epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to the
INSTITUTE of EDUCATION SCIENCES, U.S. DEPARTMENT OF EDUCATION

Privacy Act of 1974; System of Records—"Impact Evaluation of Data-Driven Instruction Professional Development for Teachers" (#18-13-39)

[FR Doc. 2015-30526]

January 4, 2016

By notice published on December 2, 2015, the Institute of Education Sciences ("IES") of the Department of Education ("Education Department" or "Department") issued a notice of a new system of records "Impact Evaluation of Data-Driven Instruction Professional Development for Teachers" (#18-13-39) ("Study").[1] According to the System of Records Notice ("SORN"), the detailed collection of personal information will facilitate "a rigorous study of the effectiveness of providing data-driven instruction professional development to teachers and principals" and "will contain personally identifying information on approximately 12,000 students, 500 teachers, and 104 principals . . ."[2]

[1] Privacy Act of 1974; System of Records—Impact Evaluation of Data-Driven Instruction Professional Development for Teachers, 80 Fed. Reg. 75,452 (proposed December 2, 2015) [hereinafter "Privacy Act SORN"].
[2] *Id*. at 75,453-54.

Pursuant to the Department's notice, the Electronic Privacy Information Center ("EPIC") submits these comments to object to the Department's proposed collection, use, and disclosure of students' personally identifiable information. Specifically, the Department's proposal violates the Privacy Act by: (1) collecting irrelevant and unnecessary information and (2) not clearly stating the purpose of the proposed routine use disclosures. EPIC recognizes the need to evaluate educational programs, including professional development of teachers. However, this particular study appears to be one more effort by the agency to transfer sensitive student data to private contractors without any meaningful privacy safeguards.

The Department may be able to achieve its research goals by using aggregate data instead of students' personally identifiable information. This would also reduce the risk that the personal data of students would be misused by the private contractors to whom the agency proposes to transfer the data. The proposed database exposes students to privacy risks by collecting and students' personally identifiable information, including but not limited to "individualized education plan status" and "discipline records."[3] Because the Department can still achieve its research goals by collecting aggregate data, the Department should not collect, use, or disclose student personally identifiable information.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, freedom of expression, and democratic values.[4] EPIC has a particular interest in preserving privacy safeguards

[3] *Id*. at 75,453.
[4] EPIC, *About EPIC*, https://epic.org/epic/about.html.

established in the Privacy Act of 1974.[5] EPIC has made numerous recommendations to Congress and federal agencies on the need to strengthen Privacy Act protections.[6]

EPIC is also a leading advocate for student privacy rights.[7] EPIC has called for a Student Privacy Bill of Rights, an enforceable student privacy and data security framework.[8] In 2012, EPIC submitted comments to IES, opposing a similar research database on teacher preparation that, in addition to teacher information, would collect students' personally identifiable information, including "birth date; demographic information such as race, ethnicity, gender, and educational background; information on attendance and disciplinary incidences; and scores on reading and mathematics achievement tests."[9] As with the Department's current proposal, EPIC highlighted the risks to student privacy arising from the gratuitous collection of sensitive student

[5] *See, e.g.*, *The Privacy Act of 1974*, EPIC, https://epic.org/privacy/1974act/; *FAA v. Cooper*, EPIC, https://epic.org/amicus/cooper/; *Doe v. Chao*, EPIC, https://www.epic.org/privacy/chao/.
[6] *EPIC Administrative Procedure Act (APA) Comments*, EPIC, https://epic.org/apa/comments/. *See also* Letter from Marc Rotenberg and Khaliah Barnes, EPIC, to Senator Daniel Akaka, Chairman, Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, and the District of Columbia (Mar. 27, 2012), *available at* https://epic.org/privacy/1974act/EPIC-on-S-1732- Privacy-Act-Modernization.pdf; Letter from Marc Rotenberg and Khaliah Barnes, EPIC, to Senator Daniel Akaka, Chairman, Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, and the District of Columbia (May 14, 2012), *available at* https://epic.org/privacy/1974act/EPIC-Supp-S1732-Priv-Act- Modernization.pdf.
[7] *See, e.g.*, *Student Privacy*, EPIC, http://epic.org/privacy/student/; *EPIC v. The U.S. Department of Education*, EPIC, http://epic.org/apa/ferpa/default.html; Comments of the Electronic Privacy Information Center 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; Comments of the Electronic Privacy Information Center et al., to the Department of Defense, DOD DHRA 04 Joint Advertising and Market Research Recruiting Database (June 22, 2005), *available at* http://epic.org/privacy/profiling/dodrecruiting.html; 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 (EPIC) 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.
[8] Student Privacy Bill of Rights, *EPIC*, https://epic.org/privacy/student/bill-of-rights.html.
[9] Privacy Act of 1974; System of Records—Study of Promising Features of Teacher Preparation Programs, Notice of a New System of Records, 77 Fed. Reg. 38,612.

