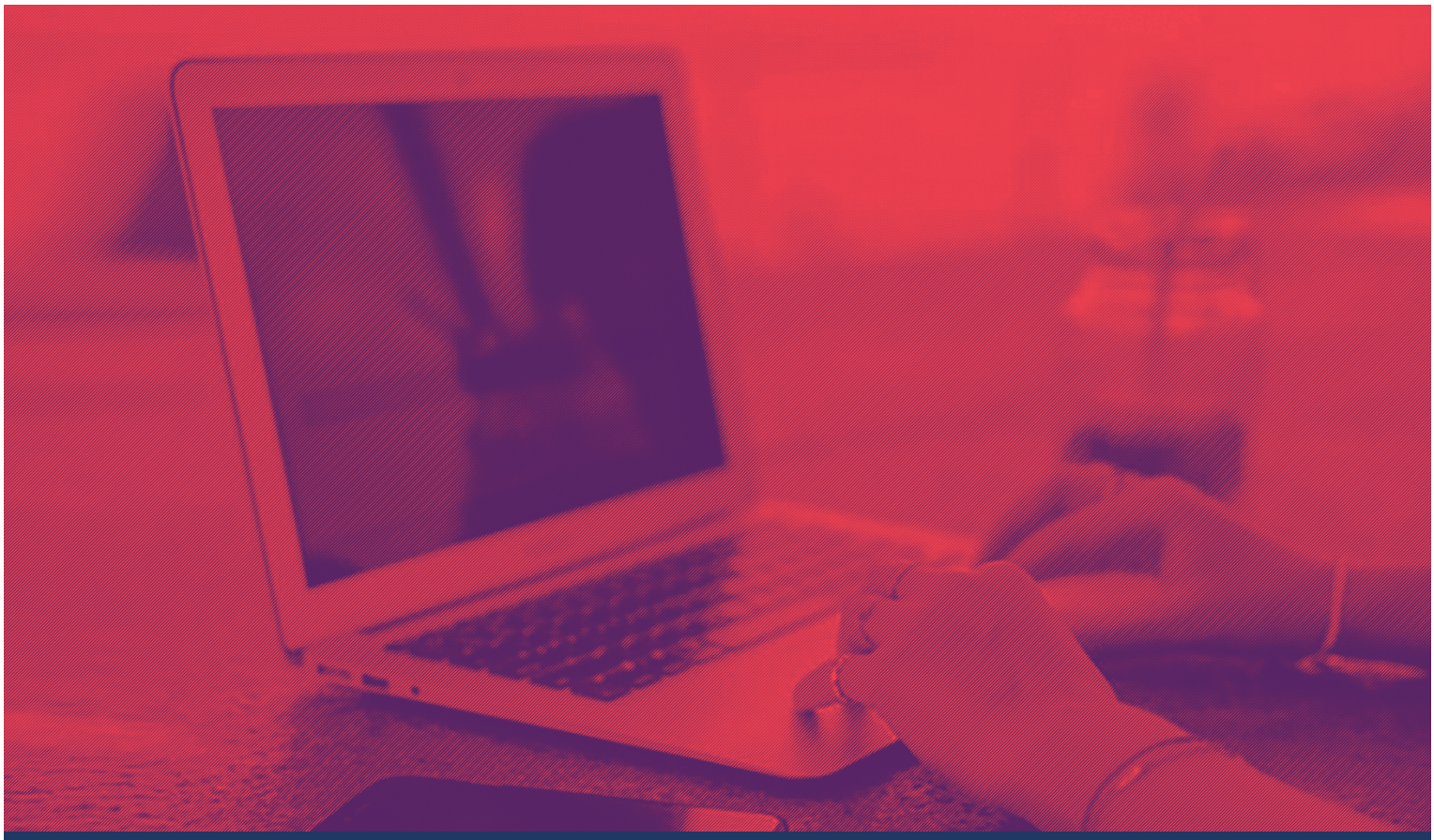

Zooming in on Students:

How Virtual Education Gets an "F" in Protecting Student Privacy

September 2020

ACLU Rhode Island

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Students do not leave their privacy rights at the door when they go to school, and they shouldn't have to fear that their schools and districts are spying on them during their education. Yet, despite the ubiquitous use of school-loaned computers due to the onset of the COVID-19 pandemic and the rapid transition to exclusively virtual education at the end of the 2019-2020 school year, and notwithstanding the role that remote education will inevitably play in public education for the foreseeable future, very few districts adequately protect the privacy of students who use school-loaned computer devices.

A survey that the ACLU of Rhode Island conducted of local school district policies regarding privacy and school-loaned computer programs revealed the following. Out of 36 public school districts:

- 24 districts allow school officials to **access the microphone or camera** on a school-loaned device **at any time**.
- 23 districts give officials the authority to **access the contents** of a school-loaned device **for any reason and with no notice**.
- 23 districts explicitly advise students and parents that they have **no expectation of privacy whatsoever** when in possession of the device.

Further, the use of independent, third-party software platforms compounds these privacy concerns by facilitating outside access to student data that could be improperly used and exploited by tech companies.

In order to effectively, comprehensively, and appropriately preserve student privacy, districts must immediately implement sufficient privacy protections for students, and the Rhode Island General Assembly should pass legislation which creates statewide privacy standards.

Included in these policies should be the following:

- A school district should not be able to access the computer's camera or microphone in the absence of legitimate educational reasons or purposes.
- A school district should be prohibited from remotely accessing the contents of a student's device except under specifically delineated circumstances.
- A school district should not search the contents of a student's device except under specifically delineated circumstances.

In addition, districts should immediately ensure that their privacy agreements with third-party software platforms are in compliance with Rhode Island law governing student data and student privacy.

Virtual learning should not come with an additional set of concerns about student privacy. In order to ensure that the privacy rights of students are protected, all districts – and the state of Rhode Island – need to immediately address this pressing topic.

INTRODUCTION

In 2017, the ACLU of Rhode Island conducted a comprehensive survey of the policies each school district had in place for the use of school-loaned computers and devices as a component of a student's education.[1] We found that, despite a majority of districts utilizing school-loaned computer programs – also known as 1:1 programs – many of the districts gave students and parents no assurances of privacy on these devices. Although alarming in itself, this lack of privacy protections became even more concerning in the context of the 2020 COVID-19 pandemic, in which all public schooling in the state of Rhode Island transitioned to fully virtual instruction for the last few months of the school year.

Following the release of our 2017 report, the ACLU of RI encouraged state legislators to pass legislation that would set a standard for privacy protection across all districts using 1:1 programs.[2] At the same time, we encouraged districts to independently update their 1:1 policies to protect their students from unnecessary and invasive monitoring by school officials on these school-loaned devices. More recently, we filed a public records request in February 2020 with the goal of obtaining an updated look at how, if at all, districts had modified their privacy policies since our 2017 report.

Unfortunately, while more districts had implemented 1:1 programs since 2017, we found that few had strengthened their privacy protections for students and families.[3] As schools had to make emergency closures in March 2020 to address the COVID-19 pandemic, Rhode Island's public education system transitioned to an entirely virtual and remote system, and the need for privacy on 1:1 computers – which quickly became integral to the entire educational process – became even more acute.

[1] See our previous report on this topic, *High School Non-Confidential: How School-Loaned Computers May Be Peering Into Your Home*, available at http://riaclu.org/images/uploads/1-1_Report_MAR_2020_UPDATE_.pdf
[2] The most recent version of the legislation was introduced in 2020 as H 7509 and S 2381.
[3] In 2017, 22 districts reported the use of school-loaned computer programs in their schools. Following the onset of the COVID-19 pandemic, all districts transitioned to programs which, to some degree, involved the administration of school-loaned computers.

Particularly concerning is a continued absence of policies restricting the ability of school administration and officials to remotely access the microphone and webcam of a school-loaned device or the data stored on it. Because virtual learning will certainly continue to be a widespread educational method – even outside the context of the pandemic by being utilized, for example, for education during snow days – the need for stronger privacy protections has become especially salient.

While more districts had implemented 1:1 programs since 2017, we found that few had strengthened their privacy protections for students and families.

Though Rhode Island recently committed to having all public school students back in schools full-time by mid-October, the COVID-19 crisis is not over, and virtual learning is certain to play a significant role in the next few years of public schooling. Especially considering this, restrictions on tracking the devices is also important because so much of a student's life – and the lives of their families – is inconsistent and in flux. As education is conducted from the home, students realistically may need flexibility in the location that they complete their schoolwork. Schools shouldn't, for example, be able to track a student from their home to their grandparents' home or to their parent's doctor appointment that they need to tag along for. Without legitimate reason, this is not information that schools should be monitoring.

In our analysis of the documents we received responsive to our February 2020 records request, we discovered the following about the school districts overall. Out of 36 districts:

- 24 districts allow school officials to access the microphone or camera on a school-loaned device at any time.
- 23 districts give officials the authority to access the contents of a school-loaned device for any reason and with no notice.
- 23 districts explicitly advise students and parents that they have no expectation of privacy whatsoever when in possession of the device.
- Only 4 districts explicitly have a ban on remotely tracking the location of a school-loaned device without cause.

After identifying the weaknesses in each individual district's privacy policies, we sent a letter in April 2020 asking them to take prompt action to strengthen their privacy policies and ensure that the confidentiality of students and parents was not compromised in the process of adjusting to this public health emergency. We particularly encouraged each district to amend their privacy protections to ensure that, at a minimum, they would not be allowed to indiscriminately review or retrieve the data or contents of a school-loaned device, or remotely access the loaned computers' camera or microphone.[4] An example of a letter addressed to one school district, Barrington, is included in Appendix A of this report. Though only one district, Tiverton, responded positively to our letter and began procedures to amend their policies, both East Greenwich and New Shoreham school districts additionally passed amendments which strengthened certain aspects of their policies.

Although not directly related to the lack of privacy protections on school-loaned devices themselves, an additional privacy issue worth highlighting concerns school districts' noncompliance with a state statute – R.I.G.L. §16-104-1 – which imposes strict safeguards against both third-party platform access to student data and use of computer-generated student data for commercial purposes. As more third-party programs are used in teachers' educational plans, these safeguards have become more critical as school-loaned device programs expand. Our letters to school districts reminded them of their obligations under this law to ensure that student-generated data would not be used to promote the commercial ends of third-party content providers or other commercial entities. This issue is addressed in greater depth later in this report.

In response to the survey we conducted in 2017, eleven districts noted that they did not participate in school-loaned computer programs.[5] At the time of our pre-pandemic February 2020 records request, no district indicated that they were uninvolved in a school-loaned computer program.[6] At the outset of the COVID-19 crisis, of course, the usage of such devices became both critical and ubiquitous across districts.

[4] At least one district, Tiverton, responded positively and is currently revising their policies.
[5] Cranston, East Providence, Foster-Glocester, Lincoln, Little Compton, New Shoreham, Newport, North Providence, North Scituate, Tiverton, and Woonsocket.
[6] The initial response from Glocester School Department noted that, in February 2020, they did not have a take-home school-loaned computer program for students and recommended referencing the policy of the Foster-Glocester

This report provides both an overview of the inadequate policies in place to protect the privacy of students and their parents, as well as suggested steps that should be taken to protect those rights as the use of 1:1 programs becomes more prevalent.

Regional School District for guidance on policies to this effect. After all schools became virtual in March 2020, we relied on this policy to determine the protections given to students in the Glocester School Department.

STUDENT PRIVACY POLICIES: THE GOOD AND THE BAD

Although there are many ways in which school districts can thoughtfully and comprehensively provide privacy protections for students, at a minimum their policies should: limit the remote access that schools have to the contents of a school-loaned computer to a few very specific, delineated instances; require parental notice for this access; and bar school officials' discretionary access to the computers' microphone, camera and location-tracking software.[7] When determining if a district's policies provided adequate privacy protections, we examined whether the policy included provisions along these lines, and whether it provided students with any expectation of privacy while using these devices.

Out of 36 school districts, 23 explicitly noted that students had no expectation of privacy; 24 districts did not ban remote access to the camera and microphone; and 23 districts retained the right to monitor the data and content of a school-loaned device without limitation. Based on this survey, a majority of Rhode Island public schools have clearly inadequate protections in place and reserve the right to severely invade the privacy of their students and families in using a school-loaned device.

