PARENT COALITION FOR STUDENT PRIVACY

Testimony at NYSED Student Forum to develop regulations implementing New York's student data privacy law, Education Law §2-d.

June 12, 2018

Thank you for the opportunity to testify today on the important topic of student privacy.

My name is Leonie Haimson; I'm the Executive Director of Class Size Matters and the co-chair of the Parent Coalition for Student Privacy. The student privacy law passed in March of 2014 was a direct result over the controversy over inBloom, a corporation created with more than $100 million of Gates Foundation funds, explicitly designed to collect a huge amount of student information, including disciplinary and disability data, from at least eight states and districts, including New York state.

The law contained two parts, one blocked inBloom or any other comprehensive student database held by a third party: § 2-c. Release of student information to certain entities [1] The other part contained new legal restrictions on how districts, schools and vendors could collect, use and disclose student data, in § 2-d. Unauthorized release of personally identifiable information. [2]

Yet many provisions of the law have not been enforced or fully implemented, more than four years later and nearly four years past the legal deadline of July 29, 2014. [3]

One of the provisions in the law was that the state would create a Parents Bill of Rights for Data Privacy and Security, explaining all the legal rights of parents to protect their children's education data under state and federal law, as well as other information critical to parents, and to post it on the state website and all district websites. And yet this Bill of Rights as posted by the state is still incomplete, and as explained below, the one posted by the NYC DOE is even more incomplete.

The law also required that the state gain input from parents and other stakeholders to expand and strengthen the provisions in the Parents Bill of Rights, so that it would not just include existing legal rights of parents under

[1] https://www.studentprivacymatters.org/wp-content/uploads/2016/06/NYS-Education-law-Section-2-c-Release-of-student-information-to-certain-entities.pdf

[2] https://www.studentprivacymatters.org/wp-content/uploads/2016/06/NYS-student-privacy-law-section-2-D.pdf

[3] "The chief privacy officer, with input from parents and other education and expert stakeholders, shall develop additional elements of the parents bill of rights for data privacy and security. The commissioner shall promulgate regulations for a comment period whereby parents and other members of the public may submit comments and suggestions to the chief privacy officer to be considered for inclusion. The parents bill of rights for data privacy and security shall be completed within one hundred twenty days after the effective date of this section." See also: https://www.lohud.com/story/news/2014/07/23/states-delay-parents-bill-rights-met-concern/13080301/

federal and state law, but would be broadened and strengthened with input from parents and other stakeholder groups.[4] Hence the need for these hearings.

First, I'd like to explain how the NYC Department of Education currently violates both federal or state student privacy law

For example, the state Education law § 2-d. requires that the current NY state Parents bill of rights for data privacy and security be posted in every district.[5] Yet even now, the NYC DOE does not post this bill of privacy rights but a much abbreviated version. [6]

According to the state law, all contracts or written agreements that districts have with contractors that receive access to personal student information are also supposed to include the NYS Parents bill of rights for data privacy and security as an appendix.[7] Yet many DOE contracts do not include this Bill of Rights and do not even mention the state student privacy law, § 2-d, that was enacted into law in 2014.

Through a Freedom of Information request made in April 2014, shortly after the law was passed, Class Size Matters requested copies of all DOE contracts with vendors that receive personal student information, and yet more than two years later, many of these contracts still have not been provided.[8] After appealing the lack of response, last week we received a contract template dated March 2015, supposed to last for two years, for the 63 CBOs that perform community school "wraparound" counseling, mental health and other services to schools.

