epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Caitriona Fitzgerald, State Policy Coordinator

Electronic Privacy Information Center (EPIC)

Before the

Legislative Council Study Committee on School Data

Wisconsin State Legislature

August 16, 2016

Chairman Thiesfeldt, Vice-Chairman LeMahieu and Members of the Study Committee on School Data, thank you for the opportunity to participate in today's Committee meeting. My name is Caitriona Fitzgerald, and I am the State Policy Coordinator for the Electronic Privacy Information Center (EPIC). EPIC is pleased to respond to the Committee's request for testimony on the issue of student privacy.

EPIC is a non-partisan research organization in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] We work with a distinguished panel of advisors in the fields of law, technology, and public policy.[2] EPIC has a particular interest in protecting student privacy and has worked in this field for many years.[3] Most recently, EPIC and a coalition of legal scholars, technical experts, and many leading privacy organizations petitioned the Education Department to establish a data security rule to protect student records.[4] In 2013, we urged Congress to investigate student privacy practices and to strengthen the Family Educational Rights and Privacy Act ("FERPA").[5] In 2014, EPIC wrote the Student Privacy Bill of Rights, an enforceable student privacy and data security framework.[6]

We appreciate the Legislature's interest in protecting student privacy. Meaningful, effective outcomes that protect student privacy are long overdue. Schools and companies collect students' location, health, discipline, social media information, and other sensitive data with no accountability.[7] In my statement today, I will: (1) describe how the current regulatory framework encourages mass collection of student records; (2) discuss the privacy risks that students today face; (3) underscore the need for data security safeguards; and (4) recommend that Wisconsin adopt the Student Privacy Bill of Rights to ensure student privacy in the digital age.

---

[1] *About EPIC*, EPIC, http://epic.org/epic/about.html (last visited August 12, 2016).
[2] *EPIC Advisory Board*, EPIC, http://epic.org/epic/advisory_board.html (last visited August 12, 2016).
[3] *Student Privacy*, EPIC, http://epic.org/privacy/student/ (last visited August 12, 2016).
[4] Letter from EPIC et al. to Secretary John B. King, U.S. Department of Education (June 6, 2016), https://epic.org/privacy/student/ED-Data-Security-Petition.pdf.
[5] Letter from Marc Rotenberg & Khaliah Barnes, EPIC, to Senate Comm. on Health, Educ., Labor & Pensions & House Educ. & the Workforce Comm. (Oct. 9, 2013), https://epic.org/apa/ferpa/EPIC-ED-Student-Privacy-Letter.pdf.
[6] *Student Privacy Bill of Rights*, EPIC, https://epic.org/privacy/student/bill-of-rights.html. *See also* Valerie Strauss, *Why a 'Student Privacy Bill of Rights' is Desperately Needed*, THE WASHINGTON POST ANSWER SHEET BLOG (Mar. 6, 2014, 3:30 PM), http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.
[7] *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/.

I. The Current Student Privacy Regulatory Framework Encourages Mass Collection of Student Records

The Family Educational Rights and Privacy Act ("FERPA") is a federal student privacy that grants students the right to control who has access to their information.[8] FERPA also permits students to access and amend their records.[9] In enacting FERPA, 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."[10] Congress enacted FERPA in response to "the growing evidence of the abuse of student records across the nation."[11] Senator James 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."[12] 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.[13]

As it was originally adopted, FERPA provided the necessary safeguards to protect students from harm. Over the last several years, however, 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 companies, government agencies outside of the education space, and other third party entities access to sensitive student information.[14]

In 2012, EPIC sued the Education Department over its 2011 FERPA regulations.[15] The 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."[16] This reinterpretation gives non-governmental actors increased access to student personal data. In our lawsuit, we argued 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 intimate student information.[17] We urged the agency to withdraw

