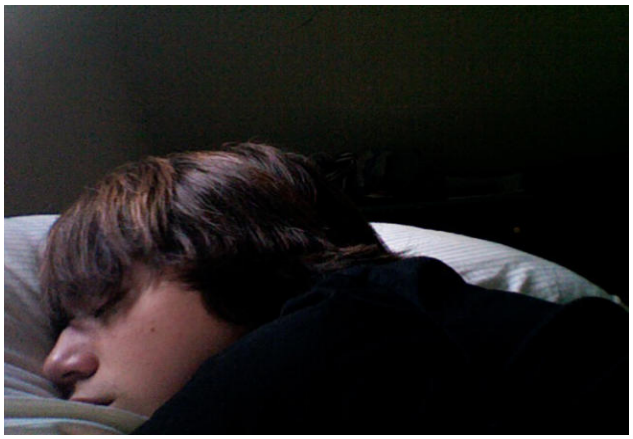
HIGH SCHOOL NON-CONFIDENTIAL:
How School-Loaned Computers May Be Peering Into Your Home

June 2017

American Civil Liberties Union of Rhode Island
128 Dorrance St., Suite 400
Providence, RI 02903
P: (401) 831-7171
F: (401) 831-7175
www.riaclu.org

Introduction and Summary

Below is a photo of a teenager sleeping in his bed at home. His name is Blake Robbins, and at the time this photo was taken, he was a sophomore at Harriton High School in Pennsylvania's Lower Merion School District. As banal as this photograph might seem, there is something deeply disturbing about it.



The photo was taken without Blake's knowledge – but even worse, it was officials of his school district who took it. That photo and hundreds of other screenshots of him were taken on the laptop computer he had been given by his school as part of a "1 to 1" program, where a third party, in collaboration with school districts, provides free laptops or tablet computers to students for the school year. After being sued, the school district acknowledged it had surreptitiously taken over 50,000 screenshots of students using their computers, and ultimately agreed to a court order banning it from remotely accessing the devices for such purposes.[1]

As startling as this might seem, many school districts in Rhode Island that have 1:1 programs also claim the right to surreptitiously access their students' loaned computers remotely. The purpose of this brief report is to call attention to this serious privacy issue and to urge Rhode Island legislators to take action to overturn school districts' troubling policies.

In an examination of Rhode Island school district 1:1 policies, the ACLU found:

- All 22 school districts with 1:1 programs require parents to acknowledge that there is no expectation of privacy in use of the device, even if the schools explicitly allow the device to be used by parents or for non-school purposes.

- Eleven districts specify that they can remotely access a student's 1:1 device at any time and for any reason, without notice or consent.

- Only six districts that indicate they have the authority to remotely access the device state that such access does not include monitoring via the camera or microphone.

1 For background on this case, see, e.g., http://www.nbcphiladelphia.com/news/local/1000s-of-Photos-Taken-of-Students-in-WebcamGate-Suit--91040834.html; https://www.forbes.com/sites/kashmirhill/2010/10/11/lower-merion-school-district-and-blake-robbins-reach-a-settlement-in-spycamgate/#5c8f444f2c60

- Fifteen districts indicate they have the right to physically inspect the device and all its contents at any time and for any reason.

- School districts that give both administrators and teachers the right to remotely access devices do not specify which particular individuals are given this authority.

- Finally, looking at financial, not privacy, issues only six school districts accommodate poorer families by providing insurance coverage for the devices for free or at reduced cost.

Some school districts equate the blanket access they give themselves to peer into the students' computers to their authority to inspect school lockers. But such an analogy is woefully misplaced. A locker is not just school property; *it is always in the school*. The 1:1 program is specifically designed to allow students to use the device at home, and the notion of school officials figuratively – or literally – peering over students' shoulders at 8 o'clock at night while they do their homework is deeply troubling. Further, searching a student's computer, even one loaned by the school, raises additional First Amendment concerns. Unlike a locker, a search of a computer necessitates reviewing documents, files, messages and other classic elements of "speech," not just a student's property.