When a student's school-loaned device may be the only electronic device that a family has, the access that schools allow themselves to these devices poses especially acute privacy concerns.

These results are even more troubling when one considers that some school districts actually encourage students to utilize these devices for non-academic purposes, and it is not unreasonable to assume that they could be used for non-academic needs within a family as well. In an emergency period like this, when a student's school-loaned computer may be the only electronic device that a family has, and families use it – with a school district's blessing – to look up medical information, file for

[7] There are instances in which cameras and microphones may be utilized for legitimate, remote learning purposes and access should be allowed in these limited cases.

unemployment or engage in online searches for information of a personal nature, the access that schools allow themselves to these devices poses especially significant privacy concerns.

Table 1: Privacy Policies by District

DISTRICT	Policies Explicitly Note No Expectation of Privacy	Policies *Do Not* Ban Remote Access to Camera and Microphone	School Maintains the Right to Monitor Data and Content Without Limit
Barrington			X
Bristol Warren		X*	X
Burrillville		X	X
Central Falls	X	X	X
Chariho	X		X
Coventry	X	X	X
Cranston	X	X	
Cumberland	X	X	
East Greenwich^		X	
East Providence	X	X	X
Exeter-West Greenwich^			X
Foster	X	X	X
Foster-Glocester	X	X	X
Glocester	X	X	X
Jamestown		X	
Johnston	X	X	X
Lincoln		X	X
Little Compton		X	X
Middletown	X	X	X
Narragansett		X	X
New Shoreham	X		
Newport			
North Kingstown	X		
North Providence			X
North Smithfield	X		
Pawtucket	X	X	X
Portsmouth	X	X*	X
Providence^	X	X	X
Scituate	X		
Smithfield	X		
South Kingstown^	X		
Tiverton (see below)	X	X	X
Warwick	X		
West Warwick		X	
Westerly	X	X	X
Woonsocket		X	X
TOTAL	**23**	**24**	**23**

^East Greenwich, Exeter-West Greenwich, Providence, and South Kingstown additionally are the only districts which prohibit remote location tracking of a school-loaned device except in instances of theft or loss of the device.
* Access to a school-loaned computer's camera, but not microphone, is explicitly banned
Tiverton School District is currently working with the ACLU of RI to create comprehensive privacy policies.

In the letter that we sent each individual district, there were several key components to an effective privacy policy we asked schools to adopt:

- An outright prohibition on school officials' ability to access the microphone or camera of a school-loaned device except during live teaching activities and with the student and family's full knowledge.
- A ban on accessing the data on a school-loaned device unless (1) a parent or guardian has signed a valid opt-in agreement which allows access by the district to specific and explicitly specified data, or (2) a school official has reasonable suspicion that a student has violated school policy, and data on the device contains evidence of the suspected violation.
- A restriction on remotely tracking the location of any school-loaned computers without cause.

Each of these components are important on their own but are integral for the formation of comprehensive privacy policies.

Remote Access to the Microphone and Camera of School-Loaned Devices

For many students and parents, the assumption that school districts wouldn't indiscriminately access the camera and microphone on a computer may be taken for granted. It should not. Although the ACLU of Rhode Island has not heard from any students or families who have knowingly experienced such an invasion of privacy, a case from the Lower Merion School District in Pennsylvania unfortunately proves that such violations are not hypothetical.

61% of districts have policies which allow remote access to both the camera and microphone of a school-loaned device.

33% of districts have policies which prohibit remote access to the microphone and camera of a school-loaned device.

6% of districts have policies which prohibit access to the camera, but not the microphone, of a school-loaned device.

In 2010, a high-school student named Blake Robbins was confronted by a school administrator who had used surreptitious photos taken through the webcam on his

school-loaned computer as evidence that he was engaging in "improper behavior in his home." After a class action lawsuit was filed alleging that such intrusions violated the Fourth Amendment privacy rights of students, evidence exposed during the case confirmed that the district had taken over 56,000 secret photos of students, including 400 of Robbins alone over a two-week period.[8]

For a school to not explicitly repudiate this authority of access is deeply problematic.