These CBOs receive a great deal of confidential student information, according to these agreements, including sexual preference, and other data, including but not limited to the following:

> *"names, addresses, contact information, school, school district, grades or other reviews, scores, analysis or evaluations, records, correspondence, activities or associations, financial information, social security numbers, student identification numbers or other identifying numbers or codes, date of birth or age, gender, religion, sexual preference, national origin, socio-economic status (including free/reduced lunch status), race, ethnicity, special education status, or English Language Learner status." According to the contract, the CBO also has access to "student and family mental health data…."*

And yet there is no mention of the provisions of either NYS Education law any state student privacy law according to this contract template. The only state privacy law mentioned in the agreement is New York

---

[4] "The chief privacy officer, with input from parents and other education and expert stakeholders, shall develop additional elements of the parents bill of rights for data privacy and security. The commissioner shall promulgate regulations for a comment period whereby parents and other members of the public may submit comments and suggestions to the chief privacy officer to be considered for inclusion."

[5] "A parents bill of rights for data privacy and security shall be published on the website of each educational agency…"

[6] http://schools.nyc.gov/NR/rdonlyres/596D9F3C-4938-4DB0-95B7-A0F1D9F44A3B/0/NYCDOEParentBillofRightsforDataPrivacyandSecurityEnglishversion.pdf the State version is posted here: http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/parents-bill-of-rights.pdf

[7] " A parents bill of rights for data privacy and security … shall be included with every contract an educational agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data."

[8] A report just released by the Fordham Law School points out that their similar FOIL request to the NYC DOE on May 6, 2016 for contracts or agreements providing for the release of student data had not either been fully responded to as of February 7, 2018, nearly two years later. Fordham Center on Law and Information Policy, Transparency and the Marketplace for Student Data, June 6, 2018. P. 11, FN 42. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191436

Education Law 3012-c(10), which protects the confidentiality of teacher evaluation data. Nor is the Parents Bill of Privacy Rights included in the contract.

Last week, after our appeal, we also received a DOE non-disclosure agreement for the "School Resource Coordinator", hired by Community Schools to help administer these wrap-around services. The NDA is dated July 1, 2016, more than two years after the NYS student privacy law was passed.

The confidentiality agreement makes clear that The "School Resource Coordinator" also may receive access to a wealth of highly confidential information related to "*students, student families/guardians, DOE employees, agents and/or volunteers obtained by or furnished to me…"* This data may include a wealth of personal data, including the following:

> *"… all findings, analysis, data, reports or other information learned or developed and based thereon, whether in oral, written, graphic, or machine-readable form; and all information marked "confidential." Confidential Information includes, but is not limited to, names, addresses, contact information, school or school attended, school district, grades or other reviews, credits, scores, analysis or evaluations, records, correspondence, activities or associations, financial information, social security numbers or other identifying numbers or codes, date of birth or age, gender, religion, sexual preference, national origin, socio-economic status (but not including free/reduced lunch status, or any other information considered confidential under the School Lunch Act or its implementing regulations), race, ethnicity, special education status, or English Language Learner status; regardless of whether such information was disclosed prior to, concurrent with or subsequent to this Agreement. Confidential information also includes photo-graphs, videos, and any digital or physical images of students, and any other information that qualifies as "personally identifiable information" as defined in 34 C.F.R. Part 99 or as "personally identifying information" in New York Education Law 3012-c(10) [which pertains to teacher evaluation information]."*

Yet as with the CBO agreement, there is no mention of the state student privacy law in this agreement, no Parent Bill of Privacy Rights, and no mention of any of the data security protections required by the state law, including encryption. The only security restriction specified in the agreement is that the coordinator should not post confidential information on the internet, should use passwords, and only transmit the information over "secure networks," without defining that term.

The agreement also states that these CBO employees may gain access to other large comprehensive student databases, maintained by DOE and/or the United Way, with the confidential information of many students other than those attending the school with which they are contracted to work.

