CEA
Advocating for teachers
and public education

Connecticut Education Association

Governance
Sheila Cohen, President
Jeff Leake, Vice President
Pat Jordan, Secretary
Thomas Nicholas, Treasurer
John Horrigan, NEA Director
Gary Peluchette, NEA Director

Executive Office
Mark Waxenberg
Executive Director

Policy, Research & Reform
Donald E. Williams, Jr. Director
Capitol Place, Suite 500
21 Oak Street
Hartford, CT 06106
860-525-5641 800-842-4316
Fax 860-725-6323

An affiliate of the
National Education Association

Testimony of

Ray Rossomando

Connecticut Education Association

Before the Education Committee

HB5469 AAC STUDENT DATA PRIVACY

March 2, 2016

Good afternoon Senator Slossberg, Representative Fleischmann, and members of the Education Committee. My name is Ray Rossomando, Research and Policy Specialist with the Connecticut Education Association. CEA helps the 43,000 active and retired teachers across the state to have a greater voice in the decisions that affect students, classrooms, and the teaching profession.

I am testifying today on HB 5469 regarding student data privacy in partnership with the CT Alliance for Privacy in Education (CAPE). CEA does not support this bill in its current form.

CEA thanks committee members for raising such an important issue in this short session. We are pleased to see in this bill language that builds upon the work begun in 2015. Protections for students against their tracking and profiling, as well as the prohibition against using personally identifiable information (PII) to target advertising to school children are commendable provisions. We are also pleased to see requirements for parental notification of student data disclosures to data storage contractors.

However, as many other states have shown, there are more comprehensive and even simple, common-sense provisions that could be included that could make the work of this committee among the best in the nation. As the National Conference of State Legislatures recently pointed out, and consistent with CEA's and CAPE's advocacy, the key is balancing the legitimate collection of student PII for use in classrooms with the thirsty demand for data by entities beyond the schoolhouse doors.

Three circumstances have resulted in so many states taking action in this policy arena:

1) Unprecedented ability to transfer Personally Identifiable Information (PII) in a click of a mouse
2) Obliteration of federal data privacy (FERPA) protections, which deleted parental consent
3) Data is the new way to mine for gold – and everyone wants more of yours.

In this new climate, data sharing has become the Wild West. Local contracts differ from district to district and state to state. Awareness of dangers remains little known and understood. Well intentioned people may be making irreversible unintended mistakes. And the situation is ripe for ill-intentioned individuals to exploit vulnerabilities in data security, especially in our schools.

Attached to my testimony is a checklist of provisions that address these concerns and provide options for the committee members' consideration. These provisions, which have been pulled from other states' laws and model legislation, have been categorized by CAPE into five topics. CEA is supportive of all of these provisions, but will focus on two topics in this testimony: "Third Party Contracts" and "Data Protection, Training, and Oversight."

Third Party Contracts

Ultimately, all stakeholders should think about student information in much the same way that we've come to understand our personal medical information. Like HIPPA, state policies should always err to the side of protecting students' information as opposed to enabling its dissemination. Like HIPPA, student PII should have protections that attach to the data elements no matter where, or to whom, they are sent. And like HIPPA, any third-party that contracts to receive student PII must document that it maintains industry-standard data security controls (such as the "Service Organization Control" or SOC Reports – see KPMG White Paper provided upon request) and state of the art encryption technologies.

As it stands, HB5469 defines "Contractors" in a very limited way as data storage providers. This is a loophole that will not prevent egregious violations of trust or inadvertent releases of student PII. Recent circumstances already make this loophole concerning.

For example, through a recent FOI request, members of CAPE learned that sensitive special education data on individual students were released to an organization that contracted with a school district to provide free services. The information that was shared with this entity met

two conditions of PII under FERPA – it included student identification numbers and other information – specific disability and hours of service – that in combination could make identification of individual students very possible.

The entity might claim that it was dubbed a "school official" and therefore qualify for an exemption under the gutted FERPA regulations. Even if that were the case, the situation raises a couple key concerns for Connecticut lawmakers:

- Why were parents not made aware that their children's information was being emailed to a third party? Shouldn't they have had the right to consent?
- Why aren't the third parties and subcontractors required to demonstrate that they have met security standards or have conducted background checks?
- Why is there no state law that requires contracts that involve student information to meet certain uniform standards?

Furthermore, this entity partnered with another third party, who could have also accessed sensitive student information without the knowledge of school officials, board members, or parents. We can prevent this from happening again.

The definition of contractor in HB5469 would not prevent this from happening again and severely limits the reach of any protections included in the bill. Instead, we recommend defining contractors to include any entity that enters into an agreement with a board of education that involves student PII. As a result, any protections for students, rights for parents, and transparency for oversight that is included in the final bill will extend to all third parties.

HB5469 should also be revised to specifically require contracts involving student data to include specific language on transparency, security, data sharing and destruction, breach notification, and other protective provisions (see attached). Additionally, entities entering into a contract with a board of education that involves student PII should register with the state and submit documentation that data security standards are in place and that background checks have been completed. This could be done in a cost-neutral manner that also provides school districts with accountability for third parties and the public greater peace of mind.

Data Protection, Training, and Oversight

While it is important to establish standards for sharing data with third parties, a good deal of data is vulnerable to disclosure even without contracts. This occurs through daily classroom and school activities. For example, FERPA permits the sharing of PII that is considered "directory information." However, what is defined as directory information is largely left to school districts and the definitions vary considerably. To prevent "oversharing," state law

should define directory information statewide as name, address, telephone#, and email. This is the standard used in some districts already; it should apply to all.

