



330 Main Street, Hartford, Connecticut 06106

860-523-9146 | www.acluct.org

Written Testimony Supporting House Bill 5469, An Act Concerning Student Data Privacy

Senator Slossberg, Representative Fleischmann, and members of the Education Committee. My name is David McGuire, and I am the Legislative and Policy Director for the American Civil Liberties Union of Connecticut (ACLU-CT). Our organization is a member of Connecticut Alliance for Privacy in Education (CAPE). CAPE's mission is to advocate for state legislation ensuring greater transparency and security of student information. My testimony will primarily focus on the search of students' personal electronic devices and the risks associated with educational apps. I am submitting this testimony in support of House Bill 5469, albeit with the recommendation that the committee strengthen the bill by amending it to include language protecting students' data from unlawful searches.

The ACLU of Connecticut strongly supports liberty and justice for all. This includes the right to privacy and freedom from baseless searches of one's personal information. Students do not check their rights at the schoolhouse door. Requiring a student to sacrifice his or her constitutional right to privacy in order to obtain equal access to education is not only wrong; it is unworthy of a twenty-first century educational system.

Today's schools and students must navigate technology in myriad ways: through school-owned devices in school and at home; through personal devices during lunch or other breaks; through educational apps from third-party companies; and more. Each form of technology presents an opportunity to prepare Connecticut's kids for the future. Each also presents privacy concerns if the data that they collect is not secure and if they are used as another on-ramp for the school-to-prison pipeline. We therefore applaud the committee for taking up the issue of student privacy. By regulating the ways in which contractors, such as those that provide educational apps, can access and use student information, House Bill 5469 is a step in the right direction, but it does not go far enough to protect students' constitutional rights.

The ACLU of Connecticut strongly encourages the committee to add language to protect students from suspicionless searches, as we have serious constitutional objections to allowing schools to search students' devices without reason. Access to a young person's cell phone, tablet, or laptop means access to their private worlds. These devices are like backpacks, if backpacks contained every note you've passed to a friend, every photo you've taken, every phone call you've made to your parents, and more. Before searching an actual backpack, however, school officials are required to have specific, reasonable suspicion that a student has broken the law or a school rule. Students' electronic devices should be held to the same standard.

Right now, however, Connecticut schools have a patchwork of unequal privacy policies. West

Haven High School, for instance, states that students' "electronic devices may be searched as part of any school investigation," and that its more than 1,800 students "should have no expectation of privacy as to any images, messages, or other files such devices might contain." This is a grave violation of students' privacy rights. Other school districts have flawed policies that purport to give school administrators the right to demand the passwords for students' personal devices without cause.

Preventing schools from conducting suspicionless searches of students' devices would not only uphold students' privacy and Fourth Amendment right to freedom from unreasonable search and seizure it also could decrease the chance that a student enters the criminal justice system. In 2013, for instance, Connecticut Voices for Children found that 2,214 Connecticut students were arrested at school, and arrest rates were higher among minority, special education, and low-income students. Nearly one in ten students was arrested for non-violent violations of school policy, such as using profanity. Without protections in place, one could easily imagine a school administrator conducting random searches of students' cell phones and finding profane language. Even if that discovery only led to a suspension or expulsion, rather than an arrest, evidence has shown time and time again that time away from school due to disciplinary action increases a child's risk of entering the criminal justice system later in life. Such potentially life-changing consequences should, at the very least, be based on a reasonable suspicion, not random acts of intrusion.

As many of you are likely well aware, personal information is also a valuable commodity in today's data and advertising-driven society. Student data is no different. Schools such as Suffield and Newington, for instance, use Google Chromebooks and Google Apps for Education as part of their one-to-one laptop programs. These devices and apps have enormous potential to provide students, particularly those from low-income families, with equal access to technology. In 2014, however, a California-based lawsuit also showed that Google was scanning students' emails in order to target advertising to children—even in cases when students had disabled advertising, and without consent from students or their parents. Google amended some of its policies, but the situation should serve as a cautionary tale about what can happen when for-profit companies, whose interests may not align with those of schools, parents, or students, have access to sensitive student data. Closer to home, last year, the Hamden School District agreed to provide the Connecticut Council for Education Reform, an outside organization, with information from students' records and classroom schedules, unbeknownst to students or parents. Incidents like this demonstrate the need for reform in this area. Although the Children's Online Privacy and Protections Act (COPPA) requires verifiable consent from a parent for an app or website to collect information from a child under 13 these protections are not enforced. We believe House Bill 5469 should include similar protections and a meaningful enforcement mechanism.

In another case, the Lower Merion School District in Pennsylvania provided students with MacBooks. Without students' or parents' knowledge, each of these laptops was equipped with spyware. The school used this spyware to capture thousands of webcam images, screenshots, and communications from at least two students whose parents later successfully sued the district for \$610,000. In the end, the district's actions cost more than settlement money: they broke the community's trust and violated students' privacy.

With House Bill 5469 and the addition of language to prevent baseless searches, Connecticut can make sure that its laws keep up with the changing faces of education and student safety. We urge you to strengthen and support this important bill.

Student Data Privacy Bill Checklist

CAPE4Kids.org

	Scoring Code
	<i>In Bill</i> ✓
	<i>Not In Bill</i> ✗
	<i>In bill, but needs improvement</i> ▼
	<i>Should not be in bill</i> ?
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)	X
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	X
Require BoE to provide school employee data handling awareness info	X
Require up-to-date encryption tools (HB5469 "industry standard" - could be more specific)	▼
Require independent audits of public agency and third party data handling	X
Ensure bill covers students covered under FERPA (prek-12; college)	X
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	X
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	X
Clarify and strengthen "authorized representatives" and "legitimate educational interests" that permit data sharing under FERPA	X
Background checks for contractor employees who handle student data	X
Require contracts to indemnify the state and hold contractors accountable	X
Allow online operators to collect and redisclose PII to subcontracted entities (lines 161-167)	💡
Establish enforcement mechanism, such as AG student data privacy enforcement	X
State Data Collection and Compiling	HB5469
State Chief Privacy Officer and Citizens Advisory Board	X
Legislative authorization for all student data elements (i.e. inter-agency sharing)	X
Transparency SLDS collection and purpose; Consider SLDS moratorium on expansion	X
Ban SLDS from being used for employability, criminal/civil liability, financial standing, or reputation of the student	X
Ban collection of sensitive student and family data in SLDS	X
Notice of SLDS collection and related parental rights	X