While these coordinators are cautioned to not search for and/or access the data about other students, this overarching access may violate FERPA, as schools and districts are supposed to limit disclosure of personal data to contractors with a "need to know" the data of those particular students to fulfill their professional responsibilities. [9]

Several months ago, we also received the DOE contract with Vanguard, via a FOIL request to the NYC Comptroller officer, dated and signed contract Feb. 24, 2016. Vanguard obtains contact information for all current NYC public school students and their parents to carry out mailings for DOE. In violation of FERPA and the state student privacy law, DOE currently allows Vanguard to make student names and addresses available to charter schools for marketing purposes, to send to them copies of promotional flyers and brochures. These disclosures occur without parental consent or opt out, which not only violates FERPA,[10] but also the state privacy

[9] https://nces.ed.gov/pubs97/web/97859.asp

[10] See the FERPA complaint from Johanna Garcia, dated November 6, 2017 https://nycpublicschoolparents.blogspot.com/2017/11/ferpa-complaint-to-us-dept-of-education.html and the follow-up here,

law, NY Education Law § 2-d. , which says personal student data cannot be released or used for "marketing purposes."[11] The Vanguard contract also contains no mention of the state student privacy law and omits the Parents bill of rights for data privacy and security.

All NYC high schools and many other schools throughout the state now schedule students to take the PSAT and the SAT exams during the school day. The US Department of Education recently posted an advisory informing districts that administer college admissions examinations they should be aware that currently, students are asked a series of personal survey questions before taking these exams, asking about their grades, their ethnic and racial background, religion and family income and more. [12]

This personal information is collected by the College Board, which in turn makes the information available to other organizations and companies. Collecting and redisclosing this data without the prior consent of parents, according to the US Dept of Education, violates several federal privacy laws, including FERPA, IDEA (Individuals with Disabilities Education Act) and/or the PPRA (Protection of Pupil Rights Amendment).[13] The US Department of Education also points out that the College Board actually sells this data to third parties, which violates NYS student privacy law, which bars the selling of personal student data.[14]

Many NYC schools are using classroom apps, with click wrap agreements that send personal data of their students directly to vendors, without parents knowing what data is being shared and how it is being used. Though these apps are supposedly free, in many cases the companies are being "paid" with student data, in that the data is used by the vendor for marketing purposes. This too violates the NYS student privacy law.

Our coalition is especially concerned as these lax privacy practices afflict not just New York state, but nationwide.

A new report from Commonsense Media reveals that in their analysis of ed tech classroom apps and services, 38% of the vendors admit in their privacy policies or terms of service that they use child or student personal information for advertising or marketing purposes. Another 30% did not reveal whether they did so or not.[15]

This report is only one of many disturbing studies showing how student data is being widely abused. Researchers at the International Computer Science Institute at the University of California, Berkeley, analyzed Android apps, many of which are also used in classrooms. They concluded that about 57% of these apps potentially violated federal privacy laws and 40% disregarded contractual obligations aimed at protecting children's privacy.[16]

Many schools assign videos on YouTube for students to watch. Yet YouTube, owned by Google, collects user data and uses it for marketing purposes, prompting a complaint to the FTC about YouTube from the Center for

---

in which the DOE falsely claims that they can share student personal with charter schools without parental consent via the "school official" exception to FERPA: https://nycpublicschoolparents.blogspot.com/2017/11/doe-and-success-academy-respond-to.html

[11] "Personally identifiable information maintained by educational agencies, including data provided to third-party contractors and their assignees, shall not be sold or used for marketing purposes."

[12] https://collegereadiness.collegeboard.org/pdf/sat-registration-booklet-students.pdf

[13] https://studentprivacy.ed.gov/admissions-exams

[14] " Personally identifiable information maintained by educational agencies, including data provided to third-party contractors and their assignees, shall not be sold …"

[15] https://www.commonsense.org/education/blog/2018-state-of-edtech-privacy-report-third-party-marketing and https://www.commonsense.org/education/blog/2018-state-of-edtech-privacy-report-third-party-marketing

[16] https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf see also: https://www.theguardian.com/technology/2018/apr/16/child-apps-games-android-us-google-play-store-data-sharing-law-privacy

Commercial Free Childhood, Parent Coalition for Student Privacy, and many other groups, that Google is "profiting off of children without parents' knowledge or consent**.** [17]

Data security is also critical given the increasing number of breaches affecting schools and their vendors.

