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

January 29, 2018

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

RE: Hearing on "Protecting Privacy, Promoting Policy: Evidence-Based Policymaking and the Future of Education"

Dear Chairwoman Foxx and Ranking Member Scott:

We write to you regarding the upcoming hearing on "Protecting Privacy, Promoting Policy: Evidence-Based Policymaking and the Future of Education."[1] The Electronic Privacy Information Center ("EPIC") strongly supports efforts to make data in the federal government more widely available to ensure better policymaking. At the same time, where data maintained by the federal government implicates identifiable individuals, privacy risks must be addressed and reduced as much as possible. Student privacy should not be sacrificed for the sake of evidence-based policymaking, and, if certain safeguards are put in place, evidence-based policymaking should not need to be sacrificed for the sake of student privacy.

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

[1] *Protecting Privacy, Promoting Policy: Evidence-Based Policymaking and the Future of Education*, 115th Cong. (2018), H. Comm. on Education and the Workforce, https://edworkforce.house.gov/calendar/eventsingle.aspx?EventID=402409.

[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.

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 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 as well as 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] Additionally, 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]

Weak data security has led to the disclosure of education records in violation of FERPA,[9] and this raises serious concerns about the use of student data in evidence-based policymaking. 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."[10] Yet, the Department "does not believe it is appropriate to regulate specific data

---

[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.
[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] 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-databreach/2014/01/08/d0163b50-78ad-11e3-8963-b4b654bcc9b2_story.html; UMD Data Breach, UNIVERSITY OF MARYLAND, http://www.umd.edu/datasecurity/; 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/; 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-of12000-students/2016/02/11/7618c698-d0ff-11e5-abc9-ea152f0b9561_story.html; 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.
[10] Family Educational Rights and Privacy Act Final Reg., 76 Fed. Reg. 75,604, 75,622 (Dec. 2, 2011).

security requirements under FERPA."[11] As a consequence, student data is routinely compromised.

In addition to strong data security protocols, requiring comprehensive risk assessments for de-identified confidential data and supporting adoption of PETs are key to protecting personal information. Even where data has been de-identified it is still possible to combine certain data sets with others to determine extensive amounts of personal information.[12] Moving forward, government agencies conducting evidence-based policymaking should adopt PETs to reduce the risk of re-identification of personal data. As was noted in the report by the National Academies of Science:

> Any consideration of expanding data must have privacy as a core value…As federal agencies seek to combine multiple datasets, they need to simultaneously address how to control risks from privacy breaches. Privacy-enhancing techniques and privacy-preserving statistical data analysis can be valuable in these efforts and enable the use of private-sector and other alternative data sources for federal statistics.[13]

Equally important is to recognize that under the Privacy Act statistical data is subject to fewer privacy constraints because it is understood that statistical does not identify specific individuals. If it is possible to re-identify aggregate data, complete privacy protections must necessarily apply. Agencies will carry the responsibility to ensure the adequacy of the privacy enhancing and privacy protecting techniques.

PETs are particularly important in this context due to the sensitivity of student data. Schools, private companies, and government agencies collect personal student information on an unprecedented scale. Student data collection is no longer limited to test scores and attendance records. The current Big Data environment increasingly demands personal student data. For example, statewide longitudinal databases, which track students from prekindergarten into the workforce, collect a range of student information, including:

- Name
- Date of Birth
- Gender
- Parents' name, address
- Where they attended preschool or Head Start
- Early assessments and interventions
- Suspension, expulsion
- Kindergarten readiness
- School(s) attended: state test scores & percentiles, enrollment, etc
- Economically Disadvantaged
- Race/Ethnicity; English Language Learner

[11] *Id.*
[12] Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Melon University, Data Privacy Working Paper, 2000, https://dataprivacylab.org/projects/identifiability/paper1.pdf
[13] Innovations in Federal Statistics at 3.

- Migrant
- Remedial
- Promoted/Retained (held back)
- Gifted/Talented
- Special Education: dates of eligibility determinations and individualized education plan review.
- Annual state test scores and percentiles starting in 3rd grade
- Identities of teachers
- Grades, attendance, suspension/expulsion, grade promotion
- Specific courses taken, including AP, and grades earned
- Did you graduate on time?
- Why did you leave school? Aged out; Expelled; Court order; Arrested; Incarcerated; Pregnant
- If you left school, where did you go? Transfer/Dropout/Home school/GED
- Did you go to college?
- If so, was it in-state/public? Which one? (Some states share with private and for-profit colleges too)
- If In-state/public, did you need remediation? In Math or English or both?
- Did you graduate college?

This information is clearly useful for making education policy based on evidence, but if improperly handled will have dire consequences for student privacy. The enactment of the Student Privacy Bill of Rights[14] 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.

[14] 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-pressoffice/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

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/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow