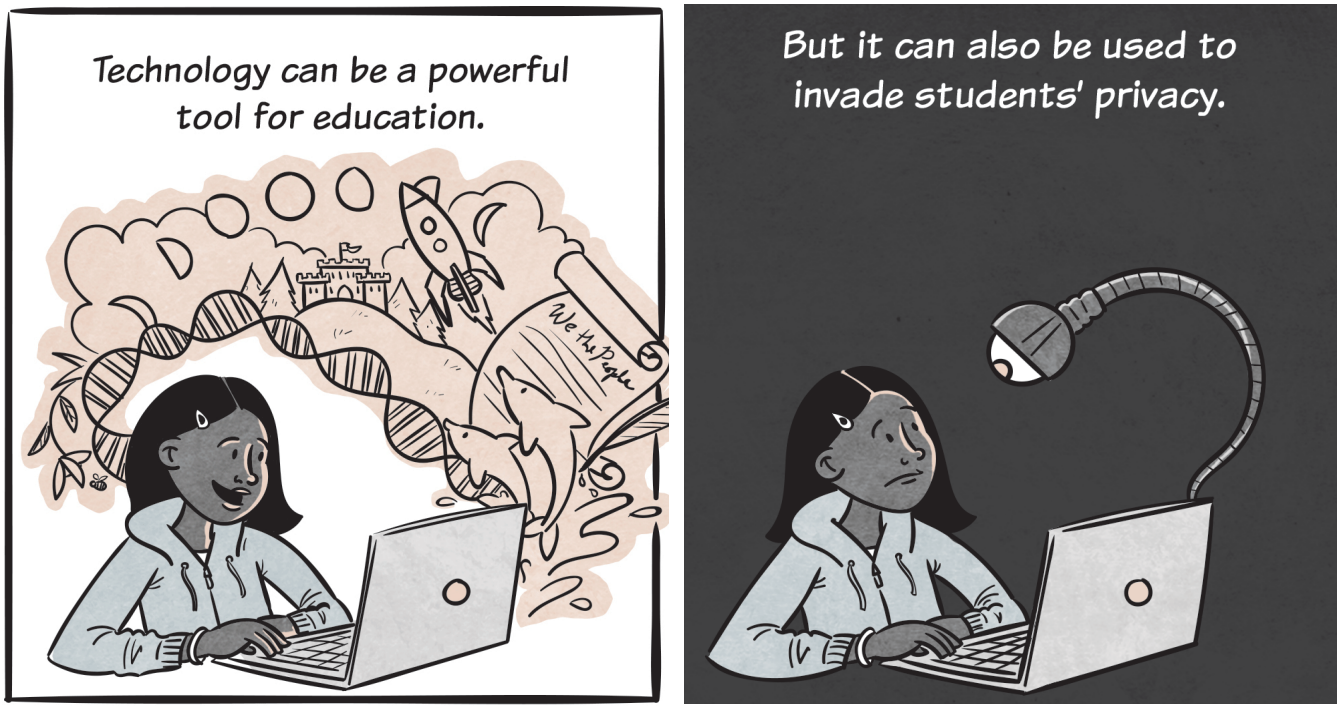
Back to the Drawing Board:

Student Privacy in Massachusetts K-12 Schools



Art by Hallie Jay Pope

ACLU FOUNDATION
AMERICAN CIVIL LIBERTIES UNION of MASSACHUSETTS

Staff from the ACLU Foundation of Massachusetts compiled this report.

Authors:
Kade Crockford, director, Technology for Liberty Program
Jessie J. Rossman, staff attorney

Press date: October 28, 2015

American Civil Liberties Union Foundation of Massachusetts
211 Congress Street
Boston, MA 02110
617-482-3170 x344
www.aclum.org

THANK YOU to the following people, without whom this report never would have seen the light of day:

Margaret A. Hazuka
Ariel G.E. Kong
Brandon Levey
Nancy MacDonald
Hallie Jay Pope
Raquel Ronzone

TABLE OF CONTENTS

I. INTRODUCTION: 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]

> Privacy does not mean total secrecy. Rather, privacy means having control over your personal information—the right to decide "when, how, and to what extent information about [you] is communicated."[5]

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 the ACLU of Massachusetts is calling for strong privacy policies, transparency with parents and students, and robust community engagement on digital student privacy issues before something like the Pennsylvania spying incident occurs here.