Because we believe that parents and students should retain some reasonable level of privacy in the home setting, even with a device loaned by the school, the ACLU urges that safeguards be put in place to prevent stories like those of Blake Robbins from occurring in Rhode Island. Specifically, this report recommends, among other things, that:

- Except in special delineated circumstances, school districts should be prohibited from remotely accessing a student's device when they are not in the school.

- A school district should not search the contents of a student's device unless there is a reasonable suspicion of specified misconduct.

- If a student is suspected of illegal conduct or activity, and in the absence of exigent circumstances, the school should not conduct a search unless a judicial warrant has been provided.

- Policies should specify which school officials have the authority to inspect the computers.

- Schools should provide insurance for the devices at reduced or no cost to needy families.

- The General Assembly should pass legislation codifying the standards contained in the above recommendations in order to ensure uniformity in privacy protections.

Background

While 1:1 programs can be very beneficial, the ACLU has found that too many schools require students – and their parents – to give up any rights to privacy to participate in the program. The waiver is made even more troubling by the fact that student participation in the program is often mandatory. This waiver of rights often includes giving schools the ability to remotely activate the device's camera, and to review the email and Internet search history stored on these computers, for no reason or any reason.

The ACLU of Rhode Island first raised concerns about these issues in a letter to school district superintendents in 2014, and offered assistance in crafting comprehensive policies to protect students' privacy by establishing standards over the schools' ability to inspect or access the devices and their content.

In January 2017, the ACLU followed up by filing Access to Public Records Act requests to thirty-three school districts in the state, requesting documents relating to their use of Chromebooks or other tablet devices. In particular, we sought copies of their policies or procedures relating to the distribution of these computers to students, copies of any agreements signed by parents, and the policies regarding the use and monitoring of these devices. A total of twenty-two school districts were identified as participating in the 1:1 program.[2] Most of the districts distribute the devices during the summer before the school year begins. Several of them begin distributing devices in the elementary schools. Virtually all of them have policies that raise privacy concerns.

In looking at the information from each school district, the ACLU wanted to specifically focus on their policies regarding student privacy, especially on the ability of school officials to perform inspections or gain remote access to the devices. We were also interested in learning about the use of internet filters on the devices and, in light of the financial implications for poor families, issues relating to insurance availability and cost and the consequences of losing or misplacing the device. In brief, the results were quite alarming.

Findings

In examining the privacy issues surrounding the use of the devices, we looked for three items in school district policies: whether they explicitly authorized remote access to the students' computers, whether there were any standards for inspecting the contents of the computers, and, more generally, what expectations of privacy the policy laid out.

Expectation of Privacy

[2] Barrington, Bristol-Warren, Central Falls, Chariho, Coventry, Cumberland, East Greenwich, Burrillville, Jamestown, Johnston, Narragansett, North Smithfield, North Kingstown, Pawtucket, Portsmouth, Providence, Smithfield, South Kingstown, Warwick, Exeter-West Greenwich, West Warwick, Westerly.

While the computers are school-loaned devices, and mainly designed for schoolwork, one would still expect some degree of privacy surrounding their use. After all, the program is designed to allow students to use the device at home, and the notion of school officials figuratively – or literally – peering over students' shoulders at 8 o'clock at night while they do their homework is deeply troubling.

Providing students with some expectation of privacy is important for a number of reasons. First, the home has often been deemed the quintessential private space beyond the reach of government snooping in the absence of exigent circumstances or judicial authorization. The notion of the home as one's castle dates back centuries as both a social and legal norm. Using new technology as an excuse to invade this sanctum should be forcefully rejected, as the consequences for privacy rights of both adults and minors are potentially enormous.

Further, some school districts specifically acknowledge that the 1:1 computers can be used for non-school work at home, and at least one policy encourages parents to use the devices. In other words, even accepting the assumption, which the ACLU does not, that a school district should have the right to monitor a student's *educational* activities miles away, even though conducted on his or her own time, it is another matter entirely for schools to be able to find out how the device is being used by non-students and by minors legitimately using the computer for private purposes.

