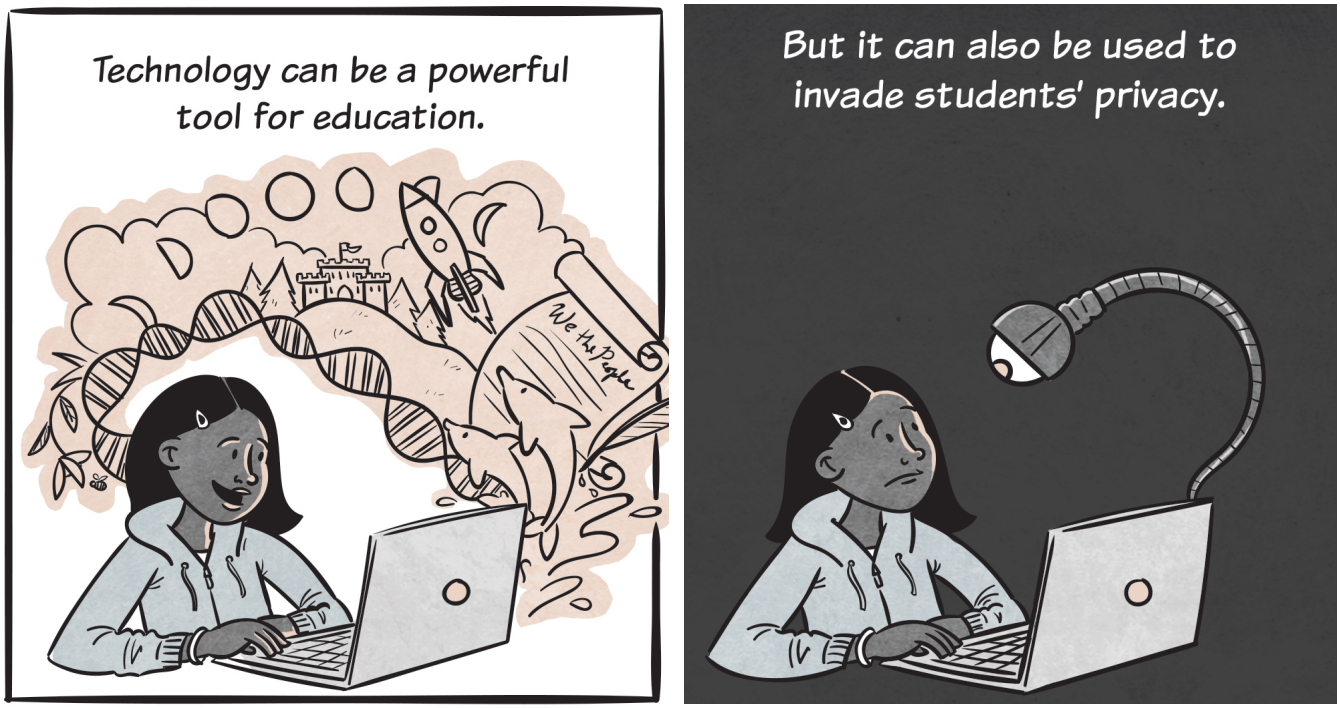
Back to the Drawing Board:

Student Privacy in Massachusetts K-12 Schools
Executive Summary and Recommendations



Art by Hallie Jay Pope

ACLU FOUNDATION
AMERICAN CIVIL LIBERTIES UNION of MASSACHUSETTS

STUDENT PRIVACY IS ABOUT CONTROL, NOT SECRECY

It seems like a matter of common sense—and common decency—that teachers and school administrators wouldn't use technology to spy on students. But consider the events that took place in Lower Merion School District just a few years ago. At the start of the 2009-2010 school year, this Pennsylvania school district gave students MacBooks loaded with spyware without telling the students or their parents. The school used this spyware to capture thousands webcam images, screenshots, and personal communications from at least two students.[1]

The two students and their parents sued, and a few months later the district settled for $610,000.[2] More allegations came out during the suit, including that the district had captured images of students partially undressed[3] and that administrators had lied to students about the capabilities of the software.[4] In Merion, student privacy was violated, the community's trust in the school system was shaken, and the town's coffers lost more than half a million dollars.