Privacy does not mean total secrecy. Rather, privacy means having control over your personal information—the right to decide "when, how, and to what extent information about [you] is communicated."[5] Control over the details of your personal life is critical to the right of personal autonomy.[6] Privacy also implicates basic rights of speech and association guaranteed in the U.S. Constitution,[7] as well as due process and liberty rights—what the former Supreme Court Justice Louis D. Brandeis referred to as "the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men."[8]

A 2015 study by the Future of Privacy Forum found that 87% of parents surveyed "worry about student data being hacked or stolen," while 68% are concerned "that an electronic record would be used in the future against their child by a college or an employer."[15]

In the context of schools, privacy has special importance. Personal information is a valuable commodity[9] for corporations wishing to target students and schools for advertising. By one estimate, the K-12 student software market is an $8 billion industry.[10] When for-profit corporations stand to make or lose that much money, what's best for public school children—including their privacy—can get left behind.

Government invasions of student privacy also produce serious consequences for young people. Student information—including detailed health, behavioral and disciplinary data—can be used to profile students, potentially forcing them into educational or disciplinary programs that may be inappropriate.[11] Even more alarming, when student information is disclosed to law enforcement officers without appropriate safeguards, students may become entangled in the criminal justice system.[12] Invasions of student privacy therefore have both immediate and long-term, life-altering consequences for youth.

Privacy also plays a central role in intellectual development.[13] Privacy lets people ask questions and test ideas that they might not be comfortable sharing with unknown parties. This is especially pertinent for students in K-12 schools, where young people develop intellectually and personally. Without protections for student privacy, schools risk stunting this development and creating a culture of conformity.

For these reasons, student privacy is critically important to parents. Surveys of American adults with children in primary schools show that parents are very concerned about their students' online privacy. A 2012 survey, for example, found that 93% of American parents with children in grades 1-12 reported being "somewhat uncomfortable" or "very uncomfortable" with advertising companies tracking student Internet use in schools.[14] A 2015 study by the Future of Privacy Forum found that 87% of parents surveyed "worry about student data being hacked or stolen," while 68% are concerned "that an electronic record would be used in the future against their child by a college or an employer."[15]

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 and regulations, and take into account the interests of students and parents. As we found when we surveyed Massachusetts schools, however, this is often not the case.

II. 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. Here is what we learned:

- **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.

III. 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 disclosures? 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.

IV. METHODOLOGY & A CALL TO REFORM THE MASSACHUSETTS PUBLIC RECORDS LAW

Our primary research was conducted through two sets of requests for information under the Massachusetts public records law, G.L. c. 66 § 10. We also examined school websites to compare the data we received through public records requests to the information a student or parent would be able to access online.[26] Unless otherwise noted, the findings in this report reflect school policies and programs as of the 2014-2015 academic school year.

The first records request focused on student information systems, or "SIS", which are applications designed to store information about individually identifiable students in a searchable and sharable format. We asked for records pertaining to the use of SIS; contracts or agreements permitting the release of student records; and policies governing access to student records, physical surveillance systems, and student email accounts. We sent this request to eighteen schools across the state, choosing a diverse mix of size, location, and demographics.[27]

The second request focused on school-controlled technologies, namely, laptops or tablets that are issued to students by the school under what are sometimes called "1:1 programs." We asked for purchase orders; lists of installed software; and policies for distributing, managing, and inspecting the devices, among other records. We sent this request to the nineteen districts that we knew—through open source research—offered school-controlled technology programs.[28]

Newton demanded $5,834 to produce all but a few records; Lexington asked for approximately $2,200; and Waltham estimated the cost would be between $1,020 and $1,360, plus the cost of making copies.