Twenty-two school districts give students *NO* expectation of privacy

Yet all twenty-two school districts that participate in the 1:1 program have cautioned within their policies that students who use the device have *no expectation of privacy* whatsoever. Typical is Narragansett's policy, which states that students "understand that there is no expectation of privacy when using the District network and devices."

Instead, several policies authorize school officials to remotely monitor the device outside of school – including accessing files and emails and in some cases even the webcam – and to physically inspect the computer without the need for any suspicion of misconduct. Most 1:1 policies covered in this report apprise students that every document, file and email may be generally accessible to the scrutiny of administrators inside and outside of school for any reason.

The ACLU of RI believes that requiring students and parents to renounce any expectation of privacy in the use of the device at home is an unacceptable diminishment of fundamental privacy rights. Indeed, looking more closely at exactly what this waiver of privacy expectations means, as the next sections do, demonstrates just how inappropriate this mandate is.

Table 1 – Schools participating in 1:1 program and their respective privacy policies

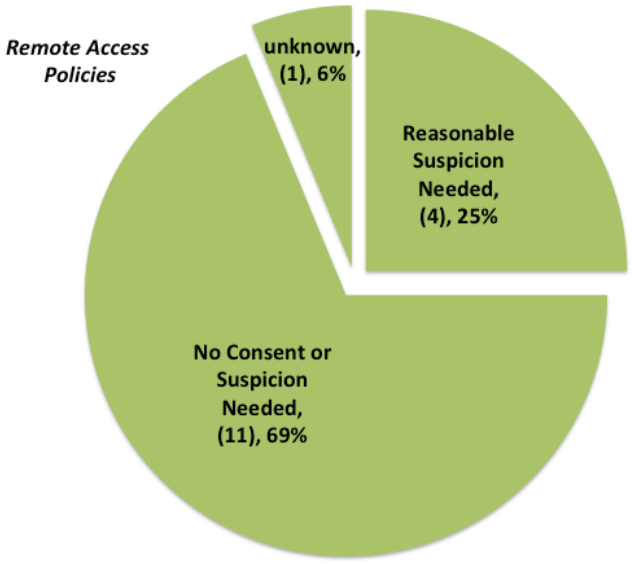
District	Policies Explicitly Note No Expectation of Privacy	School Maintains Right to Remote Access	School Maintains Right to Inspect with Suspicion of Misconduct	School Maintains the Right to Inspect for Any Reason
Barrington	X	X*		X
Bristol-Warren	X	X		X
Burrillville	X			X
Central Falls	X			X
Chariho	X	X		X
Coventry	X	X	X	
Cumberland	X	X		X
East Greenwich	X	X		X
Exeter-West Greenwich	X	X	X	
Jamestown	X		X	
Johnston	X	X		X
Narragansett	X	X		X
North Kingstown	X	X*		X
North Smithfield	X	X*		X
Pawtucket	X			X
Portsmouth	X	X*		X
Providence	X		X	
Smithfield	X	X*	X	
South Kingstown	X	X		X
Warwick	X	X*	X	
West Warwick	X	X	X	
Westerly	X			X
TOTAL	**22**	**16**	**7**	**15**

*Schools that specify that cameras and microphones will not be enabled during remote access

Remote Access

Remote access allows school districts to monitor, manipulate, or delete any information within the device, including email and files, without actually possessing the computer. Having the ability to monitor a device and its contents from a remote location, even when the student is outside of school, raises several red flags. Even more are raised when it involves accessing the computer's webcam and/or microphone.

A total of sixteen school districts explicitly include in their 1:1 policies the ability to remotely access a student's device.[3] Eleven of these policies indicate that remote monitoring can occur at any time without notice or consent.[4] Typical are the policies of the Chariho and Warwick school districts, which provide that "the district can access, review, copy, store or delete any electronic communication or files."



In at least five districts – Barrington, Bristol, Chariho, Pawtucket and Warwick – students are explicitly permitted to use the computers for personal as well as school-related reasons, and in the case of the Chariho district, parents are encouraged to use the device, making remote monitoring even more problematic.