---

[8] 20 U.S.C. § 1232g.
[9] Id. § (a)(1)-(2).
[10] 120 Cong. Rec. 39,863 (1974).
[11] 121 Cong. Rec. 7,974 (daily ed. May 13, 1975) (remarks of Senator Buckley).
[12] 120 Cong. Rec. at 13,951-52.
[13] *Id*.
[14] Family Educational Rights and Privacy Act Final Regulations, 73 Fed. Reg. 74,806 (Dec. 9, 2008); Family Educational Rights and Privacy Act Final Regulations, 76 Fed. Reg. 75,604 (Dec. 2, 2011).
[15] *Elec. Privacy Info. Ctr. v. U.S. Dep't of Educ*., CV 12-0327 (ABJ), 2014 WL 449031 (D.D.C. Feb. 5, 2014).
[16] 2011 regulations, *supra* note 14.
[17] *Comments of the Elec. Privacy Info. Ctr. to the Dep't of Educ., Notice of Proposed Rulemaking, RIN 1880-AA86*, May 23, 2011, *available at* http://epic.org/privacy/student/EPIC_FERPA_Comments.pdf.

its proposed changes. It was only after the agency failed to act on our recommendations that we chose to file the lawsuit.

In September 2013, the Court dismissed the case on procedural grounds. Importantly, the court never reached the substantive issue as to whether the Education Department had the legal authority to change the student privacy law.

In June 2016, EPIC, and a coalition of legal scholars, technical experts, and many leading privacy organizations petitioned the Education Department to establish a data security rule to protect student records.[18] The experts and groups explained that data breaches now plague schools and colleges across the country, following recent changes to the Family Educational Rights and Privacy Act. The petition calls for the establishment of rules for encryption, privacy enhancing techniques, and breach notification.[19]

By removing FERPA's well-established limitations on student record dissemination, the Education Department permitted and encouraged third party access to student records. And in response, there has been an overwhelming demand for private student information.

II. Big Data's Mass Sensitive Student Data Collection Presents Big Risks for Student Privacy

Pursuant to the Education Department's regulations, 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
- Migrant
- Remedial

[18] Letter from EPIC et al. to Secretary John B. King, *supra* note 4.

[19] *See* Valerie Strauss, *Privacy advocates accuse Obama administration of failing to properly protect student data*, THE WASHINGTON POST ANSWER SHEET BLOG (June 7, 2016), https://www.washingtonpost.com/news/answer-sheet/wp/2016/06/07/privacy-advocates-accuse-obama-administration-of-failing-to-properly-protect-student-data/.

- 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?[20]

Plans are already underway to include personalized learning analytics and information detailing whether students ends up on welfare or in jail after high school.[21]

Private companies, too, have an insatiable appetite for student information. For example, in 2013, EPIC filed a complaint with the Federal Trade Commission concerning Scholarships.com, a popular website among high school students researching college scholarships.[22] The website encouraged students to share intimidate details, including religious affiliation, and health information, including whether the student has ADD/ADHD, hepatitis, cancer related medical issues, digestive or mental impairments, and whether the student is clinically depressed or overweight.[23] The website also encouraged students to divulge whether they have current alcohol addictions or are recovering alcoholics; have parents who are illegal immigrants; are domestic abuse victims; have drug addictions or convictions; are lesbian, gay, bisexual, transgender ("LGBT") or have an LGBT parent; and are political activists.[24] The website did not disclose that it would provide this student data to its business partner for general advertising purposes.[25]

[20] Anya Kamenetz, *What Parents Need to Know About Big Data and Student Privacy*, NPR: ALL TECH CONSIDERED (Apr. 28, 2014, 11:58AM), http://www.npr.org/blogs/alltechconsidered/2014/04/28/305715935/what-parents-need-to-know-about-big-data-and-student-privacy.
[21] *Id.*
[22] *In the Matter of Scholarships.com, LLC* (Dec. 12, 2013), *available at* http://epic.org/privacy/student/EPIC-FTC-Compl-Scholarships.com.pdf.
[23] *Id*.
[24] *Id*.
[25] *Id*.