In total, we sent thirty-seven requests to thirty-five school districts in Massachusetts.[29] Nearly half the schools we contacted (fifteen) produced records within a month.[30] Another thirteen schools produced records over the following six months.[31] Twenty-four of these districts stated that they were producing all responsive records at no cost, and four charged costs ranging from $48.00 to about $200.00. In total, the responding districts gave us over 2,000 pages of documents, plus numerous links to web resources and student-parent handbooks. The Newton school district responded with a few pages from its student handbook, but requested thousands of dollars to produce internal records. The other six districts either failed to respond or requested prohibitively high costs.

While we were disappointed that numerous districts denied our requests, the denials tell an important story about the state of transparency in Massachusetts. Despite multiple contacts, Barnstable, Lynnfield, and Pittsfield never produced records in response to our requests. Newton demanded $5,834 to produce all but a few records; Lexington asked for approximately $2,200; and Waltham estimated the cost would be between $1,020 and $1,360, plus the cost of making copies. While we were interested to learn how these districts handle student privacy, we did not have the resources to meet these demands. The last school, Prospect Hill Academy Charter School, informed us in December 2014 that they were migrating to the Pearson PowerSchool student information system and would produce records when the contracts were finalized and the migration was complete. As of the publication of this report, we still have not received them.

How could these schools charge so much money for records, or ignore our requests for information? The Massachusetts public records law is among the weakest in the nation. Under Massachusetts law, government agencies – including school districts – face no real penalties for ignoring public records requests. Even if they do respond, agencies can charge almost any price they want to cover the "cost" of preparing the records. If you don't like it, you can sue, but you'll have to pay either way—Massachusetts is one of only three states where you have no opportunity to recoup your attorneys' fees even if you win a public records lawsuit.[32]

Right now, non-profits, reporters, and members of the public have to rely on agencies to act in good faith to disclose public records. While we were fortunate that many schools responded to our request promptly and without charging exorbitant fees, this "hope for the best" model isn't workable in an open society. That's why ACLUM and the Massachusetts Freedom of Information Alliance are working to fix our broken public

records law. Learn more and get involved at https://www.aclum.org/public-records.

V. UNDERSTANDING STUDENT PRIVACY LAW IN MASSACHUSETTS

The Massachusetts public records law is among the weakest in the nation. Under Massachusetts law, government agencies – including school districts – face no real penalties for ignoring public records requests.

Currently, there are two major laws protecting student information in Massachusetts: the federal Family Educational Rights and Privacy Act ("FERPA") and accompanying regulations, and the Massachusetts student records regulations.

FERPA generally prohibits schools from disclosing personally identifiable student information without parental consent.[33] But there are two large loopholes. First, schools can disclose student data to any entity designated as a "school official." FERPA gives schools a lot of leeway to decide who is a "school official,"[34] and service providers like Google have used this provision to obtain access to student data.[35] Second, the U.S. Department of Education recently reinterpreted FERPA to give private companies even more access to student information by allowing schools to designate them as "authorized representatives" that can take over various school functions, including information technology functions.[36]

The Massachusetts regulations prevent access to student records by any individual other than "authorized school personnel" without informed, written consent from the student or parent except in a limited number of circumstances.[37] There are three categories of "authorized school personnel." The first are individuals "working directly with the student in an administrative, teaching, counseling, and/or diagnostic capacity."[38] The second are "administrative office staff and clerical personnel, including operators of data processing equipment or equipment that produces microfilm/microfiche, who are either employed by the school committee or are employed under a school committee service contract, and whose duties require them to have access to records for purposes of processing information for the student record."[39] The third are individuals who evaluate students for special education services.[40]

Massachusetts student information is protected by both FERPA and Massachusetts state regulations. Unlike federal regulators, Massachusetts officials did not explicitly weaken state regulations to provide greater corporate access to student information. However, state regulations were last updated in 2006, before the explosion of third party managed student information systems and data-heavy educational technology—or 'EdTech'—applications. In light of these technological developments, the regulations must be clarified and expanded to reflect the current state of digital student privacy. Modernizing the law is necessary to fully achieve the stated purpose of the state regulations—to "insure parents' and students' rights of confidentiality."[41]

VI. GET THE FACTS: Massachusetts School Practices and Policies Impacting Students' Digital Privacy

Our research examined five areas of concern related to student privacy and technology:

• student information systems;
• school-controlled technologies (sometimes called "1:1 devices");
• in-school physical surveillance (i.e. cameras);
• in-school electronic surveillance; and
• corporate access to student information through EdTech applications and email.

