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

Before the United States House of Representatives
Committee on Education and the Workforce
Subcommittee on Early Childhood, Elementary and Secondary Education

Hearing on
"Exploring Opportunities to Strengthen Education Research While Protecting Student Privacy"

June 28, 2017

Thank you Chairman Rokita, Ranking Member Polis, and all the distinguished Members of the Subcommittee for inviting me to testify today on behalf of parents concerned about student privacy. My name is Rachael Stickland. I am a parent of two public school children in Colorado, the wife of a public schoolteacher, and the co-founder and co-chair of the Parent Coalition for Student Privacy, which represents a wide alliance of parents and organizations from across the nation.

Many parents first became aware of the severe threat to student privacy as a result of the controversy over inBloom Inc., which was created to collect and facilitate the disclosure of the personal data of millions of K12 students with a wide range of vendors and non-governmental third parties, without parental knowledge or consent. After inBloom collapsed in April 2014,[1] we formed our coalition to provide information to parents about threats to student privacy, and to give guidance as to best practices in data collection and disclosure. Since then, nearly 100 related state laws have been passed and just last month, we released a Parent Toolkit for Student privacy, in collaboration with the Campaign for Commercial-Free Childhood, to provide information and strategies to parents on how to advocate for stronger privacy protections at their children's schools and districts.

Today I would like to focus my testimony on the need for Congress to consider the broad implications to student privacy when data are collected and disclosed for various purposes, including research. I will share evidence showing how education agencies and institutions are currently unable to secure student data currently in their possession; explain why parents are apprehensive about state and federal collections of student information; and briefly outline why the Family Educational Rights and Privacy Act of 1974[2] (FERPA) must be updated before Congress moves forward with any proposal to use students' personal information for research or other purposes.

Inadequate security of student data

When inBloom first sparked a nationwide discussion on student privacy in 2013, parents were told that concerns over hacking were overblown because student data collected and disclosed by schools lacked "high target" financial information like bank account or credit card numbers. It turns out that data held by education institutions are a far bigger target than many had anticipated. Nearly every day a new breach of

[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
[2] 20 U.S.C. § 1232g

student data is reported. According to EdTech Strategies, a Virginia-based research consultancy, the number of breaches have more than doubled so far in 2017, and "U.S. K-12 public schools were reported to have experienced at least 147 separate cyber security-related incidents" in the last 18 months. Allegedly, students have had their identities stolen as a result of some of these incidents.[3] In fact, student data is extremely valuable to hackers for the purposes of identity theft because very few of them have negative credit histories.[4]

Colleges and universities also experience security threats to their networks and data repositories. In 2016 alone, 13% of "all higher education institutions" experienced a ransomware attack — "where a hacker takes control of the victim's information systems and encrypts data, preventing the owner from accessing it until the victim pays a sum of money."[5] This is the first time that the education sector outpaced the government, retail, and healthcare industries in this type of threat.

But cyber security incidents aren't limited to K-12 public schools and universities. As a 2015 report by the U.S. Government Accountability Office revealed, reports of security incidents involving breaches of personal information held by federal agencies sharply increased from 10,481 in 2009 to 27,624 in 2014 — an increase of 164 percent over five years — for a total of 144,439 reported instances.[6] The report also noted that these events can "adversely affect national security; [and] damage public health and safety."

The U.S. Department of Education has been found to have especially weak security standards in its collection and storage of student information, as reported by an audit released in November 2015 by the department's Inspector General. According to the audit, staff in the Inspector's office hacked into the Department's main IT system and gained unfettered access to personal data without anyone noticing. Overall, the audit found significant weaknesses in four out of the five security categories.[7] In May 2016, the government scorecard created to assess how well federal agencies were implementing data security measures awarded the Education Department an overall grade of D.[8]

Earlier this year, the I.R.S. disabled the FAFSA (Free Application for Federal Student Aid) Data Retrieval Tool on the U.S. Department of Education website until extra security protections could be added.[9] On

---

[3] *See* EdTech Strategies K-12 Cyber Incident Map, https://www.edtechstrategies.com/k-12-cyber-incident-map/ (147 separate incidents were catalogued from January 1, 2016 to June 21, 2017)