For a school to not explicitly repudiate this authority of access is deeply problematic. No school official should have the right to unilaterally access the contents of these computers or use them to determine what a student may or may not be doing in their private lives. This access especially comes into focus when considered through the lens of the COVID-19 crisis and the necessitated exclusive use of remote learning for a lengthy period of time. A district could inappropriately assume that a reasonable method for monitoring student engagement is through remote webcam monitoring; however, this places both the privacy of the student and their families in jeopardy, as the entirety of education – and activity beyond the school day – is being conducted in a private setting. At the very least, and with consideration for the need that teachers may have to access schoolwork remotely during any type of virtual education, policies should explicitly designate appropriate hours for select types of access which do not extend beyond normal school day hours.

Twelve districts have rightly recognized that their ability to monitor students in an invasive manner cannot and should not extend to the home.[9] The South Kingstown School District, for example, commendably affords students protection from access to the microphone or camera in school-loaned computers, and additionally bans location tracking except in the instance of a device being reported stolen. However, it is important to note that despite providing these critical protections, the school district's policy explicitly states that students have no expectation of privacy in using the devices. This type of mixed messaging is confusing, to say the least, and provides another reason for establishing uniform, comprehensive protections.

[8] http://www.nbcnews.com/id/39631890/ns/technology_and_science-security/t/school-settles-webcam-spy-lawsuits-k/#.XqsR7lNKjOQ ; https://www.nbcphiladelphia.com/news/local/school-spies-on-students-at-home-with-webcams-suit/2138208/

[9] Barrington, Chariho, Exeter-West Greenwich, New Shoreham, Newport, North Kingstown, North Providence, North Smithfield, Scituate, Smithfield, South Kingstown, and Warwick.

South Kingstown School District 1:1 Computer Privacy Policies

The District will not remotely access a District-issued student laptop for the purposes of determining the device's location (unless the device is reported as lost or stolen), nor will the District remotely access a District-issued device's cameras, microphones, or recorders under any circumstance.

With so many other districts failing to ensure that their students are protected from intrusions on school-loaned devices – which have, during the pandemic, become mandated remote learning tools – they are tacitly authorizing the types of privacy invasions unveiled by the *Robbins* case, mentioned above. Until each district passes policies that outright prohibit this type of intrusive conduct, or Rhode Island passes legislation to statutorily ban it, students' and parents' right to privacy will remain at the mercy of individual school officials.

Right to Monitor Content on a School-Loaned Device

Though some districts may compare the ability to inspect or monitor a school-loaned computer and the content it contains to the school's right to inspect a locker, there is a distinct and fundamental divide between inspecting the physical contents of a locker – which always remains on school grounds – and searching a device which, as opposed to physical property, not only is utilized within the private confines of a student's house, but can contain documents, files, or other classic elements of "speech," It is even more concerning – especially in light of emergency situations such as the COVID-19 epidemic – when one recognizes that the devices may often legitimately be used for personal and family purposes. As noted earlier, it is easy to imagine the extremely sensitive and private information that could be found in the contents of a computer used by parents for non-school-related activities.

64% of districts have policies which explicitly note that students have no expectation of privacy on a school-loaned device.

64% of districts have policies which maintain the right for the schools to monitor the content and data of a school-loaned device without limitation.

Nonetheless, 23 school districts maintain the right to monitor the content and data of a device without restriction, and 23 district policies explicitly note that students have no expectation of privacy on a school-loaned device. In authorizing this invasion of student and family privacy and the monitoring of off-campus conduct, these policies raise serious Fourth Amendment concerns. The Cumberland School District's policy, as shown below, exemplifies the types of policies which strip students of their rights in this regard when applied to computers that are being taken home.

Cumberland School Department 1:1 Computer Privacy Policies

CSD retains control, custody and supervision of all computers, networks and Internet services owned or leased by the District. CSD reserves the right to monitor all computers and Internet activity by system users. There is no expectation of privacy in their use of school computers, including e-mail messages and stored files.

Appropriate policies – as we advocated for in the letter sent to each of the state's school districts – would instead limit the instances of remote access to a school-loaned device, outside of teaching activities, to those in which there is a reasonable suspicion that the student has engaged in a violation of school policies or for other properly limited reasons. The Newport Public Schools' school-loaned device policies provide a good model. Their specific policy language is provided below.

