State of Connecticut

DIVISION OF PUBLIC DEFENDER SERVICES

Office of Chief Public Defender
30 Trinity Street, 4th Floor
Hartford, Connecticut
(860) 509-6405 Telephone
(860) 509-6495 Fax

Christine Perra Rapillo
Chief Public Defender
Christine.Rapillo@jud.ct.gov

Deborah Del Prete Sullivan
Legal Counsel, Director
deborah.d.sullivan@jud.ct.gov

Testimony of Deborah Del Prete Sullivan
Legal Counsel, Director

Education Committee Public Hearing -February 26, 2018

Raised H. B. 5170
An Act Concerning Students' Right to Privacy in Their Mobile Electronic Devices

The Office of Chief Public Defender opposes passage of **Raised H. B. 5170, An Act Concerning Students' Right to Privacy in Their Mobile Electronic Devices.** This bill is overly broad and would permit the seizure and search of a student's personal mobile device, including but not limited to their laptop, cell phone or tablet, regardless of whether a crime had been committed. If passed, basically any school employee and anyone working or volunteering at a school, would be permitted to seize a student's electronic device. Of much greater concern is that as drafted, this bill permits a "school administrator" (undefined in the bill) to search a student's mobile electronic device if the student was observed violating a school policy, such as texting in school. This bill permits unreasonable searches and seizures of personally owned electronic technology in violation of the state and federal constitutions.

Raised H. B. 5170 is overly intrusive by invading a student's legitimate expectation of privacy in their mobile electronic devices, and possibly the privacy expectations of the parents/guardians who may actually own and/or pay for the cell phone, laptop or other mobile electronic device. The bill allows for a search of the device, without probable cause and a warrant, for minor school policy violations. While we acknowledge schools' special prerogatives in maintaining discipline in the classroom and on school grounds, and in preventing "imminent personal injury" to students, by permitting such searches, this bill goes too far. In reality, if such imminent conduct is suspected, school officials may take action and simultaneously contact law enforcement.

Under current U.S. Supreme Court law, an arrestee has greater protections than this bill would provide students, as an arrestee's cell phone cannot be searched without a warrant (absent exigent circumstances). *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473 (2014). The *Riley* case involved the appeals of two defendants, one charged in a drive-by shooting and the other charged with drug and weapon offenses. The Supreme Court held that *"the interest in protecting officers' safety"* and the *"interest in preventing destruction of evidence did not justify dispensing with [the] warrant requirement for searches of cell phone data"*. *Riley v. California*, 573 U.S. ___ (2014). The Court cited cell phones' capacity to contain large amounts of personal data, and the fact that most Fourth Amendment jurisprudence predated such technology. *Riley v. California*, 573 U.S. ___ (2014). This reasoning applies to other personal mobile electronic devices, as well. If police need a warrant before searching the phone of someone already under arrest, it stands to reason that a school administrator may not conduct such a search with mere reasonable suspicion, a lower standard than probable cause, that a student violated educational policy.

Historically, the Supreme Court of the United States has long balanced the rights of students and school authorities. *See, e.g., Tinker v. Des Moines*, 393 U.S. 503 (1969); *Goss v. Lopez*, 419 U.S. 565 (1975). With respect to searches and seizures in school contexts, the Court has held that "[t]he determination of the standard of reasonableness governing any specific class of searches requires 'balancing the need to search against the invasion which the search entails.'" *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985) (quoting *Camara v. Municipal Court*, 387 U.S. 523, 536-37 (1967)). In cases predating cell phones and other mobile technology, usually school officials did not need to have probable cause to conduct a search to protect school safety, but their search must be "justified at its inception" and conducted in a manner "reasonably related in scope to the circumstances which justified the interference in the first place." *T.L.O.*, 469 U.S. at 341 (quoting *Terry v. Ohio*, 392 U.S. 1, 20 (1968)). A search is justified at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school," and "permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction." *T.L.O.*, 469 U.S. at 341-42. However, these cases do not address the issues pertaining to the substantial privacy rights in personal electronic devices as exist with today's technology.

Problematic under the bill is the broad definition of a "school employee," which includes any person who works in a school or who has regular contact with the students and who provides a service "to or on behalf" of the students. This could include parent volunteers, crossing guards, and outside vendors at the school under

contract with a board of education providing security, food, maintenance or construction services. Any of these persons would be permitted to seize a student's cell phone, tablet or laptop for even minor violations of school policy. As stated, in many instances, the mobile electronic device may actually be the property of the parent or guardian. While we are not necessarily opposed to the seizure by school personnel of a mobile electronic device upon the violation of school policy, the range of personnel so authorized must be narrow, such personnel must be appropriately trained, and searches must be prohibited.

Also problematic under the bill is that there are no time frames within which the device will be returned once it is seized. The bill states only that parents and the student would be notified 24 hours after the search of a "suspected violation" and the data accessed. As drafted, there is no limitation in time as to how soon after a seizure the search must occur, so the eventual notification could be days, weeks or months after the seizure of the device. We suggest that any device seized should be returned to the parents/guardians of the student at the end of the school day to avoid the risk to the school of having to safely secure and store the devices and its personal information. If not, the cost of storage and secure safekeeping by the school must be considered. Sadly, in this day and age, the fact that any further delay might impede family members' ability to contact each other, or authorities, in cases of emergency also must be considered.

In addition, there are no prohibitions on the sharing of the data or information obtained from the device. As a result, in addition to the constitutional issues, this legislation is unworkable because while it restricts school employee activity, it contains no penalty or other accountability mechanism to address instances in which a school employee fails to comply with the restriction against disclosure of information obtained from or observed on the student's device. As a result, any data or information obtained can be used against the student not only in a disciplinary proceeding but also in a criminal prosecution, even if the obtained information was unrelated to any perceived policy violation and law enforcement would have needed a warrant to find such information.

Finally, implementation costs are not addressed in this proposal. This legislation may create an unfunded mandate insofar as local education agencies are burdened with costs associated with the issues of: training for anyone authorized to seize a device or to conduct a search; how, when and with whom the information and data obtained would be shared (including whether other law enforcement and the school resource officer will be permitted to view the information and data); and how, where and for how long the device and information and data obtained, some of which could be of a confidential nature, would be securely stored.

Therefore, the Office of Chief Public Defender opposes searches of mobile electronic devices seized from students without probable cause and a warrant. Barring cell phones and other electronic devices from schools entirely is not the answer and is unworkable with today's technology and usage of such by students for school related work and assignments.

The Office of Chief Public Defender suggests schools have an *Acceptable Use Policy* which students and parents/guardians sign. This policy would advise the student and the parents/guardians that if the student is found to be violating a school policy, the mobile electronic device will be seized and returned to the parents/guardian at the end of the school day. However, the policy should never require anyone to consent to, or authorize a search of, any mobile electronic device.

As always, the Office of Chief Public Defender is willing to participate in further discussions held on these issues to ensure that any legislation is constitutional.