[4] *See* Kyra Gurney, Hack attacks highlight vulnerability of Florida schools to cyber crooks, Miami Herald, June 18, 2017, http://www.miamiherald.com/news/local/education/article156544589.html

[5] *See* Increasing Ransomware Attacks in Higher Education, JD Supra, January 18, 2017, http://www.jdsupra.com/legalnews/increasing-ransomware-attacks-in-higher-12045/

[6] United States Government Accountability Office testimony Before the Subcommittee on Regulatory Affairs and Federal Management, Committee on Homeland Security and Governmental Affairs, U.S. Senate and the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, U.S. House of Representatives, November 17, 2015, http://www.gao.gov/assets/680/673678.pdf

[7] Jared Serbu, Government testers easily bypassed Education defenses in recent cyber audit, Federal News Radio, November 18, 2015, http://federalnewsradio.com/cybersecurity/2015/11/government-testers-easily-bypassed-education-defenses-recent-cyber-audit/

[8] Frank Konkel, Nextgov, May 18, 2016, http://www.nextgov.com/cio-briefing/2016/05/fitara-scorecard-fewer-agencies-get-failing-scores/128410/

[9] U.S Department of Education, Update: Internal Revenue Service (IRS) and Federal Student Aid (FSA) Statement on IRS Data Retrieval Tool (DRT), March 30, 2017, https://www.ed.gov/news/press-releases/update-internal-revenue-service-irs-and-federal-student-aid-fsa-statement-irs-data-retrieval-tool-drt

April 5th, the I.R.S. testified that the personal data of as many as 100,000 taxpayers may have been compromised through this tool.[10]

In fact, my family fell victim to the FAFSA hack.[11] In a letter dated April 11th from the I.R.S., my husband learned the agency had "recently identified suspicious activities by individuals obtaining tax data from the I.R.S. through the Department of Education FAFSA application." Six days later, the I.R.S. sent another letter notifying us that someone had "attempted to impersonate" us by filing a joint tax return using our name and social security number. Within days, we discovered that two unauthorized credit card accounts were opened in my husband's name. The I.R.S. has since provided one year of identity theft protection for my husband, but nothing for me or our children.

Unless you have been a victim of identity theft yourself, it's difficult to comprehend how it can take over your life – and how much work it takes to counter such an attack. Among the many lessons I've learned through this experience, the one that is most frustrating is finding out how difficult it is to protect our children's personal information. Requesting a simple credit freeze for a minor child with the three credit reporting agencies is a nerve-racking process which may require parents to submit copies of Social Security Cards or official birth certificates for both the parent and child, and a copy of the parent's driver's license. Expecting parents to willingly *expose* their own and their child's private information after an incident such as this in order to *protect* it, prevents parents like me from taking this somewhat obvious but very challenging step to prevent further identity theft.

Whether at the local, state, or federal level, student records are vulnerable to breaches and hacks in large part because FERPA has no baseline data security requirements for the collection, storage or transfer of personal student data— unlike, for example, personal health data subject to the HIPAA Security Rule. Last year, numerous organizations and privacy experts urged the Education Department to adopt basic security provisions, including encryption, privacy enhancing techniques, and breach notification, without success.[12] Until FERPA is updated to include robust data security protections, unauthorized access to information in education records will continue to place students at risk.

Federal and state collections of student data

While parents generally support the use of research and evidence to drive decision-making in education, policymakers must consider legitimate parental concerns over the use and disclosure of student data stored in statewide longitudinal data systems or SLDSs,[13] and any federal repository of personal student information, for research or other purposes. Parents generally believe education should be in the control

---

[10] *See* Alan Rappeport, Up to 100,000 Taxpayers Compromised in Fafsa Tool Breach, I.R.S. Says, The New York Times, April 6, 2017, https://www.nytimes.com/2017/04/06/us/politics/internal-revenue-service-breach-taxpayer-data.html

