Report of the Student Data Privacy Task Force Presented to the General Law Committee Connecticut General Assembly

Monday, March 25, 2019

Contents

Introduction

This report addresses issues pertaining to the protection of student data, information, content, and records as governed under Connecticut Public Acts 16-189 (CGS §§ Chap. 170, Sect. 10-234aa – dd), 17-200, and 18-125.

Appointed members of the Task Force gathered in the winter of 2019 to review the concerns that those statutes identify, as articulated in Section 5 of Public Act 18-125. They studied these matters as well as other issues relating to the protection of student data. This report provides a series of recommendations that the task force members have collectively assembled, reflecting their own expertise, research into national best practices and precedents, and the interests of the constituents they represent.

Task Force Members

The following individuals served on the Task Force:

Name	**Organization**	**Appointed By**
Douglas Casey (Chair)	Connecticut Commission for Educational Technology	Speaker of the House
Linnette Attai	PlayWell LLC	House Majority Leader
Ben FrazziniKendrick	Locke Lord LLP	Senate President Pro Tempore
Jody Goeler	Hamden Public Schools	Senate Minority Leader
Ajit Gopalakrishnan	Connecticut State Department of Education	Connecticut State Department of Education
Michele Lucan	Office of the Attorney General	Office of the Attorney General
Glenn Lungarini	Connecticut Association of Schools	Connecticut Association of Schools
Teresa Merisotis	American Federation of Teachers	Senate Majority Leader
Shonna Mitchell	Connecticut Parent Teacher Association	Senate Majority Leader
Michael Purcaro	Connecticut Association of Boards of Education	House Minority Leader
Daniel Salazar	Novus Insight	House Majority Leader

Executive Summary

This report results from the careful study and consideration of student privacy in Connecticut, leveraging the deep expertise of the task force members. The group believes that schools, parents, and educational technology providers can strike a healthy balance between protecting student privacy and leveraging the promise of innovative instructional products to the benefit of all learners. The following points summarize the report's recommendations, with details in the sections that follow:

- Reduce Inefficiencies While Ensuring Privacy: Throughout the report, the task force acknowledges the importance of protecting student privacy in ways that also minimize impact on the limited resources of districts, especially small ones.
- Strengthen Penalties: Define and reference measures that compel vendors to comply with the law, pointing to existing state statute, when possible.
- Leverage and Ensure Coherence Across Statutes: Connecticut's data privacy law does not require additional definitions regarding requests for data deletion or public hearings, which federal statute, Connecticut education law, and local board of education policies already address. Furthermore, new state education and general privacy statutes should align with the current and future revisions to the Connecticut student data privacy law.
- Training and Professional Development: Provision of high-quality training materials by the state will minimize the need for districts to do so individually. A centralized solution would also help address the critical need to strengthen digital literacy competencies among all members of the educational community without placing additional resource burdens on districts.
- Further Study: A formal study to measure the qualitative and quantitative impacts of the law would help identify the collective direct and indirect costs on Connecticut's school districts.

Recommendations

Connecticut statute charges the task force with addressing eight topics concerning the law and operational practices to comply with it. The statute also calls on the group to address "any other issue involving student data security that the task force deems relevant."

Since the passage of that original statute, Connecticut schools have made concerted efforts to comply with the law at substantial direct and indirect cost. Subsequent revisions to the law, as well as resources developed by the Connecticut Commission for Educational Technology, have addressed some of those original topics.

Given this context — the passage of time and establishment of practice to support the statute — the following sections address all of the original concerns as well as other topics that have emerged from the educational community. Note that the language of each topic listed under "Concerns Stipulated by Connecticut Statute" come directly from those laws (PA 16-189, PA 17-200, and PA 18-125).

Concerns Stipulated by Connecticut Statute

Topic 1: When a parent or guardian of a student may reasonably or appropriately request the deletion of student information, student records or student-generated content that is in the possession of a contractor or operator

Recommendations

The task force members acknowledge and embrace parent concerns over the protection of student data. At the same time, the law needs to ensure the integrity of education records.

Parents can access and request amendments to student records following procedures in place under the Family Educational Rights and Privacy Act (FERPA), codified at 20 U.S.C. § 1232g, with implementing regulations at 34 CFR Part 99. Districts that leverage third-party services that collect and store student data should respond in a timely manner to parents and guardians, following the protocols of FERPA.

Broad deletion of records maintained for the district by a technology provider can violate state records retention laws, compromise the wholeness of the education record, or place a burden on districts by having to maintain parallel systems (online and offline). Districts leverage third parties to assist with all aspects of school operations and instruction, from student information systems to food services and transportation, assessment to academic interventions.

