Testimony of Rachael Stickland, Co-Founder, Co-Chair
Parent Coalition for Student Privacy

Before the United States House of Representatives
House Committee on Education and the Workforce

Hearing on Strengthening Education Research and Privacy Protections to Better Serve Students

March 22, 2016

Good morning Chairman Kline, Ranking Member Scott and distinguished members of the Committee. I would like to thank you for the opportunity to testify today on behalf of parents concerned about strengthening privacy protections to better serve students.

My name is Rachael Stickland. I am a parent of two public school children in Colorado, and I am co-founder and co-chair of the Parent Coalition for Student Privacy which represents a wide coalition of parents from across the nation, from Florida to Washington, California to New York, including Democrats, Republicans and Independents, public school parents and homeschoolers, professionals and stay-at-home mothers. We receive no funding from special interests, and are united in our effort to protect all children and their privacy. We came together in July 2014 after working together as individuals and groups to defeat the widely criticized inBloom project.[1]

The controversy surrounding this corporation that was designed to collect the personal information from students in nine states and districts sparked a new awareness among parents nationwide about how widely their children's personal data was already being disclosed to third parties beyond the schoolhouse doors, and how few protections existed against its misuse. Though inBloom is now gone, parents continue to seek answers to exactly what information pertaining to their children is being collected, who has access to the information and for what purpose, and when that information will be destroyed.

I would like to focus my testimony today on the need to strengthen federal educational law to meet the challenges of our modern educational ecosystem and to address the current threats to student privacy. Specifically, I will place an emphasis on personal student information collected by schools and school districts that are then disclosed to state education departments and maintained in Statewide Longitudinal Data Systems or SLDS.

Currently, schools collect much more information on students than most parents realize. While some was required by *No Child Left Behind* and individual state mandates, much of the data now collected appears to transcend legal requirements. Beyond standard transcript-type data like student names, addresses, courses taken, grades earned and days absent, schools also collect hundreds of pieces of information like disabilities and interventions, medical information from 504 plans, disciplinary incident reports, scores on standardized exams, school readiness scores and recommendations for grade retention. Additionally, schools or commercial vendors used by schools collect highly personal information from students as they use online education tools such as Google Apps for Education or Khan Academy.

[1] *See* Benjamin Herold, inBloom to shut down amid growing privacy concerns, Education Week, Apr. 21, 2014 http://blogs.edweek.org/edweek/DigitalEducation/2014/04/inbloom_to_shut_down_amid_growing_data_privacy_concerns.html

Once this information is collected at the local level, much of it is pushed up to the state to be maintained in the state unit record system called the SLDS or the P-20W (preschool through workforce). These unit record systems have been funded partly through federal grants awarded in five rounds of funding from 2005-2012. Forty seven of fifty states as well as the District of Columbia, Puerto Rico, and the Virgin Islands have received at least one SLDS grant.[2] These systems are intended to match students and teachers for the purpose of teacher evaluation, and to promote interoperability across multiple state agencies, as well as across state lines via multi-state consortia.

Rather than simply collecting standard administrative data, these SLDS systems have the capability to maintain upwards of 400 data elements on each individual child. According to the Colorado State Department of Education, our SLDS project is designed to link information from the education department to five other state agencies, including the Colorado Department of Higher Education (CDHE), Colorado Department of Labor and Employment (CDLE), Colorado Department of Corrections (CDOC), Colorado Department of Public Safety (CDPS) and the Colorado Department of Human Services (CDHS). [3] The individually identifiable life-information that is so neatly organized in these systems effectively become life-long dossiers and, if or when compromised, could give away the entire life history of every student in a state.

Interagency linkages like Colorado's SLDS and even interstate linkages [4] would not have been permissible prior to the unilateral regulatory changes to the federal student privacy law known as FERPA by the Department of Education in 2011. [5] The parents we represent strongly urge Congress to strengthen FERPA and restore the robust protections it originally contained that prohibited the expansion of the SLDS program.

SLDS's purported purpose is to help states, districts, schools, educators, and other stakeholders make data-informed decisions to improve student learning and outcomes; as well as to facilitate research to increase student achievement and close achievement gaps. Parents don't disagree with the premise that data can and should be used for purposes to help advance their children's education. However, parents are concerned about SLDS because of the lack of compelling governmental interest which would justify this level of tracking that serves as an open invitation to mission creep. The availability of a dataset as rich as SLDS quickly turns it into the go-to data mart for authorized or unauthorized use by other institutions, organizations, and state agencies.

For example, earlier this year a California organization filed a lawsuit alleging that the state is failing to ensure districts provide services to all children who need them. The federal judge ruled in favor of the plaintiff and ordered the release of records for 10 million California students dating back to 2008

[2] *See* U.S. Department of Education, Institute of Education Sciences, National Center for Education Statistics Statewide Longitudinal Data Systems Grant Program http://nces.ed.gov/programs/slds/stateinfo.asp
[3] *See* Colorado Department of Education's Statewide Longitudinal Data System "RISE" project https://www.cde.state.co.us/rise/connect
[4] *See* Western Interstate Commission for Higher Education report *Beyond Borders: Understanding the Development and Mobility of Human Capital in an Age of Data-Driven Accountability* http://www.wiche.edu/info/longitudinalDataExchange/publications/MLDE_BeyondBorders.pdf
[5] *See* U.S. Department of Education Family Education Rights and Privacy Act, Final Rule Dec. 2, 2011 https://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf

maintained in the state SLDS known as CALPADS.[6] Highly sensitive information on every child in the state's education system were to be made available to the plaintiff's legal team including student "names, addresses, disciplinary records, grades, test scores, and even details such as pregnancy, addiction and criminal history."[7] Since the initial ruling in February, thousands of parents including the California PTA vehemently protested this unprecedented release. Because of the backlash, the judge has since modified her order allowing the plaintiff's legal team to access and query the CALPADS data system rather than receive a full copy of the system. It's worth noting that this disclosure of student information is authorized under current federal law, and as a result of the controversy the judge has since suggested modernizing FERPA.[8]