Some of the policies indicate that both administrators and teachers have the authority to conduct remote monitoring, but none outline *which* specific administrators or teachers have this role. There is also a general lack of parameters set on when and for what reason they are able to engage in this undeniably intrusive activity. This type of unlimited power to remotely monitor what a student is doing at home is rather frightening.

Only four districts – Coventry, North Smithfield, North Kingstown and Smithfield – seem to place limits on when remote monitoring is authorized. Their policies indicate that they have the authority to remotely monitor the use, file or activity of a student with a district device *only when there is a reason* to believe the student has engaged in "school-related" misconduct. Even here, though, it is important to note that none of these policies outlines what type of "misconduct" is necessary for remote monitoring to take place.

During school hours, teachers and administrators are responsible for the well-being and supervision of students; however, when they arrive home, that responsibility shifts to the parent or guardian. A school's continuous and invasive remote monitoring of a student's device while under the care of a parent or guardian oversteps a school's boundaries.

One of the most concerning issues in regards to remote access has to do with the use of cameras and microphones. While policies authorizing such an invasion of privacy have already been challenged in Blake Robbins' case, as mentioned previously, and criticized

[3] Barrington, Bristol-Warren, Chariho, Coventry, Cumberland, East Greenwich, Exeter-West Greenwich, Johnston, Narragansett, North Smithfield, North Kingstown, Portsmouth, Smithfield, South Kingstown, Warwick, West Warwick.

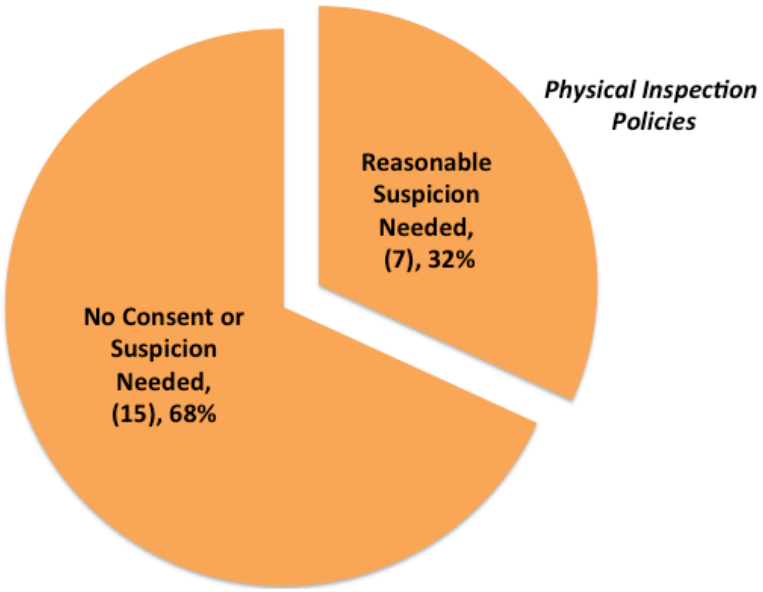
[4] Barrington, Bristol-Warren, Chariho, Cumberland, East Greenwich, Exeter-West Greenwich, Johnston, Narragansett, Portsmouth, South Kingstown, Warwick.

elsewhere,[5] only six of the sixteen Rhode Island school districts that outline their use of remote access note that they will *not* make use of the camera or microphone when monitoring the device.[6]

Activating a camera, microphone, or screen sharing software from a remote location, unless it is authorized by a warrant, should be explicitly prohibited. As the Pennsylvania case illustrated, to allow otherwise is nothing short of creepy.

Right to Physical Inspection

When it comes to physically inspecting the loaned computers during school hours, all twenty-two districts participating in the 1:1 program outline in their policies the right of school administrators or teachers to physically inspect the student's device. Fifteen districts indicate that they have the right to inspect the device for *any* reason and at any time.[7] The other seven districts have instead established policies in which devices may only be physically inspected if *there is reason to believe* that the student has violated school policies or procedures or has engaged in other misconduct while using the device.[8] Similar to the districts that have "misconduct" standards regarding remote access, though, these policies concerning physical inspection do not go into detail about what types of violations or misconduct would suffice to allow for this type of inspection.