We don't want something like this to happen in Massachusetts. That's why ACLUM is calling for strong privacy policies, complete transparency with parents and students, and robust community engagement on digital student privacy issues *before* something like the Pennsylvania spying incident occurs here.

Schools in Massachusetts and across the United States are using digital technologies—from student information systems to surveillance cameras—to monitor, track, and assess student progress, behavior, and development. These technologies collect large amounts of sensitive student information and should be governed by thoughtful, transparent policies that take into account the interests and desires of students and parents. As we found when we surveyed Massachusetts schools, however, this is often not the case.

EXECUTIVE SUMMARY

To learn about the current state of digital privacy in Massachusetts schools, the ACLU of Massachusetts filed public records requests with thirty-five school districts across the state, selecting a diverse group of districts from Boston to Springfield representing communities in cities, rural areas, and suburbs, including charter schools. Twenty-nine districts provided records. Below is a summary of what we learned. Unless otherwise noted, these findings reflect school policies and programs as of the 2014-2015 academic school year.

- **COMPLIANCE WITH PUBLIC RECORDS LAW**—In preparation for this report, the ACLU filed thirty-seven public records requests with thirty-five school districts. Twenty-nine districts provided records, although Newton only provided very limited documentation without a fee, and demanded $5,834 in fees to provide the remaining responsive documents. Six districts provided no records. Barnstable, Lynnfield, and Pittsfield effectively ignored our requests, while Lexington and Waltham demanded exorbitant fees ranging from $1,020 to $2,200. The Prospect Hill Academy Charter School promised to provide records after a contract with a private vendor had been finalized, but as of the publication of this report, we had not yet received them.

- **PRIVACY LAW AND PARENTAL CONSENT**— The Family Educational Rights and Privacy Act (FERPA) and accompanying regulations establish federal baseline rules for student privacy. These rules were recently weakened and now contain many exceptions allowing schools to share student data without parental consent in a variety of situations. Massachusetts student privacy regulations also provide protections for student privacy. While they aim to protect student privacy by generally preventing nonconsensual access to student records by any individual other than "authorized school personnel," these state regulations were last updated in 2006. In light of the widespread use of third party applications to manage student information and the proliferation of technology in the classroom, these regulations must be clarified and expanded in order to adequately achieve their stated goal of protecting student and parent confidentiality.

- **SHARING WITH PRIVATE COMPANIES**—Student information systems make it easy for schools to share sensitive student records, including disciplinary information and immigration status, with third-party corporations. Out of eighteen districts to which we sent this specific request, only one—the Mystic Valley Charter School—reported that it does not share student information with private vendors.

- **CONTRACTS WITH CORPORATIONS**—Schools that drafted their own contract terms with private corporations generally offered superior protections than schools that signed contracts written by private vendors. In response to our requests, Brockton and Worcester disclosed district-written contracts providing greater privacy protections for students than most company-drafted contracts.

- **MANY SURVEILLANCE CAMERAS BUT FEW POLICIES**—All of the fourteen responsive districts we asked about in-school physical surveillance use cameras. But only one district—Newton—provided a written surveillance camera policy in response to our records requests. At the time of our request, at least four responsive schools—Boston, Holyoke, Duxbury, and Springfield—used cameras with no policy, and eight either claimed to have a policy but did not disclose it or were silent on the question. The remaining school, Lynn, did not provide a policy in response to our request, but it was available on the district's website. Nine months after our request, Holyoke adopted a camera policy.[16]

- **SPYWARE AND MONITORING**—Many Massachusetts schools issue students laptops or iPads through "1:1" or school-controlled technology programs. These devices can be distributed pre-loaded with spyware enabling administrators to access extremely sensitive student information. At least eight districts use off-campus filtering or monitoring software.[17] Of these, at least four—Auburn, Natick, Wayland, and West Springfield—use off-campus filtering that also enables the tracking of permissible Internet activity.