More recently, Google has been under fire for illegally reading student emails for commercial purposes.[26] Students and alumni of University of California-Berkley sued Google for allegedly scanning students' emails without their consent. After a similar lawsuit in 2013, Google stated that it "permanently removed all ads scanning in Gmail for Apps for Education" which, according to the lawsuit, is an admission that, prior to that statement, Google was in fact analyzing student e-mails for advertising purposes.[27] These are just a handful of examples in the growing trend of mass student data collection.

This type of unbounded intimate data collection greatly increases the risks that students will be stigmatized, and that transgressions and shortcomings from the classroom will follow students for the rest of their lives. In fact, concerns about the long lasting implications of student data collection galvanized Congress to pass FERPA. FERPA's legislative history discusses *Merriken v. Cressman*, a federal case analyzing the privacy implications of a school program designed to identify potential eighth grade drug abusers.[28] Although the case is over forty years old, it bears many similarities to today's environment where mass student data collection is espoused, but rarely vetted. The court found that

> letters to the parents were 'selling devices' aimed at gaining consent without giving negative information that would make the parents completely aware of 'the relevant circumstances and likely consequences' of the Program . . . the letter to the parents gave only one side of the test picture. There were no statements to the parents concerning the self-fulfilling prophecy, scapegoating of those children who opted not to participate or the ultimate use of the data as it would effect their children and law authorities who might find it necessary to use that information . . .[29]

The court ultimately held that this invasive student data collection violated students' and parents' "right to privacy inherent in the penumbras of the Bill of Rights of the Untied States Constitution."[30] *Merriken v. Cressman* illustrates "the potential harm that can result from poorly regulated testing, inadequate provisions for the safeguarding of personal information, and ill-devised or administered behavior modifications programs."[31]

Through FERPA, Congress aimed to ward against the problems that currently plague student privacy. But, as discussed above, the Education Department's regulations substantially set student privacy back.

---

[26] Emma Brown, *UC-Berkeley students sue Google, alleging their emails were illegally scanned*, WASHINGTON POST (Feb. 1, 2016), https://www.washingtonpost.com/news/grade-point/wp/2016/02/01/uc-berkeley-students-sue-google-alleging-their-emails-were-illegally-scanned/.
[27] *Protecting Students with Google Apps for Education*, GOOGLE (Apr. 30, 2014), http://googleenterprise.blogspot.co.uk/2014/04/protecting-students-with-google-apps.html.
[28] *Merriken v. Cressman*, 364 F. Supp. 913, 915 (E.D. Pa. 1973).
[29] *Id*. at 919.
[30] *Id*. at 922.
[31] 120 Cong. Rec. 14,581.

III. There are No Adequate Data Security Safeguards to Protect Against Unauthorized Access to Student Records

Despite removing FERPA's privacy safeguards, the Education Department has declined to ensure student data protection. The Department itself 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."[32] Yet, the Department "does not believe it is appropriate to regulate specific data security requirements under FERPA."[33] Students have had their information continuously compromised "due to weak or nonexistent data security protocols."[34]

What follows below is a small sample of examples[35] 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."[36] The breached records included records going as far back as 1992.[37]

- 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.[38] By some estimates, the breach impacted "approximately 50 percent of current students and 65 percent of active employees."[39]

- 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.[40]

---

[32] 2011 regulations, *supra* note 14, at 75,622.
[33] *Id*.
[34] *Id*.
[35] *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-data-breach/2014/01/08/d0163b50-78ad-11e3-8963-b4b654bcc9b2_story.html.
[36] UMD Data Breach, UNIVERSITY OF MARYLAND, http://www.umd.edu/datasecurity/.
[37] *Id*.
[38] 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/
[39] *Id*.
[40] 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.

- D.C. Public Schools recently posted education records of approximately 12,000 public school special needs students online. The information included "each student's identification number, race, age, school, disabilities and any services he or she receives."[41] 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.[42]

- 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.[43]

- 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.[44]

- Iowa State reported a breach in 2014 that compromised the Social Security numbers of 29,780 students covering a seventeen-year span.[45]

- 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."[46] Butler's compromised records included names, birthdates, Social Security numbers, and academic records.[47] The hack affected former students going back as far as the 1980s.[48]According Butler University, the security breach arose from "unauthorized hacking into Butler University's computer network between November 2013 and May 2014."[49].