personal information.[10] Despite EPIC's objections, the Education Department continued to collect student personally identifiable information and transfer that information to private contractors. More recently, the Education Department reissued the research database to reflect "changes to the [research] study's design based on the infeasibility of efficiently identifying a sufficient number of teachers eligible for an impact study design."[11] Because the Department is unable to identify a sufficient number of teachers for the study, it is unclear why the Department continues to maintain the database containing sensitive information of "approximately 1,518,950 fourth through sixth grade students . . ."[12] Nevertheless, EPIC submits these comments to oppose yet another federal research database that threatens student privacy.

I. The Privacy Act Permits the Education Department to Collect Only Relevant and Necessary Information. Therefore, the Education Department Should Narrowly Tailor its Collection of Student Records and Only Collect Aggregate Student Information.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[13] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[14] Congress sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of

[10] EPIC, *Comments on the Institute of Education Sciences of the Department of Education Notice of New System of Records: "Study of Promising Features of Teacher Preparation Programs* (July 30, 2012), *available at* https://epic.org/privacy/student/EPIC-ED-SORN-Cmts.pdf.
[11] Privacy Act of 1974; System of Records—Study of Teacher Preparation Experiences and Early Teacher Effectiveness, 80 Fed. Reg. 5,523 (proposed February 2, 2015).
[12] *Id*. at 5,524.
[13] S. Rep. No. 93-1183 at 1 (1974).
[14] Pub. L. No. 93-579 (1974).

procedural and substantive rights.[15]

The Privacy Act's "relevant and necessary" requirement[16] is a fundamental and necessary part of the Privacy Act's protections, as it "is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.]"[17]

Part of the Privacy Act's purpose was to stave off the risk that government databases might become dossiers cataloging the various details of individuals' lives. By limiting the data kept by an agency only to data that is necessary and relevant to the agency's purpose, the Privacy Act limits the extent to which a system of records may invade privacy. Limiting the data to that which is necessary and relevant also reduces the risk of "mission creep," in which a system is pressed into unintended uses.

The SORN states that the research database "will contain personally identifying information on approximately 12,000 students, 500 teachers, and 104 principals from 104 schools in 12 school districts" and will include, at a minimum:

> [student] standardized math and English/Language Arts test scores, age, sex, race/ethnicity, grade, eligibility for free/reduced-price lunches, English Learner status, individualized education plan status, school enrollment dates, attendance records, and discipline records. For principals and teachers, this information will include, but will not necessarily be limited to, individual district identifiers, school assignments, grades and subjects taught, and principal and teacher background characteristics, including age, sex, race/ethnicity, certifications, degrees, years of teaching experience, and scores on licensure or certification tests.[18]

The Education Department asserts that the purpose of the database is to "conduct a rigorous study of the effectiveness of providing data-driven instruction professional development to

[15] *Id.*
[16] The Privacy Act of 1974, 5 U.S.C. § 552a(e)(1) (2006).
[17] S. Rep. No. 93-3418 at 47 (1974).
[18] Privacy Act SORN at 75,453.

teachers and principals."[19] According to the agency, the Study will focus on the following questions: "What are the impacts of data-driven instruction professional development on student achievement, teachers' instructional strategies, and school supports for using data? How are schools implementing data-driven instruction? What challenges do schools face in its implementation?"[20]

It may be appropriate for the Education Department to maintain personally identifiable information on teachers pursuant to this research study. It is unclear, however, why the Education Department could not simply collect this information as aggregate data. Nevertheless, regarding student data, the Department should not maintain student personally identifiable information. The Department has failed to justify why the Department needs a non-exhaustive list of student personally identifiable information to study the "effectiveness of providing data-driven instruction professional development to teaches and principals."[21] To protect student data, the Department should only collect information at the aggregate level to protect student privacy.