  The most invasive monitoring software we saw was disclosed to us by West Springfield. As of April 2015, its GoGuardian Chromebook application allowed real-time and historical activity tracking and screen monitoring, location tracking, keystroke logging, and even the remote activation of webcams. Despite these powerful capabilities, West Springfield's policies simply note that activities may be monitored and do not disclose that the school uses GoGuardian on the Chromebooks the district provides to students. On October 27, 2015, the day before the publication of this report, GoGuardian called the ACLU to tell us that they "heard through the grapevine" that the ACLU was about to publish a report that would discuss GoGuardian. The company informed us that its software no longer enables webcam monitoring or keylogging. We asked the company for the specific date on which they made this change; as of the publication of this report, they have not responded. According to Google cache, however, some time between October 23, 2015 and October 28, 2015, GoGuardian added the following language to its website: "As part of our ongoing commitment to student privacy, GoGuardian no longer enables keystroke logging and remote activation of the webcam."

- **"NO EXPECTATION OF PRIVACY" IN DEVICES**—Two-thirds of the districts that produced a document discussing administrator or teacher access to school-controlled devices—ten out of fourteen districts—reserve the right to search or inspect them without notice or consent. Eight districts (Bedford, Burlington, Douglas, Franklin, Hopkinton, Methuen, Sudbury, and West Springfield) state that students have "no expectation of privacy" in their school-controlled devices, and two (Millis, and West Springfield) specifically allow random or periodic searches. Only Uxbridge produced a written policy limiting device searches to physical searches "when a problem is brought to the attention of the building administration."

- **"NO EXPECTATION OF PRIVACY" ONLINE**—Districts almost universally claim that students do not have an expectation of privacy when using school networks. Revere and Salem disclosed records stating that students could not expect their in-school Internet activities to be private. Methuen, Sudbury, and Wayland reserve the right to monitor student Internet use on school networks without notice or consent. Auburn, Bedford, Burlington, Douglas, Duxbury, Hopkinton, Lawrence, Millis, Uxbridge and Shrewsbury all state that students do not have a right to privacy in their Internet use *and* reserve the right to monitor Internet use absent notice or consent. Four districts—Auburn, Bedford, Hopkinton, and Wayland—affirmatively retain the right to share with the police any information obtained over school networks.

- **CORPORATE APPS FOR EDUCATION**—About half of the twenty-eight districts that provided records for this report use Google Apps for Education. In five districts, obtaining a Google account is required to participate in school-controlled technology programs (Douglas, Franklin, Hopkinton, Natick, and Sudbury). For years, Google was mining student accounts for targeted advertising purposes. The company said it stopped the practice in 2014 after a class action lawsuit.[18] Some districts reported using other types of software. Shrewsbury, for example, uses a product called MyHomework, which tracks schedules and homework assignments. The district pays for an upgraded version of the software; the "free" option serves students advertisements.

RECOMMENDATIONS

Ultimately, decisions that impact student privacy should be part of a public conversation, with robust participation from students, parents, and teachers at its heart. Remember, privacy isn't secrecy. Privacy is control over information about oneself. In order to ensure students and parents have control over their lives, their interests and voices should be at the center of policy development pertaining to student information in the 21st century. The following recommendations provide a basic roadmap for those conversations.

STUDENTS: Practice digital self-defense and understand school policies

The ACLU is working to strengthen legal protections for your privacy. In the meantime, here are some things you can do right away to protect your own information:

- Never use school-controlled devices for personal communications, including social media. If you do, be aware that your school might reserve the right to monitor them.
- Always cover webcams when not in use—you can use a post-it note in a pinch.
- Ask your school to disable any location tracking or network monitoring software on your device.
- Ask administrators for the privacy policies for any software your school offers or requires you use.
- Take note of whether the policies allow school officials to keep track of which websites you visit, and if they allow the school to share your private information with companies.
- Request a copy of your student records, so you can see what personal information school officials—and potentially private companies—have access to.

