I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Data Collection on School-aged Children through Common Core

STACIE HUNT

INTRODUCTION

In today's digital world, the amount of data collected on individuals is incredible, both in volume and scope. The amount and extent of data collected on minors is equally expansive and is in fact mandated in the current Common Core education standards. Common Core education standards were created by the nation's governors and education commissioners, through their representative organization. The National Governors Association Center for Best Practices and the Council of Chief State School Officers led the development of the Common Core State Standards (CCSS) and continue to lead the initiative.[1] The Common Core State Standards for K-8 exist in English language arts/literacy and math. For grades 9-12 the standards are grouped into bands of 9-10 and 11-12. The educational standards vary per grade level but the overarching theme is that educational standards are the learning goals for what students should know and be able to do at their respective grade level.[2]

The CCSS was developed with funding from the Bill and Melinda Gates Foundation. The CCSS provides a set of standards that are "essential, rigorous, clear and specific, coherent, and internationally benchmarked."[3] The CCSS has come under heavy criticism since its

---

[2] *Frequently Asked Questions*, COMMON CORE STATE STANDARDS INITIATIVE, http://www.corestandards.org/resources/frequently-asked-questions (last visited Feb. 5, 2016).

[3] *Id.*

[4] *Standards-Setting Criteria*, COMMON CORE STATE STANDARDS INITIATIVE, http://www.corestandards.org/assets/Criteria.pdf (last visited Feb. 6, 2015).

inception. Some criticism includes in-test advertising, the elimination of locally appropriate standards, and the emphasis placed on standardized testing.

With the implementation of the CCSS comes an explosion of data mining in schools. Student data is stored in databases designed to follow students from pre-Kindergarten up through their entry into the workforce. The data stored in the longitudinal data systems can be shared with the federal government and other agencies.[4] They can then analyze the data, create recommendations on how to remediate student weaknesses, and then sell that information back to the states and local school districts.[5] Because there has been very little precedent, children do not have very robust privacy protections and there are efforts both at the state and federal level to further weaken these. The Common Core website states that "there is no data collection requirement of states adopting the Common Core State Standards," but the Department of Education's statements prove otherwise.[6] In 2009, Secretary of Education Arne Duncan explained President Obama's vision for the American educational system. Duncan stated that the administration would like to "see more states build comprehensive systems that track students from pre-K through college and then link school data to workforce data. We want to know whether Johnny participated in an early learning program and completed college on time and whether those things have any bearing on his earnings as an adult."[7] The Common Core State Standards and the data systems that contain detailed student information are not distinct; it is nearly impossible for states to implement the Common Core State Standards without agreeing to help create one of the largest data systems in the United States.

While there are federal laws that limit what type of information can be collected on children and how educational records can be

---

[5] *Common Core State Standards a Threat to Personal Liberty—Thomas More Law Center Develops Opt-Out Form for Parents*, THOMAS MORE LAW CENTER, https://www.thomasmore.org/news/common-core-state-standards-threat-personal-liberty-thomas-law-center-develops-opt-form-parents/ (last visited Feb. 6, 2015).

[6] *Id.*

[7] *Frequently Asked Questions*, COMMON CORE STATE STANDARDS INITIATIVE, http://www.corestandards.org/resources/frequently-asked-questions (last visited Feb. 5, 2016).

[8] Arne Duncan, *Robust Data Gives Us the Roadmap to Reform*, U.S. DEPARTMENT OF EDUCATION (June 8, 2009), http://www2.ed.gov/news/speeches/2009/06/06082009.html.

shared, many of these laws are outdated. Although many states have started to write student data privacy protections, privacy experts still think student data lacks adequate protection. In 2014 alone, thirty-six states considered 110 bills on student data privacy.[8] A study released last year by Fordham Law Professor Joel Reidenberg found that only a few schools explicitly restricted the sale or marketing of their students' information in their contracts.[9] The biggest issue comes with third party products, as these products may have very weak privacy policies or none at all.[10] This type of information is enormously valuable to "big data warehouses," who package and resell this information to retailers all around the world for marketing purposes. One example is educational apps. These apps can sell student data to third parties who use information collected in schools to target their advertising.[11]

Chairman of the House Committee on Education and the Workforce, Representative John Kline (R-MN) sent a letter to Duncan raising serious legal questions about the department's efforts to create a national student database.[12] Congress has never authorized the Department of Education to create a national student database and in fact, they have actually done the exact opposite; Congress prohibited the development of a nationwide database of personally identifiable information under the Elementary and Secondary Education Act. The Act barred the "development, implementation or maintenance of a federal database of personally identifiable information…including a unit record system, an education bar-code system or any other system that tracks individual students over time."[13] Contrary to this prohibition, the federal government has created a de facto student

---

[8] *Id.*

[9] Joel Reidenberg et al., *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems*, CLIP REPORT (Fordham Ctr. on Law and Info. Policy), Oct. 28, 2009, http://law.fordham.edu/assets/CLIP/CLIP_Report_Childrens_Privacy_Final.pdf.

[10] Adriene Hill, *A Day in the Life of a Data Mined Kid*, MARKETPLACE (Sept. 14, 2014, 1:20 PM), http://www.marketplace.org/topics/education/learningcurve/day-life-data-mined-kid.

[11] *Paving the Path to Success: Data for Action 2014*, DATA QUALITY CAMPAIGN (Nov. 2014), http://dataqualitycampaign.org/wp-content/uploads/files/DataForAction2014.pdf.

[12] Leo Hohmann, *Education? No, It's about Data-Mining*, WND (May 10, 2014, 5:52 PM), http://www.wnd.com/2014/05/education-no-its-about-data-mining/.

[13] Elementary and Secondary Education Act, Pub. L. No. 89-10 § 9531, 79 Stat. 27 (1965).

national database by attaching very specific data collection requirements to federal education funding. These databases collect and track personally identifiable information from students across the country. Without safeguards to protect this valuable and sensitive information, student data is at risk.

HISTORY OF DATA COLLECTION IN UNITED STATES EDUCATION

Schools have been collecting performance and outcome data on their students for roughly three decades in order to try and improve educational performance. Marc Tucker, President and CEO of the National Center on Education and the Economy, began advocating for a workforce development model of education beginning in the early 1990's.[14] Tucker was advocating for Outcome Based Education (OBE)---an educational model focused on outcomes that students should achieve before progressing on to the next grade level.[15] OBE then morphed into "transformative OBE" which focused on the affective and attitudinal dimensions of learning. The focus on non-academic traits in education has continued in the Common Core national academic standards, which states were incentivized to adopt in 2009.[16] Common Core is the current version of workforce development model of education that Tucker began advocating for in the early 1990's. Tucker served on the development board for the Common Core English Standards and is a known advocate for the national standards; Common Core is essentially a reincarnation of OBE.[17]

United States federal law prohibits the creation of a national student database,[18] but the government has worked around this prohibition by incentivizing states to build databases that are

---

[14] Emmett McGroarty et al., *Cogs in the Machine: Big Data, Common Core, and National Testing*, PIONEER INSTITUTE WHITE PAPER NO. 114, May 2014, at 6, *available at* http://pioneerinstitute.org/download/cogs-in-the-machine-big-data-common-core-and-national-testing.

[15] *Id.* at 7.

[16] *Id.* at 8; American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Title XIV State Fiscal Stabilization Fund, § 14005.

[17] McGroarty, *supra* note 14, at 9.

[18] 20 U.S.C. § 1015C.

identical, and easily shareable. Thus, while the federal government has not explicitly violated the law, it has enabled the states to create a de facto national student database.

The first steps toward a comprehensive student database began in 2002 with the Education Technical Assistance Act.[19] This statute established the Statewide Longitudinal Data System (SLDS). Five hundred and fifteen million dollars was distributed to forty-one states through grants to create state databases for student data.[20] In 2007, Congress enacted the America COMPETES Act (American Creating Opportunities to Meaningfully Promote Excellence in Technology), which allotted grant money to states for the purpose of developing student databases.[21] States were given grant money in exchange for further developing their P-16 systems (Preschool through Baccalaureate degree). Under COMPETES, states were to follow twelve criteria to create identical SLDS to make data available to other states. Schools are essentially required to collect data on their students. The data that is collected includes student success in postsecondary education, student demographics, and the reason why an untested student was not tested.[22]

In 2009, more grants were given through the American Recovery and Reinvestment Act, also known as the Stimulus Bill.[23] This statute created the State Fiscal Stabilization Fund.[24] Grants were taken out of this fund and given to states to expand the requirements for SLDS, requiring states to track students from pre-K through college.[25] The United States Department of Education used $4.35 billion to create the Race to the Top program.[26] This allowed states to gain back taxpayer money in exchange for adopting Common Core as well as

---

[19] McGroarty, *supra* note 14, at 10; Education Technical Assistance Act, Pub. L. No. 107-279 § 208, 116 Stat. 1940 (2002).

[20] McGroarty, *supra* note 14, at 10.

[21] America COMPETES Act, Pub. L. No. 110-69 § 6401, 121 Stat. 572 (2007).

[22] *Id.*

[23] McGroarty, *supra* note 14, at 10; American Recovery and Reinvestment Act § XIV.

[24] McGroarty, *supra* note 14, at 10.

[25] *Id.* at 11.

[26] *Id.* at 12.

expanding its SLDS.[27] The Common Core creators are clear that the success of the standards is dependent on the increased collection of student data.[28] Every state that agreed to the Common Core in order to receive Race to the Top funding also agreed "to design, develop, and implement statewide P–20 [preschool through workforce] longitudinal data systems."[29] Twenty-three states did not receive Race to the Top funding. Many of these states are part of one of the two assessment consortia. These states are also committed to collecting data on their students from preschool through the workforce.[30]

Distributing funding to states in exchange for developing SLDS allows the United States Department of Education to create a de facto national student database in contravention of the statutory prohibition. By encouraging states, through federal grants, the federal government has created identical state databases capable of sharing data. The United States Department of Education expanded Race to the Top requirements through the Early Learning Challenge (ELC).[31] The ELC was a $500 million dollar project authorized by the Stimulus Bill and co-sponsored by the Department of Health and Human Services.[32] ELC was focused on gathering more information on children from birth to third grade. The goal was to increase enrollment of students under the age of five in pre-kindergarten programs. In 2012, the U.S. Department of Labor announced $12 million in grants for states to expand its longitudinal databases linking workforce and education data.[33]

---

[27] *Id.*

[28] *See* Tabitha Grossman et al., *Realizing the Potential: How Governors Can Lead Effective Implementation of the Common Core State Standards*, REPORT (Nat'l Governors Ass'n), Oct. 2011, at 10, *available at* http://www.nga.org/files/live/sites/NGA/files/pdf/1110CCSSIIMPLEMENTATIONGUIDE.PDF.

[29] *Statewide Longitudinal Data Systems*, U.S. DEPARTMENT OF EDUCATION (July 2009), http://www2.ed.gov/programs/slds/factsheet.html.

[30] Race to the Top Fund, 74 Fed. Reg. 221 (Nov. 18, 2009) (to be codified at 34 C.F.R. Subtitle B, Chapter II).

[31] McGroarty, *supra* note 14, at 12.

[32] *Id.*

[33] Jason Kuruvilla, *US Department of Labor Announces More Than $12 Million in Grants Available to States to Improve Workforce Data Quality*, U.S. DEPARTMENT OF LABOR (Feb. 12, 2012) http://www.dol.gov/opa/media/press/eta/eta20120352.htm.

In 2011, the Department of Education unilaterally altered the Family Educational Rights and Privacy Act. [34] The change increased the types of people and who can have access to student data. Any organization or group tangentially involved in the student's education now has access to student data. This change allows for technology groups, textbook, and research companies to have access to this data without parental notification or permission.[35] These alterations diluted privacy restrictions and have made possible student data mining by private contractors.[36] The new rules took effect in January 2012 without congressional approval. The Family Educational Rights and Privacy Act (FERPA) formerly guaranteed that parents could access the data collected by their children's schools about their child, but barred schools from sharing this information to outside sources.[37] The Department of Education has reshaped the Family Educational Rights and Privacy Act. Now, any government or private entity that the Department of Education says is evaluating an education program is granted access to students' personally identifiable information without notifying the child's parents.[38] The changes allow release to third parties of student information for non-academic purposes and broadens the exceptions under which school districts may release student records to non-government entities without consent of the child's parents.[39]

The changes made to FERPA expanded the definition of authorized representative to be almost anyone as long as the data is being released in connection with an audit or evaluation of a federal or

---

[34] Family Educational Rights and Privacy Act, 76 Fed. Reg. 232 (Dec. 2, 2011) (to be codified at 34 C.F.R. Part 99).

[35] John Moran, *FERPA, Recent Changes in Federal Regulations, and State Compliance*, RESEARCH REPORT (Conn. Gen. Assembly Office of Legislative Research), May 6, 2014, at 6, *available at* https://www.cga.ct.gov/2014/rpt/pdf/2014-R-0127.pdf.

[36] Hohmann, *supra* note 12.

[37] *Family Educational Records Privacy Extension Act*, HSLDA (Sept. 21, 2011), http://www.hslda.org/Legislation/National/2011/HR2910/default.asp.

[38] Emmett McGroarty & Jane Robbins, *Controlling Education from the Top: Why Common Core Is Bad for America*, PIONEER INSTITUTE WHITE PAPER NO. 87, May 2012, at 19, *available at* http://pioneerinstitute.org/download/controlling-education-from-the-top/.

[39] *Id.*

state sponsored education program.[40] An authorized representative can then receive a student's personally identifiable information without parental consent.[41] The changes to FERPA also expanded permissible data-sharing in connections with research studies. This allows the disclosure of student Personally Identifiable Information (PII) without parental consent to organizations for research.[42] An example of how broad access to student data can be is when the Washington Department of Public Instruction shared personal student data with the media, including the *Seattle Times* and the *Associated Press*.[43] This information included individual data such as test scores, absences, and discipline information. The school districts defended their decision to release this student data by stating it considered the media sources to be research organizations and were able to give them student's personally identifiable information under FERPA.[44] This is just one example of how relaxed the standards have become to share personally identifiable information on students. Since FERPA no longer provides privacy protections to students and their families, there is no way to predict where a student's information will end up.

The data that is collected by students varies from state to state but also from district to district. Most schools collect basic data such as: emergency contact information, medical information, and home addresses.[45] Now that schools are providing more than education to students, the information they collect has become more valuable and sensitive. Many schools now offer daycare, medical treatment, and psychological treatment.[46] This information is collected by the schools, putting the student's privacy at risk. Many schools monitor and record student behavior, attitudes, as well as their overall demeanor in the school climate. This information may include

---

[40] McGroarty, *supra* note 14, at 24.

[41] *Id.*

[42] Moran, *supra* note 35.

[43] McGroarty, *supra* note 14, at 25.

[44] *Id.* at 14-15.

[45] *Id.*

[46] *Id.*

bullying, drug use, criminal behavior, and sexual activity.[47] Students that do not fit into mainstream classes may be given an Individualized Education Plan (IEP). An IEP lays out the educational plans for a student that is designated as special needs.[48] IEP's include vast amounts of information including psychological information, behavioral information, information on therapy or counseling, medications the student takes, and academic progression.[49] Schools that offer medical services, such as a school nurse or clinic, collect information on treatments and counseling received.[50]

The amount of data that is being collected on students is rapidly growing in scope and scale. It is no longer aggregated information about the school or school district as a whole, but rather as student specific data that can easily be used to identify an individual. This is problematic because, as noted above, the information that is being collected on students is highly sensitive information that can make students very vulnerable to discrimination later in life. Having a child's behavior, medical, or psychological problems collected and stored creates the possibility that this information will follow them well into adulthood.

The Common Core State Standards are assessed yearly through testing by the national test consortia. The two tests are the Partnership for Assessment of Readiness for College and Careers (PARCC) and Smarter Balances Assessment Consortium (SBAC).[51] Both of these tests collect information on student test-takers and fed into the state databases. SBAC has not publicly released a student data privacy policy.[52] PARCC published its data privacy policy which confirms it will collect personally identifiable information on student test-takers, but that information is subject to FERPA. Since FERPA has been gutted, this provides little to no protection for students information. PARCC stated PII "includes but is not limited to the student's name, parents' names, address, date of birth, and mother's

---

[47] *Id.* at 25.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.* at 19.

[52] *Id.*

maiden name."[53] The United States Department of Education will have access to all of the student-level data that is being collected in connection with the national testing.

The data systems are not confined to public school students. In states that require families to submit documentation of intent to homeschool, FERPA does not protect their information.[54] At the National Conference on Student Assessment in 2011, officials from Oklahoma explained to CCSS Officials how they are finding it difficult to meet the data requirements of the federal and state education policies.[55] This challenge is motivating them to "include student groups not now included in the data system."[56] Data collection is not limited to grades on homework assignments, and extracurricular activities.

In February 2013, the Department of Education sponsored a study called Promoting Grit, Tenacity, and Perseverance: Critical Factors for Success in the 21st Century.[57] This study analyzed how to record factors that could affect educational success. Some factors include: socioeconomic background, classroom environment, personal goals, and emotions.[58] This asks public schools to gather information on non-cognitive factors in their students,[59] which can include dispositions, social skills, attitudes, or anything else that is deemed independent of intellectual ability.[60] This information was included in Common Core standards in 2013 and shows a change in teaching not

---

[53] *Id.*

[54] *Family Educational Records Privacy Extension Act*, HSLDA (Sept. 21, 2011), http://www.hslda.org/Legislation/National/2011/HR2910/default.asp.

[55] Sunny Becker et al., *Data, Data Everywhere: Progress, Challenges, and Recommendations for State Data Systems*, CCSSO NCSA CONFERENCE (June 20, 2011), at 13, 27, http://www.hslda.org/commoncore/docs/DataSlide.pdf.

[56] *Id.*

[57] Nicole Shechtman et al., *Promoting Grit, Tenacity and Perseverance: Critical Factors for Success in the 21st Century*, REPORT (U.S. Dep't of Educ. Office of Educ. Tech.), Feb. 2013, http://pgbovine.net/OET-Draft-Grit-Report-2-17-13.pdf.

[58] *Id.* at 35.

[59] *Id.* at 37.

[60] *Id.* at v.

only content but "grit, tenacity, and perseverance."[61] The Department of Education is exploring whether these traits are teachable and malleable by building a psychological profile for each student.[62] The Bill and Melinda Gates Foundation is collaborating with researchers to explore methods of "how specific brain activity is correlated with other cognitive and affective indicators that are practical to measure in school settings."[63] The study recommends new technology to track a student's disposition at school. The new technology they suggested includes: facial expression cameras, pressure computer mice, and computer programs to track a student's mood while at school.[64]

Under the revised version of FERPA, information collected on students can now be shared with third parties; such as education product companies.[65] The Bill and Melinda Gates Foundation donated over $18 million dollars to launch inBloom,[66] a massive database that tracks students. [67] It was pioneered in 2011 with the goal of expansive data use. InBloom was brought about by the Council of Chief State School Officers and "sought to address the problem of data integration."[68] InBloom's goals were to streamline process for teachers and parents and to create personalize learning for parents. But while focusing on these seemingly positive goals, inBloom sought to provide vendors access to sensitive student data so that they could develop and market products for individual students. States such as Colorado, Delaware, Georgia, Illinois, Kentucky, North Carolina, and Massachusetts have agreed to upload data from selected school

---

[61] *Id.* at vii.

[62] *Id.* at 34.

[63] *Id.* at 45.

[64] *Id.* at 44, 69.

[65] Stephanie Simon, *K–12 Student Database Jazzes Tech Startups, Spooks Parents*, REUTERS (Mar. 3, 2013, 7:11 AM), http://www.reuters.com/article/2013/03/03/us-education-database-idUSBRE92204W20130303.

[66] *Awarded Grants*, BILL AND MELINDA GATES FOUNDATION, http://www.gatesfoundation.org/How-We-Work/Quick-Links/Grants-Database#q/k=inbloom.

[67] Jamie Lee, *Common Core-The Business Side of the New Modern Global Education System*, ACTIVIST POST (Jan. 27, 2014), http://www.activistpost.com/2014/01/common-core-business-side-of-new-modern.html.

[68] McGroarty, *supra* note 14, at 34.

districts.[69] Other states, such as Louisiana and New York, have begun uploading almost all of their student records.[70] There was a public outcry from many Civil Liberties Unions over the announcement of student data being given to inBloom. The executive director for the New York Civil Liberties Union condemned the New York school system saying, "Turning massive amounts of personal data about public school students to a private corporation without any public input is profoundly disturbing and irresponsible."[71] The American Civil Liberties Union of Massachusetts had a similar response to the Massachusetts Board of Education.[72] After these complaints, Delaware, Georgia, Louisiana, and Massachusetts said they would no longer be uploading student data to inBloom.[73] Individual school districts in states that were participating in inBloom began to pull out of the database. For example, after the Jefferson County School District (Colorado) announced their decision to not participate in inBloom, the Colorado State Board of Education pulled the entire state out of the database.[74]

In April 2014, after years of criticism and complaints, inBloom closed its doors.[75] The Department of Education is working with replacements for inBloom to take over the data collection of student

---

[69] Lee, *supra* note 67.

[70] *Id.*

[71] Corinne Lestch & Ben Chapman, *New York Parents Furious at Program, inbloom, That Compiles Private Student Information for Companies That Contract with It to Create Teaching Tools*, NEW YORK DAILY NEWS (Mar. 13, 2013), http://www.nydailynews.com/new-york/student-data-compiling-system-outrages-article-1.1287990?pgno=1.

[72] Letter from American Civil Liberties Union of Massachusetts, to Massachusetts Board of Elementary and Secondary Education (Feb. 7, 2013), http://www.commercialfreechildhood.org/sites/default/files/mass_bese_letter.pdf.

[73] Stephanie Simon, *School Database Loses Backers as Parents Balk Over Privacy*, REUTERS (May 29, 2013, 12:51 PM), http://www.reuters.com/article/2013/05/29/us-usa-education-database-idUSBRE94S0YU20130529.

[74] Todd Engdahl, *CDE Cuts Its Ties with inBloom Data Project*, CHALKBEAT COLORADO (Nov. 13, 2013, 6:19 PM), http://co.chalkbeat.org/2013/11/13/cde-cuts-its-ties-with-inbloom-data-project/#.VrfD5vHhHhM.

[75] Benjamin Herold, *inBloom to Shut Down Amid Growing Data-Privacy Concerns*, EDUCATION WEEK (Apr. 21, 2014, 10:33 AM), http://blogs.edweek.org/edweek/DigitalEducation/2014/04/inbloom_to_shut_down_amid_growing_data_privacy_concerns.html.

information from school districts. Regional information centers such as BOCES plan on storing student data to uphold the provisions of states' Race to the Top agreements.[76]

Although inBloom has shut its doors there are still many data projects collecting information on students. Some of these other projects include Workforce Data Quality Initiative, MyData ConnectED, and private companies donating technology.[77] One of the biggest concerns for privacy violations is private company donators. Private companies donate technology such as programs or apps to schools in exchange for access to student information, putting student's personal information at risk.[78] Companies are gaining access to student data by offering free services to schools in exchange for student data. With many schools operating under strict budgets, having free services such as email or word processing may seem like a blessing. Yet these schools are receiving these free products in exchange for violating the privacy of their students. Schools are making troublesome decisions as they enter agreements that virtually sell their students personally identifiable information. An example is providers such as Google, Microsoft, and Yahoo, which all provide services to schools in exchange for student data.[79] These companies use algorithms to collect data on users through emails and web activity. The companies use this data to market products and to target advertising to the specific student user.[80]

Microsoft has been a moving force in Common Core. The Bill and Melinda Gates Foundation is the chief philanthropic donor for Common Core State Standards.[81] The Bill and Melinda Gates Foundation advocates for greater collection and use of student data and encourages sharing of that data.[82] The Bill and Melinda Gates Foundation along with The Michael and Susan Dell Foundation, the

---

[76] Gary Stern, *State Ed Turns to BOCES to Track Student Data*, THE JOURNAL NEWS (Apr. 4, 2014, 10:43 PM), http://www.lohud.com/story/news/education/2014/04/03/state-turns-boces/7278285.

[77] McGroarty, *supra* note 14, at 1.

[78] *Id.*

[79] *Id.* at 38.

[80] *Id.*

[81] *Id.* at 14.

[82] *Id.*

Alliance for Early Success, AT&T, and Target, have been financial contributors to Data Quality Campaign (DQC).[83] The DQC is a data collection initiative that works with the federal and state governments to implement data policies and to report how states are doing in their data collection.[84] DQC recommended ten data points for collection; these recommendations materialized in the Stimulus Bill. States had to agree to collect this information in order to receive grant money under the Stimulus Bill in 2009. DQC had a variety of recommendations but a main takeaway was the movement from aggregate data to student-level information and providing each student with a personal identification number.[85] The student's information is tied to the personal identification number and is then stored individually, not in the aggregate, by school or even school district.

From the beginning, Common Core advocates have argued that data-mining is not a part of the Common Core standards. This is completely false. First, the DQC has acknowledged that "Common Core and robust data collection go hand in hand."[86] Second, states that participate in Common Core tests have already agreed to provide the test creators (PARCC and SBAC) unspecified student level data.[87] Third, the United States Department of Education hosted "Education Datapalooza" at the White House on October 9, 2012 and January 15, 2014.[88] At this event, leaders in education and technology from across the country gathered to discuss Big Data in education. The discussion revolved around how Common Core facilitates Big Data in education the importance of Common Core in their data collection. [89]

---

[83] *Id.* at 17.

[84] *Id.*

[85] *Id.* at 17.

[86] *Id.*

[87] *Id.* at 53.

[88] *Id.*

[89] *Id.*

FORDHAM LAW SCHOOL STUDY

Fordham University Law School's Center on Law and Information Privacy (CLIP), along with Joel R. Reidenberg, Professor of Law and Founding Academic Director of CLIP, published a report in 2009 on K-12 student privacy.[90] The report warned that student data was at risk and that sensitive information was being stored in violation of federal privacy mandates. It further found that information related to teen pregnancies, mental health, family wealth indicators and juvenile crimes were being stored.[91] This type of information may follow the students into adulthood and access to this personal data could occur for decades.[92]

Even before Common Core, states were collecting data on students, and sharing it with the U.S. Education Department. Reidenberg's study focuses on data collection under No Child Left Behind, but the privacy concerns and the nature of the information collected remain the same. Reidenberg found that the majority of databases he examined contained detailed information about each student in non-anonymous student records. The information collected included directory, demographic, disciplinary, academic, health and, family information.[93]

The amount and type of data collected varied from state to state but all the data is collected in individualized form, even if the data is not tied directly to a name.[94] Every state collects at least some information on its students, and most of them provide directory information. This directory information can include "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student."[95] Many states assign a unique identification number to each student to

---

[90] Reidenberg et al., *supra* note 9.

[91] *Id.* at Executive Summary.

[92] Hohmann, *supra* note 12.

[93] Reidenberg et al., *supra* note 9, at 2.

[94] *Id.* at 12.

[95] *Id.* at 25.

identify the student without using their name. Currently, sixteen states collect student Social Security numbers; Georgia and Louisiana, in particular, use students' Social Security numbers as the students' school identification numbers.[96] Many states also collect a wide range of demographic information including: gender, race and ethnicity, immigration status, country of birth, native language, participation in Limited English Proficiency program, and migrant status.[97]

In addition to this personal information, states also collect student academic performance data. Every state collects standardized test scores, while many collect information pertaining to special testing accommodations, tutoring, ACT scores, selection of AP courses, whether a student is considered gifted, whether a student is in special education classes, and post-graduation plans of seniors.[98]

Almost every state collects information pertaining to disciplinary records of students. This includes why a student withdraws from school, (expulsion, jail, illness, mental health, or pregnancy are common descriptors), detailed information about disciplinary actions (such as the reason and date), and student suspensions.[99] States also track economic information related to the student and their families. States collect information on whether or not the student is eligible for free lunch and whether a student is homeless.[100] Finally, states collect health information on their students. Some of the information collected by various states includes Medicaid status; recent medical examination data; health records, such as immunizations; and student weight.[101]

Reidenberg summarized his findings by indicating the percentage of states collecting different types of data on students. Most notably, 32% of states collect student's social security numbers, 22% of states record student pregnancies, 46% of states track student's mental health, illness, and jail sentences, and 72% of states collect student's family wealth indicators.[102]

---

[96] *Id.* at 26.

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.* at 26.

[102] *Id.*

After studying the data collected by states, Reidenberg analyzed the privacy protections in place. He found that the state databases have generally weak privacy protections and that very few states had even thought about privacy concerns.[103] He urged states to create effective protections for the detailed and sensitive information collected.[104] Without privacy protections for student data, a student's personal information about their school experiences and behavior will become an open book. Without proper privacy protections, this data is vulnerable to hacking and misuse. Having this private information exposed leaves children vulnerable and can jeopardize their future as they enter adulthood.

EPIC LAWSUIT

Combined with the changes to FERPA, Common Core is creating a comprehensive tracking of American children. The Electronic Privacy Information Center (EPIC) is an advocacy center that focuses on civil liberty infringements. EPIC has warned that the FERPA revision will expose sensitive non-academic data.[105]

In 2012, EPIC filed a suit against the Department of Education for violating student privacy rights.[106] EPIC alleged that the Department of Education is promoting regulations that undercut student privacy and parental consent.[107] This lawsuit stems out of the changes the Department of Education made in the Family Educational Rights and Privacy Act in 2011. EPIC's lawsuit was ultimately dismissed in the United States District Court for the District of Columbia for lack of standing.[108]

EPIC and other privacy advocates oppose the change to FERPA because of how easily student data can be shared. Privacy advocates

---

[103] *Id.* at 31.

[104] *Id.* at 53.

[105] Valerie Strauss, *Lawsuit Charges Ed Department with Violating Student Privacy Rights*, WASHINGTON POST (Mar. 13, 2013), http://www.washingtonpost.com/blogs/answer-sheet/wp/2013/03/13/lawsuit-charges-ed-department-with-violating-student-privacy-rights/.

[106] Elec. Info. Privacy Ctr. v. U.S. Dep't of Educ., 48 F. Supp. 3d 1 (D.D.C. 2014).

[107] Strauss, *supra* note 105.

[108] Elec. Info. Privacy Ctr. v. U.S. Dep't of Educ., 48 F. Supp. 3d 1 (D.D.C. 2014).

argue that FERPA was revised so that third parties could have easier access to student data by funding student databases.[109] These databases have files from students who are identified by name, address, and sometimes social security number. Information is documented about them such as test scores, attendance, attitude, homework completion, and learning disabilities.[110] Privacy advocates believe this is a serious threat to student privacy. President and CEO of EPIC, Marc Rotenberg states that "once the data gets out there it has all sorts of ramifications. It weakens the [FERPA] structure Congress put in place because Congress understands that a lot of student data can be stigmatizing, keeping people out of jobs, for example."[111]

PII AND PRIVACY SOLUTIONS

PII in student records increases privacy concerns because of the sensitivity of some of this information and its lack of protection. PII includes information such as the student's name; the name of the student's parents or other family members; the student's address; the student's social security number, the student's date of birth, and other information that is linked or linkable to a student that would allow identification of the student with realistic certainty.[112] The release of this information can be harmful to a student, especially when combined with an identifier and the student's educational record.[113] This combination creates the potential for violating a student's right to privacy and could lead to harm or embarrassment for a student. A student may experience adverse effects from exposure of their personally identifiable data. The loss of confidentiality could lead to identify theft, discrimination, or emotional distress.[114]

---

[109] Strauss, *supra* note 105.

[110] *Id.*

[111] *Id.*

[112] Marilyn Seastrom, *Data Stewardship: Managing Personally Identifiable Information in Student Education Records*, SLDS TECHNICAL BRIEF (National Center for Education Statistics), Nov. 2010, at 2, *available at* http://nces.ed.gov/pubs2011/2011602.pdf.

[113] *Id.* at 3.

[114] *Id.* at 7.

Personal identifiable information, because of its sensitivity, demands protection . Administrators and data managers can protect personal identifiable information by developing and maintaining a privacy and data protection program. Personal identifiable information can be categorized by the level of sensitivity.[115] This would help mitigate the risk of disclosure of personal identifiable information. After a risk level is established, more protections and more restrictions can be put in place to safeguard student data.[116] An example of protection for student data would be to store highly sensitive information apart from the rest of the student records. This information would be stored in a secured database with limited access.[117]

To prevent student privacy breaches, a system must be put in place to protect this information. There are many different types of privacy solutions to fix the lack of protection for student information. As a start, states should implement written policies and procedures governing this data. Having written policies and procedures will help safeguard student data. Legislation is needed to protect sensitive personal identifiable information. In 2014, twenty states passed student data privacy bills into law. Although the new laws vary from state to state, the overarching theme is addressing the safeguarding of educational data.[118]

Many of the new laws created a data governance body. These governance bodies have many roles including general education data governance and making decisions about data disclosures, making data transparent and accessible to the public, studying student privacy issues, and addressing the concerns of parents about data use.[119] A data governance body is a great start to student data protection. A governance body with decision-making power can limit the data collected on students. Hopefully, these bodies will be able to curb the collection of highly personal or sensitive information. A governance body can restrict access to student data to authorized users and even

---

[115] *Id.*

[116] *Id.*

[117] *Id.* at 9.

[118] *State Student Data Privacy Legislation: What Happened in 2014, and What Is Next?*, DATA QUALITY CAMPAIGN, http://dataqualitycampaign.org/files/State Student Data Privacy Legislation Resource.pdf.

[119] *Id.*

create a set of rules governing authorized users. This could include prohibiting browsing of student data, not sharing data with unauthorized users, and not leaving data on an unattended computer screen.[120] Furthermore, state data governance bodies could limit the time period in which student data is kept. Student data with personally identifiable information should be deleted after the student graduates or otherwise exits the system. Data, other than student transcripts, needs to be destroyed within a few years of a student's graduation.[121] Following graduation there is little value in the data for research purposes, so in order to protect student privacy as they progress into adulthood the data should be destroyed.[122] The governing body could create rules and procedures on how to destroy student information at the end of the access period.

In order to safeguard student data, more legislation needs to be passed and the current legislation needs to be expanded. Legislation is being presented on the floor in many state legislatures as well as in Congress. As President Obama campaigns for a student privacy law, changes in the United States are imminent.[123] Within the next few years we will see student data privacy protection continue to be discussed and addressed by state legislatures and at the national level.

CONCLUSION

Contrary to the federal prohibition of a national student database, the federal government has enticed states to create SLDS in exchange for funding. The federal government has created identical state databases capable of sharing data which collect and track personally identifiable information from students across the country. With the protections of FERPA gutted by Congress, children no longer have protection over their valuable and sensitive information. Personal identifiable information in student records increases privacy concerns because of the sensitivity of some of this information. Without safeguards to protect this valuable and sensitive information,

---

[120] Seastrom, *supra* note 112, at 11.

[121] Reidenberg et al., *supra* note 9, at 54.

[122] *Id.*

[123] Benjamin Herold, *Federal Student-Data-Privacy Legislation to Be Introduced in U.S. House*, EDUCATION WEEK (Feb. 5, 2015, 3:12 PM), http://blogs.edweek.org/edweek/DigitalEducation/2015/02/student-data-privacy_U.S._house.html.

student's data is at risk. The release of this information could lead to harm or embarrassment for a student.

Currently in the United States House of Representatives, a discussion draft of a proposed overhaul of FERPA is being circulated for feedback. A rewrite of FERPA was released by the bipartisan leadership of the Education & the Workforce Committee. John Kline, (R-MN), is the committee's chair, and Robert "Bobby" Scott, a Democrat from Virginia, is its ranking member.[124] The bill is intended as a potential complement to the pending Student Digital Privacy and Parental Rights Act. The Student Digital Privacy and Parental Rights Act was introduced in the U.S. House of Representatives, in April 2015, by Congressmen Luke Messer (R-IN) and Jared Polis (D-CO).[125]

The Student Digital Privacy and Parental Rights Act bars education technology providers from targeting students with advertising, selling student data to third parties, or creating non-school-related student profiles, as well as requiring them to disclose to schools and the public what kind of information they are collecting and how it will be used.[126] The FERPA re-write includes significant changes. First, the definition of what constitutes a student's educational record would be expanded, and a ban would be placed on using this information for marketing or advertising.[127]

Second, state and local education would be subject to new requirements when contracting with vendors handling student information. The bill would allow fines of up to $500,000 for educational service providers that improperly share student information, and parents would be given new opportunities to access and amend their children's data and opt out of the use of that information for research purposes.[128] Third, parents will be able to opt their children out of some uses of their data. Under the draft, "organizations conducting studies for, or on behalf of, educational

---

[124] Benjamin Herold, *Major FERPA Overhaul Under Consideration in U.S. House*, EDUCATION WEEK (Apr. 7, 2015, 2:27 PM), http://blogs.edweek.org/edweek/DigitalEducation/2015/04/ferpa_overhaul_US_House.html.

[125] Roger Riddell, *Bipartisan Student Data Privacy Bill Introduced in U.S. House*, EDUCATION DIVE (Apr. 29, 2015), http://www.educationdive.com/news/bipartisan-student-data-privacy-bill-introduced-in-us-house/392423/.

[126] *Id.*

[127] Herold, *supra* note 124.

[128] *Id.*

agencies or institutions" would be required to ensure that "parents have been notified of the study and have had a reasonable amount of time to opt out."[129] To prevent student privacy breaches, a system has to be put into place to protect this information. Legislation must be passed at the federal and state level and the changes to FERPA should be reversed to provide privacy protections to student data.

[129] *Id.*