Providing greater clarity over deletion rights will help minimize unintended outcomes and indirect costs on the district. For example, deletion rights should permit removal of extraneous, unnecessary data, but not allow parents to delete graded assignments and tests in order to favor the overall academic record of their children. To minimize the possibility of these types of scenarios, the group recommends the addition of language regarding the conditions under which schools and parents should consider removal of student records. Doing so should only take place in consultation with the school district, in alignment with FERPA, and to the extent that doing so preserves the wholeness of the educational record.

Topic 2: The means of providing notice to parents and guardians of students when a student uses an Internet web site, online service or mobile application of an operator for instructional purposes in a classroom or as part of an assignment by a teacher

Recommendations

The group has no further guidance to offer on this topic. Public Act 18-125, Section (g)(1) changed the notification mandate for districts. Instead of requiring electronic notifications for each new or renewed contract (i.e., software package in use), it

allowed for an annual electronic notification (e-mail) sent to parents and directing them to a district Web page with details on the contracts, data shared, etc.

Topic 3: Reasonable penalties for violations of the provisions of sections 10-234bb to 10-234dd, inclusive, of the general statutes, as amended by this act, such as restricting a contractor or operator from accessing or collecting student information, student records or student-generated content

Recommendations

The current statute has no other penalty for noncompliance except for the voiding of contracts. While perhaps intended as an incentive for contractors to bring their terms into compliance, it generally places a burden on districts. They have assumed significant indirect (contract negotiations) as well as direct (e.g., external legal fees) costs. The current statute also leaves other requirements of the law, such as those in Sections 10-234cc – dd, without any enforcement framework. The task force recommends several classes of penalties, defined below.

Vendor Contracting Penalties

Regarding contracts that do not comply with the requirements of Connecticut law, the task force recommends allowing vendors a "cure period" after which the contract is void [see, for example, California Educ. Code § 49073.1(c)]. The resulting penalty against the vendor could include non-payment of remaining license or usage fees by the district and other consequences of a voided contract. This approach would afford vendors a reasonable amount of time — the task force recommends 30 days — to address and resolve such contract non-compliance.

Vendor Practice Penalties

Providers that do not comply with Connecticut statute (e.g., failing to maintain reasonable security practices or engaging in targeted advertising) should be subject to existing, relevant penalties for "willful violations" of the Connecticut Unfair Trade Practices Act (CUTPA). *See* Conn. Gen. Stat. § 42-110o as well as Conn. Gen. Stat. § 36a-701b(g) (e.g., failure to comply with breach notification constitutes an unfair trade practice). These would include damages, aligned with CUTPA, such as State action as well as private right of action for boards to take in situations where a contractor fails to negotiate the contractual terms required by Conn. Gen. Stat. §§ 10-234bb(a)(1) through (a)(10) in good faith. *See also* Conn. Gen. Stat. §§ 42-110b and 42-110g. Non-compliance with aspects of that law, including contract requirements, can result in applicable financial penalties under state law.

The State could also penalize vendors for non-compliance by banning them from collecting and storing student data for a defined, meaningful time period. This practice is similar to those defined under FERPA. *See* 34 CFR § 99.67(c). Companies should align their terms and practices with the requirements of Connecticut state law.

School District Penalties
In a scenario where a district does not post the use of compliant educational software as required by Conn. Gen. Stat. § 10-234bb(g), the district should acknowledge and resolve the issue in a reasonable amount of time.

In situations where a district willfully uses non-compliant software, state law already provides methods to address alleged failures of local and regional boards of education to comply with the law. *See* Conn. Gen. Stat. § 10-4b; Regs. Conn. State Agencies § 10-4b-1 *et seq*. Further, FERPA provides parents with means to address improper data sharing by local and regional boards of education. *See* 34 CFR §§ 99.10; 99.20 through 99.22; 99.30 through 99.39; and 99.63 through 99.67.

Topic 4: Strategies in effect in other states that ensure that school employees, contractors and operators are trained in data security handling, compliance and best practices

Recommendations
In Connecticut, some districts already provide their teachers and staff with professional development around data privacy and security. Creating a common store of training materials — developed or curated at the state level — would help ensure high quality and consistency of messaging while relieving the burden on each town of developing these resources. The task force members felt strongly that students, teachers, and the broader educational community need support in understanding best practices in data protections. This training should align with and leverage other frameworks and practices, such as the ISTE digital learning standards, adopted by the State Board of Education (2018) and Commission for Educational Technology (2016).

Some other states have created entire departments to produce materials and deliver training to staff, students, parents, and contractors. Utah's State Board of Education, for example, has a staff of six personnel who develop engaging and highly informative videos, Webinars, and presentations that address a broad range of privacy topics concerning state and federal law. *See* https://schools.utah.gov/studentdataprivacy for more information. In Utah, state law (2017 SB 102) also requires that districts create a list of employees who can access student data, then provide such employees with privacy training.

