June 6, 2016

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

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

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

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

- 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 [.]"

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

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