Most recently, one of the most widely-used education technology companies, Edmodo, had records for over 77 million users, both students and teachers, breached.[18] Another widely used app, Schoolzilla exposed personal data of more than 1.3M students and staff.[19] Many schools and districts across the country are now being hit with ransomware attacks, in which hackers warn they will release personal information of students or staff and/or freeze their data and email systems, unless they are paid thousands of dollars as a bounty. Many of these crimes are committed by a group called the Dark Overlords.[20] NY State itself was hit with a data breach of student information from its testing vendor, Questar in 2018.[21]

A growing number of cybersecurity-related incidents affecting student data, both intentional and unintentional, have been reported in the media since January 2016.[22] And yet among district IT leaders surveyed in 2017, only 15% said they have implemented a cybersecurity plan; and only 19% said they have cybersecurity practices audited by an outside group and only 28% are adding security safeguards to vendor negotiations. [23]

The NY law requires a certain amount of security protections, including encryption. Yet we still have no way of knowing how either the state, NYC or vendors secure the data because either the contracts are not posted, or the contracts don't specify how the data is secured. Even if the contracts do specify strong privacy or security practices, there is little or no enforcement or oversight.

The NY privacy law only specifies that "reasonable methods" be used to secure personal data, and that encryption be required for its transmission and storage, and specifically the methodology required under HIPAA under S13402(H)(2) of Public Law 111-5 be used.[24]

Yet this methodology is not mentioned in the Parents Bill of Rights, and we have no evidence that it's been used or enforced. The law also calls for the Commissioner, in consultation with the chief privacy officer, to "promulgate regulations establishing standards for educational agency data security and privacy policies and shall develop one or more model policies for use by educational agencies." In any case, we urge the state to require industry best practices in securing data, with the methods used by the financial industry, and at minimum those

---

[17] http://www.commercialfreechildhood.org/blog/google-and-youtube-are-invading-childrens-privacy
[18] https://www.edsurge.com/news/2017-05-11-hacker-steals-77-million-edmodo-user-accounts
[19] https://www.edsurge.com/news/2017-04-20-schoolzilla-file-configuration-error-exposes-data-for-more-than-1-3m-students-staff
[20] https://www.csoonline.com/article/3230975/security/dark-overlord-hacks-schools-across-us-texts-threats-against-kids-to-parents.html
[21] http://www.nysed.gov/news/2018/state-education-department-announces-breach-data-held-vendor-questar
[22] https://thejournal.com/articles/2017/06/08/k12-cyber-incidents-have-been-increasing-in-2017.aspx
[23] https://www.edweek.org/ew/articles/2017/11/29/schools-struggle-to-keep-pace-with-hackings.html
[24] Contractors shall "maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody; (5) uses encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5."

outlined by the FBI and the US Department to Education in recent guidance to protect against cyberattacks and ransomware, described in more detail in the appendix below.[25]

There are also serious problems with the State's current version of the Parent Bill of Rights and the way the State Education Department has implemented the state law:

- While it is supposed to list all the rights that parents have to protect their children's privacy under federal and state law, the Parent Bill of Rights posted on the state website omits many of the most important federally protected student privacy rights, including those specified in the *Individuals with Disabilities Education Act* (*IDEA*), National *School Lunch* Act (NSLA), *Children's Online Privacy Protection Act* (*COPPA*), and *Protection of Pupil Rights Amendment* (*PPRA*).[26] Nor does it include the right of every parent to access the personal data that the state itself holds for his or her children, and to challenge it if it is wrong, as required by FERPA and the state privacy law.

- The list of personal data elements currently collected by the state for every student include many elements that are highly sensitive, including students' out-of-school suspensions, their disabilities, whether they are homeless, and their date of entry in the U.S.

