epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Khaliah Barnes
Administrative Law Counsel
Electronic Privacy Information Center

Study Session regarding inBloom, Inc.

Before the

Colorado State Board of Education

May 16, 2013

Mister Chairman and Members of the Board, thank you for the opportunity to participate in today's study session concerning inBloom and private company educational technology services. My name is Khaliah Barnes. I am Administrative Law Counsel and I coordinate the Student Privacy Project at the Electronic Privacy Information Center ("EPIC").

EPIC is a non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues. We work with a distinguished panel of advisors in the fields of law, technology, and public policy. EPIC has a particular interest in protecting student privacy and has worked in this field for many years.[1]

The Family Educational Rights and Privacy Act ("FERPA") is a federal student privacy and confidentiality statute that: (1) grants students certain rights — such as access to and amendment of their education records; and (2) details how schools and other entities entrusted with student records must protect that information from unauthorized disclosure. FERPA's legislative history expresses Congressional intent that, with the adoption of the Act, "parents and students may properly begin to exercise their rights under the law, and the protection of their privacy may be assured."[2] FERPA was enacted in response to "the growing evidence of the abuse of student records across the nation."[3] Senator Buckley, one of FERPA's principal sponsors, emphasized the "larger problem of the violation of privacy and other rights of children and their parents that increasingly pervades our schools."[4] FERPA's purpose is to "affirm the privacy and rights of children and their parents," ensure parental access to student information, and extend the "personal shield for every American against all invasions of privacy" to students.[5]

Over the last several years, the Education Department has issued regulations interpreting FERPA that have significantly diminished students' control over their education records. These regulations, issued in 2008 and 2011, grant third party entities and companies, like inBloom, with access to sensitive student information. In 2012, EPIC sued the Education Department over its 2011 FERPA regulations. The decision is currently pending in federal court.

We appreciate the Board's interest in protecting student privacy. In my statement today, I will explain EPIC's longstanding interest in student privacy, including our recent lawsuit against the Education Department, underscore the concerns that many students and parents today have regarding student privacy, and recommend affirmative steps that the Colorado Board of Education should implement should it continue to use inBloom and other private technology education services.

---

[1] *Student Privacy*, EPIC, http://epic.org/privacy/student/ (last visited May 15, 2013).
[2] 120 Cong. Rec. 39,863 (1974).
[3] 121 Cong. Rec. 7,974 (daily ed. May 13, 1975) (remarks of Senator Buckley).
[4] 120 Cong. Rec. at 13,951-52.
[5] *Id*.

EPIC's Interest in Student Privacy

EPIC has a strong interest in supporting the rights of students and their parents to control the collection and disclosure of education records. We have specifically worked to protect the student privacy rights that were established by FERPA.

In 2009, EPIC, joined by more than 100 local, state, and national organizations, urged then Secretary of Defense Donald Rumsfeld to end the "Joint Advertising and Market Research Studies" military Recruiting Databases because it did not have sufficient privacy protections.[6] This massive database contains troves of information, including student information (*e.g.*, grade point average, graduation date), date of birth, address, and ethnicity.[7] Because of EPIC's efforts, the Defense Department granted individuals the right to opt-out of the database.[8]

In 2011, EPIC filed an *amicus* brief in *Chicago Tribune v. University of Illinois*, a case involving student privacy rights protected by FERPA.[9] EPIC's brief argues that Congress intended to protect student records, including admissions files, from unauthorized release and that Illinois' open government law must yield to the federal privacy law.

And more recently, in 2012, EPIC sued the Education Department for its 2011 FERPA regulations.[10] The proposed regulations removed limitations prohibiting educational institutions and agencies from disclosing student personally identifiable information, without first obtaining student or parental consent. Specifically, the Education Department's regulations reinterpreted FERPA statutory terms "authorized representative," "education program," and "directory information." This reinterpretation gives non-governmental actors increased access to student personal data. In our lawsuit, we argue that under the Administrative Procedure Act, the Department's 2011 regulations amending FERPA exceed the agency's statutory authority and are contrary to law.

EPIC's lawsuit followed detailed comments we submitted to the agency, explaining the purpose of FERPA, the importance of student privacy, and the growing privacy risks that third parties present when granted access to sensitive student information. We urged the agency to withdraw its proposed changes. It was only after the agency failed to act on our recommendations that we chose to file the lawsuit.

---

[6] Letter from Privacy Coalition to the Hon. Donald H. Rumsfeld (Oct. 18, 2005), *available at* http://privacycoalition.org/nododdatabase/letter.html.

[7] *Defense Privacy and Civil Liberties Office—Privacy—System of Records Notices (SORNs)—DoD Wide Notices—DHRA 04*, DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE, http://dpclo.defense.gov/privacy/SORNs/dod/DHRA04.html (last visited May 15, 2013).