Additionally, every year, parents receive a FERPA form discussing directory information. This form also varies by districts and some parents have reported such forms being combined with PTO sign-ups, confusing matters for parents. This form should be uniform across the state, solely address student data privacy, and be used to inform parents of other key laws and data collection efforts such as the state's longitudinal data system collection.

Awareness and engagement are important ingredients in securing data and enabling them to be used for the most appropriate purposes. CEA recommends the creation of local and state oversight boards comprised of parents, educators, and board members. We recommend the creation of model data security plans that can be used by school districts, as was done recently in Virginia. We also advocate the development of guidelines that educators and other school personnel can use to learn about safe and secure data handling strategies. And to further ensure proper handling of data by state agencies and third parties, CEA urges committee members to require appropriate auditing measures (such as those noted above in the SOC report).

At the same time that significant student PII is being collected and shared, data collection on educators is also rampant. The explosion in data on educators, which is sometimes linked to students and classrooms, has concerning potential for abuse and misuse that can be detrimental to the learning environment. New York law extends many of the same notification and protection standards applied to student data to educator data. Connecticut should consider this too. This is a sensible provision that protects the sanctity of the classroom and the school climate.

As committee members consider legislation securing the privacy of educational records, we urge you to be comprehensive. You have a role to step in where the federal government has recently dug a hole. It's a heavy lift, but not an impossible one.

Like the provisions that we and other states have highlighted, engagement of parents, educators, and experts is a key ingredient in addressing this issue. CEA and the members of CAPE have been working to provide you with viable options and will continue to do so. We hope members of the committee will reach out to our groups and continue to invite input and assistance. We stand ready to lend a hand.

Thank you.

Student Data Privacy Bill Checklist CAPE4Kids.org	
Scoring Code *In Bill* *Not In Bill* *In bill, but needs improvement* *Should not be in bill*	 ✓ ✗ ▼ 👎
Student Electronic Devices, Apps, and Online Services	**HB5469**
Protections from unreasonable search and seizure of personal electronic devices	✗
Prohibit student tracking and profiling	✓
Prohibit remotely accessible webcams on school issued devices	✗
Ensure password privacy on student devices	✗
Ensure security of school issued passwords	✗
Limit data collection by school-contracted apps and websites used by schools.	✓
Incorporate COPPA into state law for students up to age 18.	✗
Limit online advertising	✓
Require de-identification of student information for use to improve site or product	✓
Parental & Educator Notification, Engagement, and Transparency	**HB5469**
Uniform FERPA and SLDS notice to all parents when school year begins	✗
Parental notification of student data disclosures to third parties or contractors in local board of education contracts	✓
Parental consent of student data disclosures to third parties (formerly in FERPA)	✗
Parental notification of state agency contract involving student data	✗
Parental inspecting, correcting, and removing data held/shared by schools (HB5469 Only covers "Operators" - parental rights should apply to all contracts)	▼
Limit the sharing of sensitive personal and family information and strengthen protections of student medical data	✗
Require posting of state and local data collection, sharing, and related contracts	✗
Increase parent representation on P20 and other state and local data oversight boards	✗
Educator notification and consent of data disclosures to contractors or other third parties	✗

Student Data Protection, Training, and Oversight	HB5469
Define uniform "directory information" solely as name, tel#, address, and email; ban intrusive data elements (e.g. biometric data)	✗
Prohibit sharing of PII w/ certain research exceptions (HB5469 permits collection of PII by "operators" and is weak on redisclosure; rules should follow data like in HIPPA)	▼
Ban digital advertising on school required devices, apps, sites, online textbooks, etc. (HB5649 is unclear, see sec. 1(10)C)	▼
Establish local student data advisory boards consisting of parents, educators, and board members	✗
Require BoE to provide school employee data handling awareness info	✗
Require up-to-date encryption tools (HB5469 "industry standard" - could be more specific)	▼
Require independent audits of public agency and third party data handling	✗
Ensure bill covers students covered under FERPA (prek-12; college)	✗
Student Data and Third Party Contracts	HB5469
Defines contractor only as a data storage software/service (Severly limits reach of bill)	👎
Defines "Operator" as a person, not an entity or business as used under "contractor"	👎
Require data contractors to register with the state and document data security system compliance	✗
Establish uniform basic student data security contract and cloud provisions linked to specific industry security guidelines or body (HB5469 references less specific "industry standard")	▼
Require victim notification of data breaches	✓
Establish penalties/fines/rights of action for breach/violations of data protocols	✗
Clarify and strengthen "authorized representatives" and "legitimate educational interests" that permit data sharing under FERPA	✗
Background checks for contractor employees who handle student data	✗
Require contracts to imdemnify the state and hold contractors accountable	✗
Allow online operators to collect and redisclose PII to subcontracted entities (lines 161-167)	👎
Establish enforcement mechanism, such as AG student data privacy enforcement	✗
State Data Collection and Compiling	HB5469
State Chief Privacy Officer and Citizens Advisory Board	✗
Legislative authorization for all student data elements (i.e. inter-agency sharing)	✗
Transparency SLDS collection and purpose; Consider SLDS moratorium on expansion	✗
Ban SLDS from being used for employability, criminal/civil liability, financial standing, or reputation of the student	✗
Ban collection of sensitive student and family data in SLDS	✗
Notice of SLDS collection and related parental rights	✗