Newport Public Schools 1:1 Computer Privacy Policies

Remote access to student devices off campus will be limited to the following:

- *There is reasonable suspicion that the student has engaged in a specified misconduct and their [sic] is reasonable suspicion related to the health and safety of a student*
- *Access is necessary to address technological threats to the school computer system or to update or upgrade the device's software*
- *A warrant will be obtained if the search is designed to look for evidence of criminal activity*
- *The parent has given consent to search on an individualized basis*

A physical search of the contents of a student's device will be limited to the same reasons stated to obtain remote access, or for legitimate educationally related reasons.

THIRD-PARTY SOFTWARE PLATFORMS

The further liberties that third-party software platforms have to control, utilize, and sell student data warrant an additional layer of student privacy protections which are often left unaddressed.

Although a school official's ability to remotely access student information through a school-loaned computer is a major concern, the further liberties that third-party software platforms have to control, utilize, and sell student data warrant an additional layer of student privacy protections which are often left unaddressed.

A Rhode Island statute comprehensively and appropriately prevents any student data, whether deidentified or not, that is gathered in the process of any academic work or educational activity from being used for any commercial purpose, including marketing.[10] The law further mandates that any district engaging with a third-party platform for the purpose of providing a cloud-computing service to students must enter into a contract which guarantees that the platform will conform with the statute's requirements. Though the law is clear, contracts for the disparate programs that districts use inconsistently address the confidentiality requirements established within the statute.

For example, sixteen school districts participate in a consortium called the Rhode Island Student Privacy Alliance (RISPA),[11] which operates with the intent to "set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations."[12] RISPA's model privacy agreement, however, does not explicitly reference the state statute governing the acceptable uses of student data, despite this statute specifically prescribing a need for this in any such agreement. Further, the model agreement, while

[10] Rhode Island General Laws §16-104-1.
[11] Bristol-Warren, Burrillville, Coventry, Cumberland, Exeter-West Greenwich, Jamestown, Little Compton, Middletown, Narragansett, North Kingstown, Portsmouth, Smithfield, South Kingstown, Tiverton, Warwick, Woonsocket.
[12] https://sdpc.a4l.org/about_alliance.php? state=RI

following many of the tenets of the student data privacy statute, allows a school or Local Education Authority (LEA), such as a school district, to consent in writing to the sale of student data.[13]

Positively, however, the agreement does provide for deletion of student data when it is no longer needed for the purpose for which it was obtained, and requires any program contracting with an LEA to specify precisely which student data is being collected. While the agreement also mirrors language within the statute that strictly prohibits the use of student data for commercial purposes, this prohibition appears to be in some tension with the language giving LEAs the ability to otherwise consent to the sale of student data.

Tech companies should not have the ability to utilize the data of students for their own financial gain

The concern with these types of third-party platforms is multilayered. First, if districts are not following through with their statutory obligation to procure written agreements, third-party platforms may be using student data for their own gain in ways that are illegal under this law, as this statute expressly prohibits use of student data for any commercial purpose. Regardless, tech companies should not have the ability to utilize the data of students – especially those who are minors and going through the public school system – for their own financial gain. Finally, and even more disturbingly, these programs may access the contents of not only school-loaned computers, but also *private family computers* in unprecedented and wholly inappropriate ways if the programs have been downloaded for use on a home computer.

The use and breadth of third-party platforms certainly have become more common in the emergency transition to virtual learning and the widespread use of electronics in public schooling. The promises of what these platforms can provide to teachers and students are compelling on the surface, but the potential implications are much more sinister than the simple ability for teachers to check up on their students' progress and have access to their screen-time and work habits.

[13] Article II, Section 4 on page 2 of the model data privacy agreement notes that "the provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, *without the express written consent of the LEA* or without a court order or lawfully issued subpoena." (emphasis added)

One particular platform that had cropped up in specific districts' virtual learning plans, or which we have heard anecdotally is being used by teachers, is Go Guardian, a learning platform hosted by Google which provides teachers and administrators with truly invasive remote capabilities, including a thirty-day lookback period for browser history and real-time access to the activities being performed on a computer. Although this is problematic when instituted on a school-loaned device, it becomes increasingly concerning when such programs are activated on family-owned devices or computers. There are many sensitive pieces of information that a parent, guardian, or student may be transmitting on a private computer, and broadening access to such devices when used for remote learning can only endanger the privacy of a student and their family.