Across these five issue areas, we found that many of the Massachusetts schools surveyed do not provide sufficient disclosures to parents or students about what kind of information schools are collecting about students, or whom they share it with and under what circumstances. Ultimately, parents should be able to opt their children out of some kinds of information gathering and sharing. Most schools surveyed do not provide such opportunities.

STUDENT INFORMATION SYSTEMS: Big data brings bigger privacy challenges

A CAUTIONARY TALE: inBloom goes bust

Today's school administrators do not keep student records in paper files like they once did. Now, student information ranging from test scores and attendance records to immigration status and out-of-school disciplinary reports is stored in what administrators and corporations call Student Information Systems ("SIS"). When it comes to student privacy and SIS, the key questions for parents are: What kind of data is the system collecting about my child, with whom is the school sharing it, and do I have an informed say in either process?

The story of one SIS's rapid rise and sudden downfall is a cautionary tale. In 2014, debate raged nationwide about the implementation of a Bill & Melinda Gates Foundation-funded SIS platform called inBloom. Based on the company's marketing materials, inBloom appeared to provide a repository where schools, districts, and states could upload student data to share with private EdTech companies. Under FERPA's amended regulations, which allowed schools to designate private companies as "authorized representatives," schools didn't need to get student or parent consent before using the service.[42] inBloom shut down in 2014 when, in the face of pressure from parents and privacy activists, all nine states (including Massachusetts) that had contracted with the company withdrew their support.[43]

The central reason people and organizations like the ACLU opposed inBloom was that the company enabled the collection of massive amounts of data—over 400 fields on each student, including sensitive information like disciplinary records, disabilities, and family structure.[44] Many of these data fields had no discernable relevance for private service providers, such as students' criminal records, times when a student was restrained, whether a student is homeless, pregnant, or an immigrant, and reasons why students left a school district.[45] It's not at all clear that schools need to track these kinds of information, but even if they do, there is absolutely no reason for it to be shared with for-profit corporations.

The inBloom program collapsed in part because parents and the public opposed its plan to collect, mine, and share student data. The public response was clear: no tracking without informed notice and consent. Although over 150 EdTech companies have signed the DC-based think tank Future of Privacy Forum's voluntary student privacy pledge, [46] our research shows that schools across Massachusetts and the nation continue to use technologies that trigger the same privacy concerns as inBloom.

A voluntary commitment to student privacy, while valuable, is not enough to protect young people from

predatory corporate collection and abuse. That's why we need strong state and federal regulations restricting the collection and use of student data, as well as transparency from both private companies and the government entities that partner with them. But in order to secure stronger student privacy protections in the law, we first need to understand the lay of the land.

LARGE COMPANIES collect big data in the shadows

Student information systems implicate student privacy rights in two ways: through data inputs and through policy controls of data access. In Massachusetts, none of the eighteen school districts we surveyed make publicly available a complete list of the data fields tracked by their respective information systems. None of the companies that provide student information systems to these Massachusetts districts makes a complete list of tracked data fields publicly accessible online, either. As a result, parents are left in the dark about exactly what kinds of information schools are collecting and potentially sharing with third parties.[47]

> A voluntary commitment to student privacy, while valuable, is not enough to protect young people from predatory corporate collection and abuse.

Public records and open source research revealed that Massachusetts schools contract with a number of different companies for their student information systems, including Aspen, PowerSchool and iPass. These systems and others in use at Massachusetts schools offer similar technical capabilities. Perhaps most importantly, because their data is stored in a structured format, every SIS platform enables districts to easily share student information with private, third party software providers. Our research showed that schools in Massachusetts are taking advantage of this capability.