Moreover, the Education Department has recently faced criticism for failing to safeguard student data. In 2014, the Education Department Inspector General found that Education Department "information systems continue to be vulnerable to serious security threats."[22] The Department currently has 184 information systems, with 120 of those systems being managed by outside contractors.[23] The Education Department's vulnerable systems coupled with the

[19] *Id.* at 75,454.
[20] *Id.*
[21] *Id.*
[22] U.S. Dep't of Educ., ED-OIG/A11O0001, The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014: Final Audit Report 2 (2014), *available at* https://www2.ed.gov/about/offices/list/oig/auditreports/fy2015/a11o0001.pdf.
[23] *U.S. Department of Education: Information Security Review Before the Full H. Comm. On Oversight and Gov't Reform, 114th Cong.* (2015), https://oversight.house.gov/hearing/u-s-department-of-education-information-security-review/.

expansive outside parties having access to student records places student personal information at risk. To safeguard against the risk, the Education Department should only collect aggregate student data.

II. The Education Department Does Not Clearly Articulate the Purposes of its Proposed Routine Use.

Under the Privacy Act, the Education Department does not meet its burden to establish a "routine use" exception. The Privacy Act defines "routine use" to mean "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[24] The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[25]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted the above Congressional explanation of routine use to mean that a "'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[26]

Subsequent Privacy Act case law interprets the Act's legislative history to limit routine use disclosure based upon a precisely defined system of records purpose. In *United States Postal*

[24] 5 U.S.C. § 552a(b)(3) referencing § 552a(a)(7).
[25] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[26] *Id.*

Service v. National Association of Letter Carriers, AFL-CIO, the Court of Appeals for the D.C. Circuit relied on the Privacy Act's legislative history to determine that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[27] The Court of Appeals went on to quote the Third Circuit as it agreed, "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[28]

The Education Department's sole routine use of information disclosure will be to contractors and contractor employees that "perform *any* function that requires [the Education Department] [to disclose] records in this system to the contractor's employees . . ."[29] (emphasis added). As discussed above, Privacy Act routine uses must be narrowly and specifically defined and compatible with the purpose of the system. As it is written, the proposed routine use is overly broad because does not establish a clear nexus between the proposed routine use and the system's purpose. The Department must clarify the specific "functions" that will require the agency to disclose records to contractors and their employees. Moreover, the Education Department should limit disclosing records to outside contractors to diminish risks to student data privacy. Pursuant to a 2013 lawsuit, EPIC uncovered that many Education Department contractors failed to submit required documentation regarding Privacy Act compliance.[30]

---

[27] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[28] *Id*. at 145 (quoting *Britt v. Natal Investigative Serv.*, 886 F.2d 544, 549-50 (3d. Cir. 1989). *See also Doe v. U.S. Dept. of Justice*, 660 F.Supp.2d 31, 48 (D.D.C. 2009) (DOJ's disclosure of former AUSA's termination letter to Unemployment Commission was compatible with routine use because the routine use for collecting the personnel file was to disclose to income administrative agencies); *Alexander v. F.B.I*, 691 F. Supp.2d 182, 191 (D.D.C. 2010) (FBI's routine use disclosure of background reports was compatible with the law enforcement purpose for which the reports were collected).
[29] Privacy Act SORN at 75,454.
[30] *EPIC v. Education Department—Private Debt Collector Privacy Act Compliance*, EPIC, http://epic.org/foia/ed/.

Accordingly, the Education Department should limit disclosure to contractors and clarify the specific functions for which the Department will disclose records. This clarification is required by the Privacy Act, and will ensure accountability, oversight, and transparency when the Department discloses student records.

Conclusion

For the foregoing reasons, the Education Department must revise its Privacy Act notice for the Impact Evaluation of Data-Driven Instruction Professional Development for Teachers. To meaningfully protect student data, the Department should not collect student personally identifiable information and should instead only collect aggregate student data. If, however, the Department collects students' personal information, the Department must revise the Privacy Act SORN to: (1) limit the collection of student information to only that which is necessary and relevant; and (2) clarify the circumstances under which it will disclose information pursuant to the routine use exception. EPIC anticipates the Education Department's specific and substantive responses to each of these proposals. As the SORN provides, EPIC anticipates that the system of records will not go into effect on January 4, 2016 as a result of these public comments.[31]

Respectfully submitted,

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Associate Director and
Director, EPIC Student Privacy Project

Electronic Privacy Information Center
1718 Connecticut Avenue NW
Suite 200
Washington, DC 20009
202.483.1140 x 107

[31] Privacy Act SORN at 75,452.