Another example of the unintended yet currently allowable use of SLDS was the attempt by the New York State Education Department, without public input or comment, to declare that all data in the SLDS should be placed into the state archives for a hundred years or more with no clear restrictions on access. After parent advocates discovered this decision in an obscure memo and protested, the state is now reconsidering this decision, but such a reckless policy without strong citizen oversight should never be allowed.[9] Should children of uniformed parents be any less protected?

Examples of authorized uses of SLDSs such as the California and New York cases are threat enough in their own right, but the high probability of breach or abuse should give advocates of maximal data collection in SLDS considerable pause. There are currently no specific security protections required for the collection and storage of this data unlike those required in HIPPA, for example, even though education records maintained by the SLDS often contain equally sensitive health information.

As Congress weighs competing interests in the student privacy debate, parents in our coalition urge you to always first think of the individual child. Allowing or incentivizing the government to track autonomous individuals through most of their lives in the name of research has speculative benefits at best and can instead lead to profiling, stereotyping and discrimination that can hinder a child's potential for growth and success. We agree with both the testimony provided by National PTA[10] and Microsoft[11] to the House Subcommittee on Early Childhood, Elementary and Secondary Education in February 2015 that an individual owns his or her own data. Parents believe this to mean the right to decide with whom it will be shared and under what conditions.

Recommendations

---

[6] *See* Elizabeth Weise, Calif. judge allows data release on 10M students, USA Today, Feb. 17, 2016 http://www.usatoday.com/story/tech/news/2016/02/16/morgan-hill-kimberly-mueller-california-public-schools-information-disabled-release-10-million/80472900/

[7] *See* Sharon Noguchi, Judge backtracks on release of California student records, San Jose Mercury News, Mar. 4, 2016 http://www.mercurynews.com/bay-area-news/ci_29590794/judge-pulls-back-from-calif-student-records-release?source=infinite-up

[8] *Ibid*

[9] New York Archives, Records Disposition Request rec-3, dated 12/20/13

[10] *See* Ms. Shannon Servier, National PTA, testimony before the U.S. House of Representatives Subcommittee on Early Childhood, Elementary and Secondary Education, Feb. 12, 2015 http://edworkforce.house.gov/uploadedfiles/sevier_testimony_final.pdf

[11] *See* Ms. Allyson Knox, Microsoft, testimony before the U.S. House of Representatives Subcommittee on Early Childhood, Elementary and Secondary Education, Feb. 12, 2015 http://edworkforce.house.gov/uploadedfiles/knox_testimony_final.pdf

Should Congress continue supporting the development and expansion of SLDS through federal grants, and as you contemplate student privacy as a legislative matter, please consider our coalition's recommendations for the SLDS program as well as the use of personal student information by schools and districts:

1. Increased transparency: At minimum, SLDS unit record systems must be subject to the Privacy Act of 1974's code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.[12] Optimally, parents must be told what student information is collected and by whom, how it is to be used and when it is to be destroyed, and to be notified in advance of any disclosure of personal student information to any persons, companies or organizations outside of the school or district.

2. In addition to increased transparency, parents also advocate for state Institutional Review Boards or IRBs to vet all uses of personal data, to question whether de-identified, anonymized or aggregated data could not be used in its stead, and to ensure that there are strict security standards and requirements for data destruction. We also urge that citizen oversight of the SLDS be required.

3. There should be no commercial uses of personal student information; or use for any marketing purposes should be banned.

4. Security protections: At minimum, there must be encryption of ALL personal data at motion and at rest, required training for all individuals with access to personal student data, audit logs, and security audits by an independent auditor.

5. Increased parent/student rights: Re-disclosures by vendors or any other third parties to additional individuals, sub-contractors, or organizations should be prohibited without parental notification and consent. Parents must be allowed to see any data collected directly from their child by a school or a vendor given access through the school, delete the data if it is in error or is nonessential to the child's transcript, and opt out of further collection, unless that data is part of their child's educational records at

[12] The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The Privacy Act of 1974 requires each federal agency that maintains a system of records shall publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include:
(A) the name and location of the system;
(B) the categories of individuals on whom records are maintained in the system;
(C) the categories of records maintained in the system;
(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
(F) the title and business address of the agency official who is responsible for the system of records;
(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and;
(I) the categories of sources of records in the system.

school. Any data-mining for purpose of creating student profiles, even for educational purposes, must be done with full parental knowledge. Parental consent must be required for disclosure for highly sensitive information such as their child's disabilities, health and disciplinary information. We also urge that HIPPA be used as a model which requires individual notice and consent before personal health information can be used in research, with few exceptions.

6. Enforcement: Any federal student privacy law should specify fines if the school, district or third party violates the law, their contracts and/or privacy policies; with parents able to seek redress on behalf of their children as well.

Thank you again for the opportunity to participate in this hearing and for your consideration of my testimony.