North Dakota statute (SB 2326 – 2015) requires annual training for any district or state employee with access to its state longitudinal data system. Colorado HB 1294 (2014) requires the state board to develop an education data security plan that includes staff training. Taking a more holistic approach, Virginia's HB 2350 (2015) requires the State Department of Education and the Virginia Information Technologies Agency to develop a model data security plan for districts to implement policies and procedures related to the protection of student data and data systems. It also requires the Department of Education to designate a chief data security officer to assist local school divisions with the development or implementation of policies around data security and data use.

Topic 5: The feasibility of developing a school district–wide list of approved Internet Web sites, online services and mobile applications

Recommendations

Even before the passage of PA 16-189, which requires the creation and posting of district-wide educational software, some schools had already established protocols for vetting and implementing such products. These conventions varied from district to district, with some centralizing the procurement of educational products and others taking a more distributed approach, allowing for adoption at the school or classroom level. The law requires districts to adopt a more centralized process, which has slowed the adoption of software that benefits students while imposing more indirect costs on staff in the form of internal and external vetting and negotiations, as well as administrative time to post and maintain centralized lists of apps, contract dates, etc.

With regard to the "feasibility" of these activities, the task force members have seen widespread and serious efforts to comply with the collection and reporting of information about educational technology use. Most districts have created separate Web pages or sections that list these products. Examples include the contract pages from Stamford Public Schools as well as the Google Sheet solutions of South Windsor Public Schools (http://bit.ly/2IAQVx2) and Manchester Public Schools (http://bit.ly/2T0ABL1). Rapidly creating such inventories has resulted in an additional burden on districts, contributing to an estimated 80,000 additional staff hours annually, with no additional resources, based on survey responses from district leaders (2017 Commission for Educational Technology survey). A precise response to the question of feasibility and impact would require a more formal study (see recommendation for a full impact assessment, Topic 12, below).

Topic 6: The use of an administrative hearing process designed to provide legal recourse to students and parents and guardians of students aggrieved by any violation of sections 10-234bb to 10-234dd, inclusive, of the general statutes, as amended by this act

Recommendations

The law governing student data privacy requires no additions or modifications to address the use of administrative hearings. As task force members — representing the highest levels of school district and municipal leadership as well as school law attorneys — noted, parents and board members widely understand and exercise the existing ability to conduct administrative hearings concerning grievances, disciplinary issues, and other matters (e.g., proof of residency).

FERPA already provides for a hearing process for parents and eligible students to "challenge the content of student's education records on the grounds that the information contained in the education records is inaccurate, misleading, or in violation

of the privacy rights of the student" (34 CFR § 99.12). It also provides for a complaint process through the U.S. Department of Education (34 CFR § 99.63). Defining or endorsing a separate type of administrative hearing would not change how parents currently raise and escalate such concerns with district administrative teams.

Topic 7: The feasibility of creating an inventory of student information, student records and student-generated content currently collected pursuant to state and federal law

Recommendations

As with Topic 5, above, districts have largely responded to this requirement of the law. Regarding the inventory of student information, records, and content, schools have taken different approaches. Some have established specific approval workflows that assess the instructional benefit to and data shared through educational software. Some automation tools, such as those available free through the Commission's Educational Technology Software Hub, allow districts to monitor real-time access to instructional apps.

Topic 8: The feasibility of developing a tool kit for use by local and regional boards of education to (A) improve student data contracting practices and compliance, including a state-wide template for use by districts, (B) increase school employee awareness of student data security best practices, including model training components, (C) develop district-wide lists of approved software applications and Internet web sites, and (D) increase the availability and accessibility of information on student data privacy for parents and guardians of students and educators

Recommendations

A number of resources now exist to address the concerns listed in this topic. Two months after the passage of PA 16-189, the Commission for Educational Technology developed a Student Data Privacy Toolkit and hosted a briefing (June 27, 2016) to explain the law and Toolkit. The document, with revisions and additions since its first publication, includes background on state and federal laws, contracting resources such as sample agreement language, communication templates, staff training resources, and guidance on establishing a district privacy and security program.

As one of its strategic initiatives, the Commission for Educational Technology has partnered with the Consortium for School Networking (CoSN) to launch a cohort of districts pursuing the Trusted Learning Environment (TLE) credential. The TLE framework provides free resources and a national peer network for districts to address the leadership, business, security, training, and classroom aspects of data privacy. In addition to the Commission's work, the State Department of Education hosted a half-

day conference September 8, 2016 to address student privacy. The agency provides a Web page with links to resources concerning federal privacy laws.

The launch in 2017 of the Commission's Educational Technology Hub provides a free and open platform for contractors to share contract terms that they have attested as compliant with Connecticut law. The Commission has also worked directly with a number of prominent, widely-used software companies to help ensure their compliance with state statute. More recently, Public Act 18-125 required the Commission to create a Model Terms of Service Addendum to assist districts and contractors with developing compliant terms for contracts. The Commission completed and published the Addendum in June 2018. In addition to these steps, districts across the state have developed and published lists of software in use, with the requisite contract and data-usage details posted as well. See Topics 5 and 7. All of these activities have come with significant direct and indirect costs, without additional state resources.

