUC., http://www2.ed.gov/programs/slds/factsheet.html.

[40] 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).

[41] Student Privacy Protection Act, H.R. 3157, 114th Cong § 4 (2015); Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. § 3 (2015); Protecting Student Privacy Act of 2015, S.1322, 114th Cong. § 2 (2015).

amend 34 C.F.R. Part 99 to establish administrative, physical, and technical safeguards under FERPA.[42]

Specifically, we petition the Education Department to amend 34 C.F.R. Part 99 to include:

> "What Administrative, Physical, and Technical Safeguards Apply to Educational Agencies or Institutions or Third Parties Receiving, Maintaining, or Disclosing Education Records or Personally Identifiable Information Contained In Education Records?

The safeguards would apply to education agencies and institutions required to comply with FERPA by virtue of receiving federal funds, as well as any third party, agency, or institution receiving education records and personally identifiable information pursuant to FERPA. Baseline FERPA data security rules should require encryption, privacy enhancing techniques ("PETs") that minimize or eliminate the collection of personally identifiable information, and breach notification.

Congress enacted FERPA in response to "the growing evidence of the abuse of student records across the nation."[43] 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."[44] The Education Department must issue FERPA data security regulations to assure student privacy protection.

Contact: Marc Rotenberg and Khaliah Barnes, EPIC, 1718 Connecticut Avenue, NW, Suite 200, Washington, DC 20009. + 1 202-483-1140.

[42] *See*, *e.g*, 45 C.F.R. part 164 – Security and Privacy.
[43] 121 Cong. Rec. 7,974 (daily ed. May 13, 1975) (remarks of Senator Buckley).
[44] 120 Cong. Rec. 39,863 (1974).

Respectfully submitted,

EPIC Advisory Board

Ann Bartow
Rod Beckstrom
Colin Bennett
Christine L. Borgman
Danielle Citron
Simon Davies
Laura Donohue
Cynthia Dwork
Dave Farber
Addison Fischer
David Flaherty
Deborah Hurley
Joi Ito
Ian Kerr
Chris Larsen
Harry Lewis
Anna Lysyanskaya
Mary Minow
Pablo Molina
Peter Neumann
Helen Nissenbaum
Frank Pasquale
Deborah C. Peel, MD
Stephanie Perrin
Chip Pitts
Anita Ramasastry
Ron Rivest
Pam Samuelson
Bruce Schneier
Katie Shilton
Barbara Simons
Robert Ellis Smith
Nadine Strossen
Sherry Turkle
Edward Viltz
Christopher Wolf
Shoshana Zuboff

Organizations

American Association of School Librarians
American Library Association
Bill of Rights Defense Committee/Defending
Dissent Foundation
Center for Digital Democracy
Center for Financial Privacy and Human Rights
Common Sense Kids Action
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Watchdog
Cyber Privacy Project
Eagle Forum of New Jersey
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Home School Legal Defense Association
National Consumers League
National Network to End Domestic Violence
Patient Privacy Rights
Privacy Rights Clearinghouse
Young Adult Library Services Association