Three districts – Central Falls, Burrillville and West Warwick – compare the right to inspect a student's 1:1 computer to that of a student's locker, by stating, "any computer or network storage area will be treated like school lockers. Network administrators may review files, communications and network sites visited to maintain system integrity and to ensure that users are responsible in using the system." Yet such an analogy fails to take into consideration the significant privacy differences involved. A locker is not just school property; *it is always in the school*. If a school district provided students free backpacks to use to carry their books and paraphernalia back and forth to school, would anybody seriously argue that gave

[5] http://www.huffingtonpost.com/2010/02/26/dan-ackerman-school-sdmin_n_477935.html

[6] Barrington, Smithfield, North Smithfield, North Kingstown, Portsmouth, Warwick.

[7] Barrington, Bristol-Warren, Burrillville, Central Falls, Chariho, Cumberland, East Greenwich, Johnston, Narragansett, North Kingstown, North Smithfield, Pawtucket, Portsmouth, South Kingstown, Westerly.

[8] Coventry, Exeter-West Greenwich, Jamestown, Providence, Smithfield, Warwick, West Warwick. Notably, only two of the four districts requiring a "reasonable basis" standard for accessing the computers remotely – Coventry and Smithfield – also have such a standard in place for physical inspections.

school officials the right to check the bags' content while it was in the child's home, or even to search it, without any cause, in school?

They have the right to inspect the device *for any reason and at any*

Further, searching a student's computer, even one loaned by the school, raises not only Fourth Amendment concerns, but First Amendment ones as well. Unlike a locker, a search of a computer necessitates reviewing documents, files and other classic elements of "speech," not just a student's property. The school lets students eat lunch at tables owned by the school, but that doesn't mean officials have the right to listen in on students' conversations while they're sitting there.

When examining a student's expectation of privacy in regards to the right to inspection, we found that of the seven school districts that specified in their policy that a device may *only* be physically inspected when there's reason to believe that a student has violated a rule or may be engaged in misconduct, five also have policies – somewhat contradictorily – about remotely accessing the student's device without the need for a specific reason.[9]

There were only two districts, Jamestown and Providence, that did *not* have a policy regarding remote access *and required* that before a device is physically inspected, the administration must confirm that the student has violated a school policy, regulation or has engaged in misconduct. Providence goes so far as to state that while the district can have access to records, files and emails within their network, these would not be inspected without the consent of the sender or a recipient, unless it is necessary to investigate a complaint. Unfortunately, Providence's more protective policy was not duplicated elsewhere.

Internet Filtering

Every school district in Rhode Island uses Internet filtering software to block or filter content that is obscene, pornographic, and harmful to minors. Federal law requires this filtering. But we know that school districts filter much more than those categories, often to absurd lengths.[10]

Thirteen districts highlight in their policies that their Internet filtering software will be active while the student uses the computer at home, even if they are outside of the school's network.[11] Similar to the use of remote monitoring and access when a student is away from school, mandating that the school's Internet filter be in place while the student is under their parent or guardian's supervision is unnecessary and inappropriate – at least to the extent the filtering goes beyond what federal law requires – since it diminishes parental authority and limits the educational value of the computer's use in the first place.

---

[9] Coventry, Exeter-West Greenwich, Smithfield, Warwick, and West Warwick. See fn. 6, supra.

[10] See our report, "Access Denied: How Internet Filtering Harms Public Education," available at: http://riaclu.org/images/uploads/Access_Denied-_How_Internet_Filtering_in_Schools_Harms_Public_Education.pdf

[11] Barrington, Chariho, Coventry, East Greenwich, Burrillville, Narragansett, North Kingstown, North Smithfield, Pawtucket, Portsmouth, Smithfield, South Kingstown, Warwick.