PARENTS: Ask school administrators for basic transparency; policy and technology details to look for

At the beginning of every school year, ask your child's school administration the following questions:

- What are the privacy policies for student email, computer, and/or tablet use?
- What software is installed on school-controlled technologies my child uses? Who can access data under what circumstances?
- Do you have policies about how student information is shared with third parties? Can we opt out of some disclo-

sures? If so, how?
- Does the school have policies about who can see surveillance camera footage and in what circumstances?
- What is the school's policy for contacting police to conduct searches or administer discipline?

When you receive policies or other records from your child's school, pay close attention to issues related to parental knowledge and consent. Federal and state student privacy regulations are floors, not ceilings. The following are standards the ACLU believes parents should encourage administrators to adopt to better protect student privacy while the state legislature considers proposals for modernizing the law:

- ***Consent requirements for all disclosures of student information:*** The right to privacy is the right to control your personal information. You should be notified before your or your child's personal information is shared with another entity. Your district should share personal information only with your consent, unless the school is legally required to make the information available to a third party.

- ***Public lists of all releases of student data and software applications:*** You need to know if your child's privacy is at risk. School districts should publicly post all contracts, agreements, and terms of service that grant third-party access to student data. Your district should also provide a complete list of all software installed on school-controlled devices and an explanation of how each application uses student data. These lists should be updated at least once a year.

- ***Clear policies on surveillance:*** The government should not be collecting information about your child without your knowledge. Your district should have a publicly available, written policy for all forms of student surveillance. This policy should, at a minimum, specify what technologies are being used, who has access to surveillance records, how long they are retained, when they are shared with law enforcement, and how students can get access to their own records to challenge disciplinary or legal proceedings. Your school should also require student or parent consent before activating location tracking, keylogging, or remote webcam access on any school-controlled device.

ADMINISTRATORS: Adopt best practices for technology acquisitions and policies

Teachers, administrators, and local school board officials have the power to protect student privacy while instilling a strong sense of civic responsibility in youth. Starting today, administrators can do the following to strengthen their student privacy practices while the state legislature considers proposals for modernizing the law:

- ***Be smart when choosing technologies:*** You'll be making decisions about what technologies to use in your classroom, school, and district—you have a responsibility to make choices that support student privacy. Only use software with privacy policies that ban all use of student data for advertising. Make sure that all vendors' privacy policies conform to FERPA, the Massachusetts student records regulations, and privacy best practices.[19] The law is the floor for student privacy, but it shouldn't be the ceiling.

- ***Respect privacy with your search policies:*** Every search of a student's belongings, including school-controlled devices, should require a reasonable suspicion that a student has violated a school policy. If you suspect a student has violated the law, the search should require probable cause.[20] Police involvement should be a last resort, and should take place only if there is probable cause to believe a student violated the law. Administrators should document each digital search, and provide immediate notification to parents including the reason for the search and any information sought and/or seized.

- ***Get the community involved:*** In a democratic government, public participation is key to formulating good policy. All policies implicating student privacy—including those governing student records, searches and other surveillance, and EdTech partnerships—should be adopted in public meetings, with student and parent feedback. Engaging in this public process is a great opportunity to promote transparency, accountability, and privacy while teaching students about the importance of democratic process.

When communicating with parents about digital privacy matters impacting their childrens' information, consider these best practices:

—Describe the relevant law in plain language.
—Distinguish between mandatory and optional disclosures.
—Notify students and parents of their right to challenge mandatory disclosures.
—Describe the process for opting out of optional disclosures and for consenting to partial disclosures without opening an entire student record.

When drafting contracts with private vendors, consider these best practices:

—Write the contract in-house—do not rely on company-provided language.
—Limit the use of student data to the purpose described in the contract.
—Prohibit third parties from re-disclosing or selling student data to any other entity.
—Require deletion of all student data upon termination of the contract.

LEGISLATORS: Pass comprehensive 21st century student privacy law

Students and parents can advocate for strong privacy protections, and local officials can implement them on a district-by-district basis, but legislators are best positioned to enact statewide reforms. You can help by making student privacy a legislative priority.

As we describe in this report, although the Massachusetts student privacy regulations explicitly aim to protect student and parent confidentiality, they need to be clarified and expanded in light of revolutionary technological change.