---

[41] 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.
[42]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.
[43] 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/.
[44] Indiana University Reports Potential Data Exposure, INDIANA UNIVERSITY (Feb. 25, 2014) http://news.iu.edu/releases/iu/2014/02/data-exposure-disclosure.shtml.
[45] *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.
[46] 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.
[47] June 26, 2014 Butler University letter.
[48] *Supra* note 46.
[49] *Supra* note 47.

- 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.[50] The breach exposed personal information including "names, birth dates, Social Security numbers, and bank account information [.]"[51] This breach followed an earlier 2011 MCCD breach.[52]

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. [53] 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."[54]

IV. Wisconsin Should Adopt the Student Privacy Bill of Rights, an Enforceable Student Privacy and Data Security Framework

In a March 2014 *Washington Post* article, EPIC unveiled the Student Privacy Bill of Rights, an enforceable student privacy and data security framework.[55] In line with President Obama's Consumer Privacy Bill of Rights, which is based largely based on the well-established Fair Information Practices ("FIPs"), schools, districts, and EdTech and other cloud-based service providers should adhere to the following practices when collecting student data. These rights should transfer from parents or legal guardians to students once the student is eighteen or attending college:

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.

---

[50] *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.

[51] *Id*.

[52] 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.

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

[54] 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).

[55] Valerie Strauss, *Why a 'Student Privacy Bill of Rights' is Desperately Needed*, THE WASHINGTON POST ANSWER SHEET BLOG (Mar. 6, 2014, 3:30 PM), http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.

- There are gaps in current laws and proposed frameworks concerning students' access and amendment to their data. Schools, companies, government agencies, and other entities that collect any student information should provide student access to this information. This includes access to any automated decision-making rule-based systems (*i.e*, personalized learning algorithms) and behavioral information.

2. **Focused collection:** Students have the right to reasonably limit student data that companies and schools collect and retain.
    - EdTech companies should collect only as much student data as they need to complete specified purposes. "Educational purposes" and "educational quality" are frequent examples of broad and fluid purposes that grant EdTech carte blanche to collect troves of student data. A more focused collection would, for example, specify that the collection is necessary to "improve fifth grade reading skills" or "enhance college-level physics courses." In focusing student data collection for specific purposes, schools and companies should consider the sensitivity of the data and the associated privacy risks.

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.
    - Schools and companies should never repurpose student data without express written student consent. This includes using student data to serve generalized or targeted advertisements. The Education Department's guidance states that federal student privacy laws do no prohibit schools or districts "from allowing a provider acting as a school official from serving ads to all students in email or other online services." This allows service providers to repurpose the information. Schools provide private companies access to student data to help enhance education quality. When companies use this access for general marketing purposes, they have repurposed the student data and turned the classroom into a marketplace.

4. **Security:** Students have the right to secure and responsible data practices.
    - Amid recent, large-scale student data breaches, schools and companies must increase their data safeguards to ward against "unauthorized access, use, destruction, or modification; and improper disclosure" as described in the CPBR. Companies should immediately notify schools, students, and appropriate law enforcement of any breach. And schools should immediately notify students when there is a breach. Schools should refrain from collecting information if they cannot adequately protect it. Securing student information also entails deleting and de-identifying information after it has been used for its initial and primary purposes (no secondary uses allowed!).

5. **Transparency:** Students have the right to clear and accessible information privacy and security practices
    - Schools and companies should publish the types of information they collect, the purposes for which the information will be used, and the security practices in

place. Schools and companies should also publish algorithms behind their decision-making.

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
    - Schools and companies should be accountable to enforcement authorities and students for violating these practices.

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.

In light of (1) how the current regulatory framework encourages mass collection of student records; (2) the privacy risks that students today face; and (3) the need for data security safeguards, Wisconsin should adopt the Student Privacy Bill of Rights to ensure student privacy in the digital age.