With the above steps as context, the task force reiterates its recommendations in Topic 4 to develop statewide resources for training staff and parents on data privacy best practices. Doing so would reduce the burden on districts to create these materials independently and help ensure consistency, accuracy, and high quality.

Other Concerns Raised by the Task Force

The task force recommends that the General Assembly consider the following, additional topics. These recommendations reflect the concerns of the task force members as well as the groups they represent, including Connecticut students, educators, school leaders, parents, and school law experts.

Topic 9: The requirement for each contractor and district to establish compliant terms and conditions, especially for the use of educational software, remains highly inefficient and costly while leading to wide differences in contract language

Recommendations

To streamline the contracting process, define the term "Contract" to include all forms executed in accordance with Connecticut law, including electronic agreements. Doing so would obviate the need for districts to request separate contracts from vendors if standard online terms already meet the requirements of Connecticut's student privacy law. Use of terms that acknowledge Connecticut's statutes as governing the agreement would also provide accountability by contractors. *See* Topic 3 concerning penalties, above. Connecting their agreements to existing State consumer protection laws would help hold them accountable to all aspects of CGS §§ 10-234aa – dd.

In addition, task force members recommend that when a state agency or office acquires software on behalf of one or more local education agencies, and the terms of the agreement governing that acquisition align with the requirements of state statute, that districts may use these software resources without having to execute separate agreements. An example of such a scenario is that, when the Connecticut State Library purchases licenses to EBSCO and other subscription services, use of this educational software by districts should not require them to enter into separate agreements with the same vendors. In such instances, the original agreement would anticipate use by districts and otherwise comply with statutory requirements.

Topic 10: A number of key terms within the law have no clear definitions, making it difficult for districts and contractors to identify and meet measures of compliance

Recommendations

Having put the requirements of Connecticut's statutes into practice, district leaders, vendor representatives, and school law attorneys have called for definitions to terms used in the law to clarify their meaning. The task force recommends doing so with the following:

- Written Contract: The task force recommends changing the term "written contract" simply to "contract."
- Student Data Sources and Accounts: Address ways to handle instances where data is co-mingled between personal and school accounts.
- Personally Identifiable: Many districts take a broad view of this term, making the law apply to even non-personal information, whereas others define it more narrowly, thus seeing the law as not applying to many use cases.
- Educational Software: Consider a clearer definition of educational products, rather than simply those sold to schools. Many other state laws specifically exempt products not designed and marketed primarily for K – 12 use.
- Standardized Assessment: Current Connecticut statute [CGS §§ 10-234aa(6)] exempts "student responses to standardized assessments." Schools have interpreted "standardized assessment" broadly to mean any test administered to students as well as narrowly, to cover only the Smarter Balanced and SAT exams. Districts would benefit from further definition in general terms.

Topic 11: The law could define separate protections for directory information

Recommendations

The current law acknowledges the different levels of sensitivity of student data. See, for example, the different breach notification windows for directory and non-directory information [CGS §§ 10-234dd(a) and (b)]. FERPA currently permits the release of directory-level information. *See* 34 CFR §§ 99.3 and 99.37. Connecticut statute might at some point exempt directory-level information to align with commonly accepted

standards of harm, though the task force does not recommend making such a revision at this point.

Topic 12: The State needs a quantitative assessment of the law's impact on boards

Recommendations

A study should take place to measure the direct and indirect costs to boards of education of the data privacy acts, especially with a concern for equity of access. The Commission conducted an informal survey in 2017, for example, that estimates 80,000 staff hours spent statewide per year to conduct additional contract review and negotiations to comply with the law. A more formal study would look at the impact of the statute across all districts, measuring internal staff time as well as costs for external services, such as those provided by third-party legal counsel. The law may pose burdens especially on smaller districts with limited staff and financial resources to comply with the statute.

The results of the study would inform future changes to the law and possible appropriations to offset the costs of compliance.

Topic 13: The law only addresses protection of the data of public school students

Recommendations

Consider extending the law to address the protection of data for all students in the state, not just those enrolled in public institutions. The revised statute would include protections over the data of students in private and parochial schools as well as those enrolled in public districts.

Topic 14: Having different breach notification windows remains confusing to districts and contractors

Recommendations

Consider making all external (operator and contractor) breach notification periods 30 days. Having a single notification window would simplify the tracking of such incidents.

Topic 15: The requirement that districts publicly post contract language can compromise sensitive information

Recommendations

Modify the language to allow for redactions in contracts to protect sensitive, confidential information that is not otherwise material to data privacy requirements, the disclosure of which could compromise the privacy of students.