- The law requires that the state report on "the legal or regulatory authority outlining the reasons such data elements are collected and the intended uses and disclosure of the data." Yet NYSED never explains the reasons or intended use by the state for the data, and for each element simply claims the "Statutory authority for collection, maintenance and disclosure," as relying on ESEA of 1965, as amended through the ESSA of 2015."[27] However, there is nothing in either ESEA or ESSA that requires that the state collect any personal, individual-level student data from districts, only that it collect aggregate student data by various categories.

We also urge you to require that every district post all written agreements and contracts with vendors or other entities with whom it shares personal data, as do other states, including Connecticut. Otherwise we will never know what companies have received our children's sensitive data and how it is secured.

Need for a NYS stakeholder oversight board:

In 2009. NYSED promised the federal government to create a data stakeholder advisory board in exchange for a $7.8M federal grant.[28] Yet this board was never created.

It is important that a Stakeholder advisory board be appointed, with representation from parent groups, teachers and privacy experts, to provide oversight for which student data is collected by the state and local districts, which data is made available to vendors and other third parties and under what conditions, and ensure that this information is safeguarded from breach and abuse.

---

[25] FBI warning, https://info.publicintelligence.net/FBI-CyberCriminalsSchools.pdf dated 1.31.18 and US Ed Department Guidance, at: https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html, dated 10.16.17

[26] http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/parents-bill-of-rights.pdf For a description of all these rights, see the Parent Toolkit for Student Privacy, posted at bit.ly/ParentToolkitStudentPrivacy

[27] http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/collected-data-elements.pdf

[28] http://nces.ed.gov/programs/slds/pdf/NewYork2009.pdf

I urge the state to adopt, implement and enforce all the formal proposals to strengthen, enhance and regulate the State Student privacy law that we propose below.

Thank you for your time.

Leonie Haimson
Co-Chair, Parent Coalition for Student Privacy
www.studentprivacymatters.org
info@studentprivacymatters.org

Appendix: Parent Coalition for Student Privacy recommendations for NYS:

Transparency:

- Any educational agency, whether the state education department, a district or school, should require written contracts or and/or written agreements with any third parties that gain access to personal student/teacher/principal data, whether they be vendors, researchers or evaluators. [this is implied in the law but not clearly stated]
- These contracts should be posted online as well along with any separate relevant privacy policies or terms of service (TOS) with a link to the site from the Parents Bill of Rights. This is what many other states and districts already do.
- This is already suggested in the NYS student privacy law which says: *"The parents bill of rights for data privacy and security shall include supplemental information for each contract .... where the third party contractor receives student data or teacher or principal data*."

Privacy protections:

- The terms and conditions of these agreements may not be modified unless agreed to before in a written document signed by both parties.
- The contracts should specify all the vendors' subcontractors that will receive data and for what specific purposes and under what conditions they will be obligated to secure the data, with no other redisclosures allowed without the prior written approval of the state/district/school AND the child's parent.
- Clickwrap agreements, where a user consents to a company's terms and conditions by checking a box, should **not** be allowed without careful vetting by the district for strong privacy and security provisions, and compliance with state and federal laws.
- Best practice would be to bar clickwrap agreements at all, since they are generally "freemium", where basic products are "free" and additional services are offered at a "premium", and as widely acknowledged, the school/district is likely paying for the free service with student data. In addition, they would not likely include the NY Parent Bill of Rights and thus do not comply with the state law which requires this for every contract.
- No third party vendor should have access to child's highly sensitive disability, social emotional, or disciplinary data without the consent of the parent.
- The law should cover charter school students as well as public school students; right now this is ambiguous.