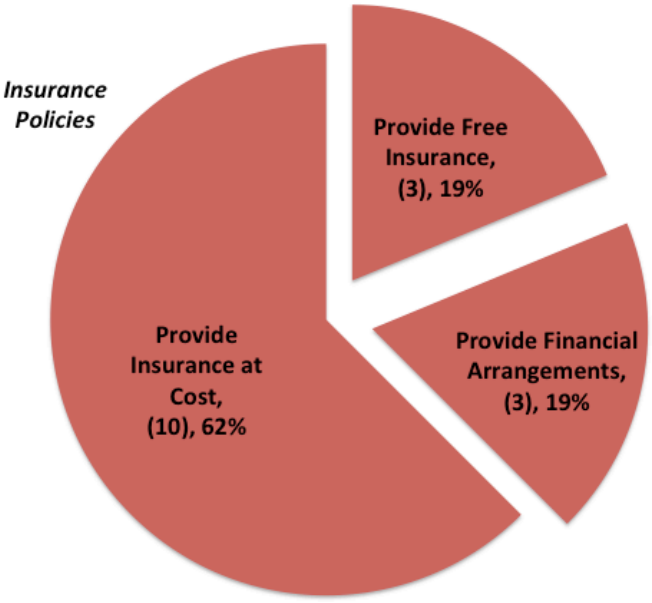
Only three districts – Bristol-Warren, Exeter-West Greenwich, and West Warwick – point out that when the student uses their device at home it will not be filtered. Yet all three of these districts also advise that the computers can be remotely accessed at any time and for any reason – meaning any internet searching done by the students is subject to monitoring by school officials. The remaining six districts do not make mention about the filtering software being enabled while the student is away from the district's network, but they do mention the use of it while inside the school's network.

Finances

In addition to the privacy issues raised by the 1:1 program, we were also interested in examining some of the financial implications for students and families who often have no choice but to participate in the program. In that regard, we looked at school policies governing missing or lost devices and the availability of insurance.

Insurance

Sixteen school districts contain within their policies guidelines regarding insurance for the devices provided to the students.[12] The school districts that provide optional insurance do so through third parties; those that don't offer insurance encourage families to look into adding the device into their home or renters' insurance coverage.[13] Insurance costs are used for replacements, upgrades, and normal wear and tear of the devices. Most policies explicitly point out that intentional damage, loss or theft of the device will not be covered by the insurance.



Coventry and Cumberland provide insurance coverage for up to three years; they do so for a total cost of $40 and $47 respectively. Pawtucket and Providence charge an annual fee of $25 and $30 respectively for insurance while Narragansett's insurance starts at $24 and goes up to $54 depending on the Chromebook model that the student receives.

Only three districts make specific arrangements to meet the financial needs of families that may not be able to afford the cost of insurance. East Providence charges $22 for annual insurance coverage but offers financial assistance for parents who need it. Warwick and Coventry consider the price of insurance based on the family's eligibility for free or reduced lunch.

[12] Chariho, Coventry, Cumberland, East Greenwich, East Providence, Jamestown, Johnston, Narragansett, North Smithfield, North Kingstown, Pawtucket, Portsmouth, Providence, Smithfield, South Kingstown, Warwick.

[13] Central Falls and West Warwick School Districts

Three additional districts – Portsmouth, Jamestown, and South Kingstown – address the issue by providing insurance coverage to all students at no cost. As the Portsmouth policy details, "all issued devices will include district-purchased property insurance. The district-purchased property insurance will cover mechanical or physical breakdowns that may result from normal usage during the life of the 1:1 agreement." Similar to districts that charge for third party insurance, these districts highlight that "the district-purchased property insurance may not cover intentional misuse, abuse, or lost devices." The ACLU believes that every school district should be making accommodations to address the situation faced by poorer families, as these three school districts do.

Missing or Lost Devices

The loss, theft, or damage of a device can become the full financial responsibility of parents and students in the majority of the districts, according to their policies. Similarly, ten districts that participate in the 1:1 program highlight that a device that is missing from school for two or more days will be considered stolen and would be reported to the local police.[14] Other districts such as Chariho and Portsmouth state that if a student has multiple occurrences of going to school without their device they will be subject to disciplinary action. While none of the ten district policies explicitly outline what legal or disciplinary actions may be taken against a parent or student, it is safe to say that due to the policy requirements regarding "full financial responsibility" for any lost or stolen device as stated above, they would be responsible for replacing the device.