[8] *Id*.

[9] *Chicago Tribune v. University of Illinois*, EPIC, http://epic.org/amicus/tribune/ (last visited May 15, 2013.

[10] *EPIC v. The U.S. Department of Education*, EPIC, http://epic.org/apa/ferpa/default.html (last visited May 15, 2013).

As discussed below, inBloom has access to educations under both the 2011 and 2008 regulations.

Current State of Student Privacy

Students are currently subject to more forms of tracking and monitoring than ever before. This raises significant privacy problems because of the amount of sensitive data collection, and the opacity of student databases and how student information is used. Previously, schools assessed student achievement through objective and transparent standards such as test scores, grade point averages, attendance records, and graduation credits. Students routinely had access to their evaluation metrics and could readily understand why they received a particular grade or were marked late for a class.

Also, schools maintained education records in-house. As a practical matter, this meant that the ability of third parties to get access to students' educational records was limited. And schools treated requests from third parties for such records like transcripts with significant care. Decisions were made about what information to include in the record that was made available to others. Efforts were also undertaken to ensure the accuracy of the information provided. And students were notified about the release of these records. In fact, student records were often disclosed to third parties, such as colleges where a student might be applying, at the request of the student.

The 2008 FERPA regulations permit schools to release education records to outside contractors, consultants, volunteers, and other parties performing a school function or service that the school would otherwise perform itself. Pursuant to the 2008 regulations, many schools increasingly outsource schools tasks to third party private companies, like inBloom. While we understand the value of data for promoting and evaluating personalized learning, there are too few safeguards for the amount of data collected and transmitted from schools to private companies.

inBloom operates a highly complex, multilayer data model that schools use to evaluate students. inBloom states that some of the data are "interdependent" and can be used to understand a causal relationship between certain data.[11] Some of this information is useful for student instruction. We expect for schools to collect, and there is a causal relationship between, student attendance information, credit requirements, and test scores. inBloom, however, is equipped to collect other data sets that raise privacy problems. Moreover, students and their parents are at a fundamental disadvantage when schools collect hundreds of data elements, and use those to evaluate students unbeknownst to them.

For example, the inBloom database is equipped with a "student cohort" domain, which "represents a wide variety of collections of students," which can include "students that are tagged for interventions or . . . for the purposes of tracking or analysis, such as a principal watch

[11] *Introduction to the inBloom Data Store Logical Model*, INBLOOM, https://www.inbloom.org/sites/default/files/docs-developer/data_model-intro.html (last visited May 15, 2013).

list."[12] To the extent that Colorado schools maintain "principal watch lists" and disclose this information to inBloom, students should be informed of the criteria for inclusion on and removal from the list, and have to right to access and amend their information. Further, inBloom's Discipline Domain has categories representing "actions or behaviors that constitute and 'offense' in violation of laws, rules, policies, or norms of behavior.'"[13] While violating laws, rules, or school policies is a clear disciplinary infraction, violating "norms of behavior" is a seemingly arbitrary standard to be included on an education record, subject to the review of a potential employer.

inBloom's Disciple Domain also permits schools to label students based on their involvement with discipline incidences (*e.g.* "perpetrator" or "accomplice").[14] These are only a fraction, and some of the most troubling data components within inBloom's database. Although certain disciplinary infractions do involve law enforcement, and therefore terms like "perpetrator" or "accomplice" are arguable appropriate, schools should be reluctant to label K-12 students using criminal terminology in an electronic database. This is because these records could be used later in life for employment and postsecondary school decisions.

As Joel Reidenberg, law professor and the director of the Fordham Center on Law and Information Policy ("CLIP") has stated, "[t] he choice of [inBloom] data fields is a policy decision."[15] Because Colorado controls the data it discloses to inBloom, we encourage Colorado to make a policy to limit the data that it makes available to inBloom.

Student Records and Data Security

By collecting troves of sensitive student information, schools, and the private companies to which they outsource information, have a duty to ensure the security of that data. In 2009, Fordham Law's CLIP conducted a study on the privacy protections in statewide K-12 longitudinal databases.[16] The study underscores the current problems with student data security. Among its other findings, Fordham found that "most states collected information in excess of what is needed" for government reporting requirements," student 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 . . .