No commercial uses

- Right now the state law bars the sale of data or its use for marketing purposes, but doesn't define this sufficiently.
- The regulations should make clear that this includes "de-identified" data, and data about data, known as metadata.
- Neither data nor metadata should be able to be "licensed" for a fee by the vendor, or transferred in an asset sale or merger.
- No student data or metadata should be able to be used to develop new products or services or improve the current ones since this is a commercial use. (Pearson recently experimented on students without their knowledge or consent in their program, claiming doing so for the purpose of "product improvement" was allowable.)
- All rights, including intellectual property rights, shall remain the exclusive property of the district/school/teachers and students, with the vendor only afforded a limited license for the sole purpose of performing its obligations as outlined in this agreement.

Parent Bill of Rights

- The Parent Bill of Rights should reference the right that parents can access and review the actual personal data that the state along with the district and the school has for their child within 45 days of their request, and they cannot be charged for gathering it and only a minimal charge for copying, if necessary. [this is already in FERPA and the NYS law.]
- The Parent Bill of Rights should include reference to and a link to their rights under other federal laws including *Individuals with Disabilities Education Act* (*IDEA*), National *School Lunch* Act (NSLA), *Children's Online Privacy Protection Act* (*COPPA*), and *Protection of Pupil Rights Amendment* (*PPRA*)
- The Parent Bill of Rights needs to include the correct and complete list of student data that the state/district or school collects, along with the rationale for collecting it, as the law references.
- The Parent Bill of Rights should include that parents have the right to opt out of directory information sharing, the types of information that the school/district designates as directory information, and the amount of time the parent has to opt out of this, and how they can do so. [As specified in FERPA.]
- No third party vendor should have access to child's highly sensitive disability, social emotional, or disciplinary data without the consent of the parent. (see above)

Security:

Each district and vendor should use best practices in securing student personal data, given the increased threat and number of cyberattacks, breaches, and ransomware.

- Districts, schools and vendors should be required to implement physical and administrative safeguards that reflect technology best practices and consist with industry standards to protect the data during storage and transmission.
- At a minimum these should include those that the US Department of Education recommends for districts to protect against cyberattacks and breaches:

    - conducting regular security audits to identify weaknesses and update/patch vulnerable systems;
    - ensuring proper audit logs are created and reviewed routinely for suspicious activity;
    - training staff and students on data security best practices and phishing/social engineering awareness; and
    - reviewing all sensitive data to verify that outside access is appropriately limited.

- Vendors should notify the district or school office, and the state Chief Privacy Officer in writing within three days of experiencing any data breach, breach of security, privacy or unauthorized use or access to

the data, including when it occurred and the extent of the access, and what the plans are to remediate the breach.

- Parents of students whose data has been breached or other affected parties should then be notified within 24 hours, by the district or school or state.
- Upon request of the state or district, the state/district/school should be allowed to audit or hire an independent auditor at the vendor's expense to assess the vendor's security and privacy measures in place to ensure the data's protection.
- Vendors should delete the data that it collects or receives under the agreement upon request and/or once the services in the agreement lapses, and allow independent verification of that deletion.
- The vendor shall be liable for any and all damages, costs and attorneys' fees which the state/district/school may incur as a result of any claims, suits and judgements against it that arise out of the acts or omissions of the vendor, its representatives or agencies during the term of the agreement.

Need for Student Data Privacy Stakeholder Advisory Board

- A permanent Data Privacy Stakeholder Advisory Board should be appointed, subject to open meetings law, to oversee the implementation of the state student privacy law and to consider if the amount of personal student data the state is currently collecting is excessive. The board would also provide input into any future changes proposed to the state's collection of data elements. The board will meet regularly and be empowered to hold hearings, if necessary. The board should include representatives from parent groups, privacy experts, educators and others.

- In 2009. NYSED promised the federal government to create a data stakeholder advisory board in exchange for a $7.8M federal grant.[29] Yet this board was never created. It is important for a citizen's advisory board to be appointed, with representation from parent groups, teachers and privacy experts, to provide oversight on which student data is collected by vendors, the state and local districts, and ensure that their personal information is safe from breach and abuse.

[29] http://nces.ed.gov/programs/slds/pdf/NewYork2009.pdf