Schools Not Participating in 1:1

A total of eleven school districts in Rhode Island stated that they do not take part in the 1:1 program.[15] Five of them provided us information regarding their Internet monitoring policies within their network, including that "students should not have any explicit expectation of privacy" when it comes to monitoring their Internet searches and use.

Two districts, Cranston and Foster, indicated that they do not participate in the 1:1 program, but they do loan Chromebooks and other devices to their students. The Cranston school district's status is somewhat confusing, though. They enclosed several copies of "School Department Equipment Loan Agreements," which detail the description of the equipment used, the reason for the equipment loan, condition of equipment, loan period, as well as signatures from both the parent and student, and sometimes specify that the device is for use at home. By allowing students to take a device home, the Cranston school district is, for all intents and purposes, essentially participating in a 1:1 program but without specific parameters to accompany it.

Foster's Chromebook loaning agreement states that "at this point, the Chromebooks will stay at school and it's expected that students use their home computer/device for

[14] Barrington, Bristol-Warren, Central Falls, Coventry, Cumberland, Jamestown, Johnston, North Smithfield, Warwick, West Warwick.

[15] Cranston, East Providence, Foster-Glocester, Lincoln, Little Compton, New Shoreham, Newport, North Providence, North Scituate, Tiverton, and Woonsocket.

assignments," which suggests that while each student is assigned a particular device, they are not allowed to bring it home.

None of the school districts that fail to participate in the 1:1 program mentioned any interest in doing so in the future.

Recommendations

In light of the serious privacy issues raised by school access to these computers when used by students outside the classroom, the ACLU of RI urges that steps be taken to protect the privacy of students and their families.

Prohibit Remote Access to Cameras and Recorders

- School districts and/or third parties should be prohibited from activating or remotely accessing the camera and recording functions in a students' devices when they are not in the school for any reason unless:
    - The student initiates the access through video or audio chat for educational purposes
    - The activation and/or access is ordered through a judicial warrant
    - Access is necessary to respond to an imminent threat of life and safety

Restrict Remote Access to the Device

- School districts and/or third parties should be prohibited from otherwise remotely accessing a student's advice out of school unless:
    - There is reasonable suspicion that the student has engaged in specified misconduct, that suspicion is documented, the search is limited to finding evidence of such misconduct, and parents are notified of the search
    - Access is necessary to address technological threats to the school computer system or to update or upgrade the device's software,
    - A warrant has been obtained if the search is designed to look for evidence of criminal activity
    - The parent has given consent to search on an individualized basis

- Location tracking of a device should be restricted to situations where the device has been reported stolen, a student has not returned the device to school, or there is an imminent threat to life or safety

Standards Required for Search

- A school district should not physically search the contents of a student's device except for reasons otherwise allowed to obtain remote access, or for legitimate educationally related reasons

- The browser, keystroke or location history of a device should not be accessed in the absence of reasonable suspicion of a violation of school policy or for technological reasons
- Any actions of misconduct that would lead to a search should be detailed within school district policy.
- Policies should specify which school officials have the authority to search the computers remotely or otherwise

Financial Considerations

- Schools should provide insurance at reduced or no cost to needy families.

Promote Uniformity in Internet Access through Legislation

- In order to promote uniformity, the General Assembly should pass legislation codifying the standards contained in the above recommendations in order to ensure uniformity in privacy protections statewide. The ACLU of RI supports the adoption of legislation pending in the General Assembly, and sponsored by Sen. Adam Satchell and Rep. Brian Patrick Kennedy, that addresses many of these key issues.[16]

[16] http://webserver.rilin.state.ri.us/BillText/BillText17/HouseText17/H5682.pdf; http://webserver.rilin.state.ri.us/BillText/BillText17/SenateText17/S0434.pdf