[11] *See* Daniel Douglas-Gabriel, Identity thieves may have hacked files of up to 100,000 financial aid applicants, The Washington Post, April 6, 2017, https://www.washingtonpost.com/news/grade-point/wp/2017/04/06/identity-thieves-may-have-hacked-files-of-up-to-100000-financial-aid-applicants/

[12] *See* the Electronic Privacy Information Center's letter to Education Secretary John King, June 6, 2016, https://epic.org/privacy/student/ED-Data-Security-Petition.pdf

[13] For more information, see the U.S. Department of Education's Statewide Longitudinal Data System webpage, https://www2.ed.gov/programs/slds/factsheet.html

of their local community and that a student's data should remain within the school or district for the benefit of the child. When state or federal agencies access identifiable student data without parental consent, many parents perceive this action as government overreach.

Other parents recognize that data collected on individuals, even when limited to certain elements and collected ostensibly for one purpose, could be expanded in scope and subjected to mission-creep, to be used for purposes beyond the original prescribed intent. K-12 student data currently maintained by most states in their SLDS contain upwards of 700 highly sensitive personal data elements, including students' disciplinary records, disabilities, immigration status, and homelessness data. The comprehensive nature of these data sets creates life-long dossiers on individuals, and could quickly become a go-to repository for other state agencies or the federal government. It's not difficult to imagine how this gold mine of data could be repurposed for political or ideological gain, which is one reason that our coalition supports maintaining the Higher Education Act's 2008 ban on the creation of a federal student unit-record system.[14]

A real-life example of the repurposing of education data was recently reported in Great Britain. There, a federal student data repository called the National Pupil Database (NPD) was intended to be maintained "solely for internal departmental use for the analytical, statistical and research purposes." But as Freedom of Information requests revealed, sensitive student information in the NPD had been accessed 39 times by police and the Home Office for various purposes, including to curb "abuse of immigration control."[15] A British advocacy organization, concerned with the rights of the undocumented students launched a national boycott, urging parents and schools to withhold their children's birthplace and nationality data from the government's annual NPD survey for this reason.[16]

The need to update and strengthen FERPA

Enacted more than forty years ago, FERPA became law when students' paper files were held under lock and key in the principal's office, and for the most part, never left the school. We've found that many parents believe this is still the case and are shocked to learn that troves of electronic student data are collected by schools and their contractors, stored online, and digitally disclosed to private companies to develop and deliver educational products and services, and to state and federal agencies for accountability, compliance and research purposes without their consent.

We believe the disconnect for parents stems in part from FERPA's lack of important transparency requirements, or fair information practices, for any company, agency, or organization who accesses student information. At a minimum, parents should be able to know who has their children's data and for what purpose, how it is secured, when it will be destroyed, and how to access and correct inaccurate information. Optimally, parents should be notified in advance of any disclosure of student data to anyone

---

[14] *See* the Parent Coalition for Student Privacy's comments submitted to the Commission for Evidence-Based Policymaking, November 14, 2016, https://www.studentprivacymatters.org/wp-content/uploads/2016/11/letter-to-CEP-w-signers-final-11.14.16-pdf.pdf

[15] *See* Kat Hall, Blighty's National Pupil Database has been used to control immigration, The Register, October 12, 2016, http://www.theregister.co.uk/2016/10/12/national_pupil_database_has_been_used_to_control_immigration/?mt=1476378123415

[16] *See* Against Borders for Children website, https://www.schoolsabc.net/

outside of the school or district and given the opportunity to opt out, and delete any information not necessary to their child's transcript.[17] Perhaps most importantly, robust security protections for the collection, storage and use of personal student data must be required.

Conclusion

FERPA was enacted before computer technology was used in schools, and is long overdue for an update. The law must be modernized to assure students that their personal information will be protected from unauthorized access, and misuse. Until then, our coalition strongly urges policymakers not to enable new or expanded data collections for research or any other purposes.

Thank you again for the opportunity to share our coalition's concerns with you today and for your consideration of my testimony.

[17] For additional recommendations, see the Parent Coalition for Student Privacy's Five Principles to Protect Student Privacy, https://www.studentprivacymatters.org/five-principles-to-protect-study-privacy/