Because the ACLU of Rhode Island was cognizant of the rapidly expanding use of such platforms, our April letter to school districts asked them to do the following in the course of their remote learning and remote education plan implementations:

- Disable privacy-invasive features on any third-party programs that students are required to download in order to participate in virtual learning.
- Ensure that any third-party programs used in the course of remote education are in compliance with the state's data-cloud computing privacy law, §16-104-1.

HOW DO WE ENSURE BETTER PRIVACY PROTECTIONS FOR STUDENTS?

The initiative to provide better privacy protections for students can come from two separate bodies that oversee school policies – individual school committees and the Rhode Island General Assembly, which can create a set of uniform privacy guidelines that each district must follow.[14]

The ACLU of Rhode Island has been advocating for both of these efforts. To ensure that each student in Rhode Island is guaranteed the same level of protections, statewide legislation that comprehensively addresses the standards that should be contained in districts' policies is critical. However, the onset of the COVID-19 crisis and the temporary closure of the legislative session in 2020 prompted the letters which the ACLU sent to every district, asking them to independently promulgate policies that would protect student privacy in light of the emergency transition to virtual learning. However these standards are implemented, and whether students are on school property or engaging in education at home, the time for school districts to act is now.

The following requirements should be codified in the policies for each school district as the new school year starts, and enacted into law at the next legislative session:

Prohibit Remote Access to Cameras, Microphones, and Recorders

- School districts, and any third parties, should be prohibited from activating or remotely accessing the camera, microphones, and recording functions in any devices in the hands of students when they are not in school 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; or access is necessary to respond to an imminent safety threat.

[14] A third option would be for the Rhode Island Department of Education (RIDE) to establish a uniform set of regulations for all school districts to follow. Due to the agency's preoccupation with many other matters relating to the pandemic and our historic experience with RIDE's wariness in promulgating statewide regulations, we consider this alternative a less likely one.

Restrict Other Remote Access to School-Loaned Devices

- School districts and third parties should be prohibited from otherwise remotely accessing students' devices unless:
    - There is documented, reasonable suspicion that the student has engaged in specified misconduct, 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 for a search designed to look for evidence of criminal activity; or
    - 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 safety threat.

Provide Strict and Specific Standards for the Searching of a School-Loaned Device

- A school district should not physically search the contents of a student's device except pursuant to the allowable standards in place for remote access, or for legitimate academic or educationally related purposes.
- The browser, keystroke, or location history of a device should not be accessed in the absence of reasonable suspicion of a violation of a privacy-sensitive school policy or for technological purposes.
- Any type of misconduct which could lead to a search should be detailed within the school district policy.
- Policies should specify which school officials have the authority to search a school-loaned device, remotely or otherwise.

CONCLUSION

As this report is being finalized, the COVID-19 pandemic has continued to surge across the country. Though Rhode Island has set forth a plan to have all students back in school full-time by mid-October, transition to virtual learning remains the backup plan if schools simply become too unsafe for students and their families. Regardless, the school-loaned devices are certain to be an educational platform which is utilized for years to come.

With the degree of uncertainty that the pandemic has caused, the need to protect privacy rights for students has never been more salient. Without a concrete, comprehensive plan for reintroducing students to the physical school environment, ensuring their privacy in the virtual one must be a top priority. This will take place by guaranteeing a reasonable expectation of privacy through the actual devices that students are using to perform and complete their schoolwork, meet with their teachers, and store their information on.

Though districts should be taking steps to individually implement these privacy measures, it is of tantamount importance, during such a tumultuous and vulnerable time, that the General Assembly also prioritize legislation to codify comprehensive privacy protections for students. When so much is at risk, students and their families should be assured that their privacy, and the privacy of their personal information and data, are not victims of the widespread use of school-loaned devices.[15]

[15] This report was prepared by ACLU of RI Policy Associate Hannah Stern.