Fortunately, state legislatures across the nation have recognized that need. According to the National Association of State Boards of Education, in the first six months of 2015 "47 state legislatures introduced more than 180 [student data privacy] bills in total."[21] California passed a student data privacy law in 2014,[22] with sixteen states[23] following suit in 2015.[24] California's law, among others, prohibits companies from selling student data or using it for advertising and profiling purposes. In Congress, Massachusetts' own Senator Ed Markey, along with Utah Senator Orrin Hatch, reintroduced the Protecting Student Privacy Act, a bill aimed at increasing transparency and limiting advertising in the EdTech sector.[25]

Massachusetts must join the movement to advance student privacy in the digital 21st century by passing a comprehensive new student privacy law that protects youth privacy in the Information Age.

1 Muskus, Jeff. "Lower Merion School District Settles Webcam Spying Lawsuits For $610,000." *The Huffington Post*. TheHuffingtonPost.com. Web. 22 Sept. 2015 See http://www.huffingtonpost.com/2010/10/11/lower-merion-school-distr_n_758882.html.

2 Martin, John. "Lower Merion District's Laptop Saga Ends with $610,000 Settlement." Philly.com. 12 Oct. 2010. Web. 22 Sept. 2015. <http://articles.philly.com/2010-10-12/news/24981536_1_laptop-students-district-several-million-dollars>.

3 Martin, John. "Lawyer: Laptops Took Thousands of Images." Philly.com. Web. 22 Sept. 2015. <http://www.philly.com/philly/news/year-in-review/20100415_Lawyer__Laptops_took_thousands_of_photos.html>.

4 Keizer, Gregg. "Report Blames IT Staff for School Webcam 'spying' Mess." Computerworld. Web. 22 Sept. 2015. <http://www.computerworld.com/article/2517968/data-privacy/report-blames-it-staff-for-school-webcam--spying--mess.html>.

5 Some filtering software can also be used to create a record of permissible Internet activity.

6 http://www.hps.holyoke.ma.us/pdf/sc_agendas/Full%20Board%209-14-15.pdf.

7 Williams, Lauren. "Under Pressure Of Lawsuits, Google Says It Will Stop Reading Students' Emails (Updated)." ThinkProgress. 30 Apr. 2014. Web. 23 Sept. 2015. <http://thinkprogress.org/justice/2014/04/30/3432582/google-scans-students-gmail>.

8 The Organization for Economic Cooperation and Development (OECD) offers eight privacy principles that constitute an excellent reference point for the development or interrogation of any data-sharing program or policy. Find the OECD privacy principles at http://www.oecd.org.

9 Under the Fourth Amendment to the United States Constitution, the government may only search someone's personal belongings if they show a judge probable cause to believe that evidence returned in the search will be evidence of a specific, suspected crime. This is the gold standard of American justice and should apply in schools.

10 National Association of State Boards of Education, Policy Update, Trends in State Legislation on Student Data, June 2015. http://www.nasbe.org/wp-content/uploads/NASBE-Policy-update-2015-legislative-session-data-privacy_-June-2015.pdf.

11 "EPIC - State Student Privacy Policy." EPIC - State Student Privacy Policy. Web. 23 Sept. 2015. <https://epic.org/state-policy/student-privacy>.

12 National Association of State Boards of Education, Policy Update, Trends in State Legislation on Student Data, June 2015. http://www.nasbe.org/wp-content/uploads/NASBE-Policy-update-2015-legislative-session-data-privacy_-June-2015.pdf.

13 "New Hampshire and Oregon Pass Student Privacy Laws." Practical Law. Web. 23 Sept. 2015. <http://us.practicallaw.com/8-616-6448>.

14 Sens. Markey & Hatch Reintroduce Bipartisan Legislation to Protect Student Privacy." Senator Ed Markey. 13 May 2015. Web. 23 Sept. 2015. <http://www.markey.senate.gov/news/press-releases/sens-markey-and-hatch-reintroduce-bipartisan-legislation-to-protect-student-privacy


ACLU
AMERICAN CIVIL LIBERTIES UNION
of MASSACHUSETTS
FOUNDATION