---

[12] *Student Cohort Domain*, *Data Domains*, INBLOOM, https://www.inbloom.org/sites/default/files/docs-developer/data_model-domains.html#data_model-domains-StudentCohort (last visited May 15, 2013).
[13] *Discipline Domain*, *Data Domains*, INBLOOM, https://www.inbloom.org/sites/default/files/docs-developer/data_model-domains.html#data_model-domains-Discipline (last visited May 15, 2013).
[14] *Id*.
[15] Ellis Booker, *Education Data: Privacy Backlash Begins*, INFORMATION WEEK (Apr. 26, 2013, 09:55 AM) http://www.informationweek.com/education/data-management/education-data-privacy-backlash-begins/240153668.
[16] 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 (2009).

outsource the data warehouse without any protections for privacy in the vendor contract."[17] FERPA requires that educational agencies or institutions use "reasonable methods" to ensure that school officials and authorized representatives like inBloom properly safeguard individual data. Because the Education Department encourages a reasonable method standard, and because inBloom itself states that it is the responsibility of "each adopting stated . . .to ensure that their use of [inBloom]" is compliant with FERPA and other data security laws,[18] Colorado should take this opportunity to pass legislation concerning data security to govern inBloom and other private education technology companies. Currently, inBloom has a Data Privacy and Security Policy, but it reserves the right to modify it "from time to time, as approved by [an] independent advisory board."[19] Moreover inBloom states that a "[c]ustomer's continued use of the SLI Services will indicate its acceptances of the Data Privacy and Security Policy."[20] If, however, the data provided by Colorado belongs to Colorado, as inBloom has stated, then Colorado should also exercise control over how student data is protected, and Colorado should craft student data security legislation.

The 2009 Fordham CLIP report on elementary and secondary school statewide longitudinal databases made explicit recommendations referenced below, that Colorado should incorporate when disclosing student personal information to inBloom and other education technology companies.

1. Colorado should use "comprehensive agreements that explicitly address privacy obligations":

Colorado's current agreement with inBloom (and other companies) should, among other things, "set out the obligations of confidentiality, require physical and access security, define the duration of data storage," and "specify the standards to be applied for each of these obligations (*e.g*. level or type of encryption, etc.)."[21]

2. Colorado should limit its data collection and transfer to inBloom solely to "necessary information."

CLIP aptly notes that the "risk of security breaches and misuse is too large to justify the collection of sensitive information in an electronic record." [22] It is for this reason that Colorado should explicitly adopt privacy practices that restrict the amount of data schools collect and in put into the inBloom database.

---

[17] 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).
[18] *Privacy Commitment*, INBLOOM, https://www.inbloom.org/privacy-commitment (last visited May 15, 2013).
[19] Service Agreement between Colorado Dep't of Educ. and the Shared Learning Colloborative, LLC, Nov. 2, 2012, 4.
[20] *Id*.
[21] FORDHAM LAW SCHOOL CTR. ON LAW AND INFO. POLICY, *supra* note 16, at 54.
[22] *Id*.

3. Colorado should have increased access to conduct independent and network security reviews of inBloom and other private technology services

The 2012 Service Agreement between inBloom and the Colorado Department of Education only allowed Colorado to conduct independent code and network security reviews for each major release, and no more than once every six months.[23] In the event that Colorado had reasonable cause to believe inBloom was not in compliance with this Agreement, Colorado could conduct this independent review up to once every three months.[24] Subject to a mutually agreeable time for both contract parties, Colorado should have increased access to conduct independent network security reviews of inBloom. The current proposal is too restrictive. If Colorado is not granted increased access to audit inBloom's system, Colorado cannot meaningfully ensure student data security.

4. Colorado should provide parents and students with access to any agreements with inBloom and other private education technology services.

We applaud the Colorado State Board of Education for conducting a collaborative and transparent dialogue concerning inBloom. We do note, however, that because of the complexity of the database, the Colorado Department of Education should provide access on its website to: "an easy to read summary" of inBloom; inBloom and the Colorado State Board of Education privacy policy and agreement; and "an electronic record review and change procedure so that parents can easily stay up-to-date on what information is in their child's record."[25]

5. Colorado should ensure that students and parents have access to the educational records that are being maintained by third party providers and also be able to limit disclosure to third parties

The central concern of FERPA was the prospect that secret profiles would be created on students and that this information would later be used in ways that could cause real harm later in life when students pursued educational opportunities, sought jobs, or applied for credit. Congress made clear that student and their parents should know what information is collected and should be able to limit its use. As the Department of Education moves to loosen these safeguards, the states should step in and protect student privacy.

Conclusion

The sweeping increase of student data collection must be met with increased privacy protections. State and local legislation and oversight can help safeguard student privacy.

Thank you for the opportunity to participate in today's study session. I will be pleased to answer your questions.

---

[23] Service Agreement, *supra* note 19, at 17.
[24] *Id*.
[25] FORDHAM LAW SCHOOL CTR. ON LAW AND INFO. POLICY, *supra* note 16, at 56.