APPENDIX A

ACLU
AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

April 10, 2020

Superintendent Michael Messore
Barrington Public Schools
283 County Road
PO Box 95
Barrington, RI 02806

VIA MAIL AND EMAIL

Dear Superintendent Messore,

In the wake of the recent, and indefinite, school closures in Rhode Island, emergency steps have appropriately been taken to accommodate remote learning for all public school students. Since school-loaned devices, such as Chromebooks, and third-party programs that facilitate online learning are being used for virtual education in most districts, we are writing to ask – if you have not already done so – that you take prompt action to protect the privacy rights of students and families making use of these devices and platforms.

The ACLU of Rhode Island has, for several years, expressed concerns about school district policies that give officials broad and fairly indiscriminate abilities to remotely access school-loaned devices while in students' hands at home. It is additionally of importance to note the substantial invasions of privacy that can occur when third-party programs are installed on personal family computers as well. For example, a program like Go Guardian – which we understand is being used by some school districts – not only provides real-time access to a student's computer, but can allow school personnel to examine weeks of web history and data on the computer, which could include the private browsing history of the student's parents. The emergency transition to fully remote education heightens the acute need for districts to take steps to preserve student privacy in both of these capacities.

When the ACLU of RI surveyed school districts three years ago on their policies governing home use of such devices, we were troubled to find that almost every district authorized wholesale access to the laptop's content – including files, photos, and web history – at any time and for any reason, even when families were encouraged to use the computers for non-academic purposes. Even more ominously, the authorization rarely barred school access to, and activation of, the device's microphone and camera.

In February of this year, as you know, we filed a follow-up open records request to determine if those policies had changed at all in order to provide students and their families with much-needed privacy protections. Although your district has yet to respond to this most recent request, the response to our inquiry from 2017 revealed that the policies for such programs for Barrington Public Schools indicated that students should have no expectation of privacy, that the district maintains the right to remote access of the device, and that the school retains the right to inspect the device at any time and for any reason.

Although we did not inquire into whether your district utilizes remote teaching platforms such as Go Guardian – and we recognize that any usage of such platforms may only be in response to the current closures and public health crisis – it is additionally important for your district to disable any features that intrusively authorize access to information beyond what is necessary for classwork.

Given the ongoing nature of the school closures, and the need to balance both the administration of reliable educational services and the maintenance of student privacy while classes are conducted outside of school, we therefore urge you to immediately adopt privacy protections regarding at-home computer use, and make students and parents aware of those protections. They should include the following:

- An outright prohibition on school officials' ability to access the microphone or camera of a school-loaned device except during live teaching activities and with the student and family's full knowledge.
- A ban on accessing the data on a school-loaned device unless (1) a parent or guardian has signed a valid opt-in agreement which allows access by the district to specific and explicitly specified data, or (2) a school official has reasonable suspicion that a student has violated school policy, and data on the device contains evidence of the suspected violation.
- A restriction on remotely tracking the location of a school-loaned device without cause.
- Disabling privacy-invasive features on any third-party programs that students are required to download in order to participate in virtual learning.
- Ensuring that any third-party programs used in the course of remote education are in compliance with the state's data-cloud computing privacy law, §16-104-1.

Since the implementation of school-loaned device programs, the ACLU of RI has been approached by many parents who felt uncomfortable with signing away their child's privacy rights but were given no other option for engagement in the important educational activities taking place with them. Now that students, and their parents and guardians, have no other option but to continue their education through such devices – and, on occasion, utilize their home computers for this learning – we believe it is imperative that the privacy rights of students be protected. Clear standards on access to the visual and audio components of the computers – whether school-loaned or personal – are essential. Also of tantamount importance is ensuring that platforms such as Go Guardian do not expose sensitive information about students and their families to school staff, and that the usage of such platforms does not unintentionally facilitate the ability for school staff to access more data than they need to complete their job responsibilities.

We hope that you agree, and we ask that you advise us of any action you plan to take to address these consequential privacy concerns. The ACLU of Rhode Island would be happy to assist in the drafting of procedures or policies that promote this important goal, and we look forward to hearing back from you. Thank you for your consideration.

Sincerely,

Steven Brown
Executive Director

Hannah Stern
Policy Associate