SHARING STUDENT INFORMATION WITH THIRD PARTIES: We need more transparency

As always when it comes to information privacy, the devil is in the details. With respect to student privacy, the details reside in each district's policies and contracts with private vendors, which govern access to and control over student information.

> None of the eighteen school districts we surveyed make publicly available a complete list of the data fields tracked by their respective information systems.

Twelve districts produced contracts or invoices with SIS providers.[48] Only one—the Mystic Valley Charter School—explicitly stated that it housed the records on its own server and did not provide third party access to student records. The remaining eleven districts made no mention of parent or student consent in their SIS agreements either to release information to the SIS provider or to allow the SIS provider to share information with other third party corporations. At least four school districts—Brockton, Chelsea, West Springfield, and Worcester—have released student data to third parties for purposes other than records management. Not one of these districts required parent or student consent for these releases. Only Brockton prohibited these third parties from sharing information with other corporations absent parent consent.

The responsive districts disclosed two categories of documents related to sharing student information: (1) general policies on when student information will be released, detailing whether student or parent consent is required, and how students and parents are notified; and (2) specific contracts to release student data to par-

ticular outside companies, government entities, and private researchers.

Troublingly, we found that the general policies and specific contracts did not always align. Despite the presence of general data release policies requiring parental consent for disclosures, no contract conditioned a school's release of information to a third party on parent or student consent, and only one district prohibited third parties from sharing information with other corporations absent parent or student consent.

ON GENERAL INFORMATION SHARING POLICIES: Simple restatements of the law or in-depth communications with parents?

> Only one district—the Mystic Valley Charter School—specified that it had not released student data to private vendors.

Under the Massachusetts student privacy regulations, all districts are required to store and delete records according to certain protocols, and to make student records available to both custodial and non-custodial parents.[49] And, absent special circumstances, schools are required to obtain consent before disclosing information to anyone other than a student or parent.[50] The content of the general student data release policies we received all reflect these general requirements.

However, there were noticeable differences in how these general policies are *presented* to students, parents, and staff. Regarding transparency, we encountered some best practices, including:

- Describing the relevant law in plain language.
- Distinguishing between mandatory and optional disclosures.
- Notifying students and parents of their right to challenge mandatory disclosures.
- Describing the process for opting-out of optional disclosures and for consenting to partial disclosures without opening an entire student record.

However, we rarely saw all of these best practices in a single policy, and some districts failed to hit any of them.

The Boston public schools provide the most robust transparency of the districts we surveyed, listing various types of mandatory and optional disclosures in the student-parent handbook, with instructions on how to opt out of optional disclosures. The handbook also refers students and parents to a Superintendent's Circular that instructs staff to seek parental consent before sharing data with third parties, except in specifically delineated circumstances such as court-ordered disclosures and safety emergencies.

Boston also released copies of its parental notification and consent forms. The notification form specifically informs parents of their right to challenge subpoenas, court orders, and probation officer requests for records. Boston's consent form allows parents to grant access to specific types of student data, such as academic, disciplinary, attendance, and extracurricular information, while denying access to others.

Responses from other districts showed less detail, while still providing some information to students and parents:

- New Bedford, like Boston, provided a Release of Information Form authorizing parents to opt in or out of

releasing specific types of student data, but did not release any accompanying guidance or policies.
- Chelsea student records policies provide detailed, user-friendly explanations of student records regulations, but lack detailed information on parental rights to challenge releases, or to release some, but not all, student data.

Other districts, such as Salem and Lawrence, were less protective, providing only general summaries or plain restatements of the applicable laws, and sometimes glossing over required disclosures with assertions such as, "[w]ith a few exceptions, information in a student's record will not be released to a third party without [] written consent[.]"[51]

THE DEVIL'S IN THE DETAILS: Contracts with private vendors show school districts should dictate terms

Our public records requests also sought specific contracts and agreements with private software vendors and other third parties. Despite the presence of general data release policies requiring parental consent for disclosures, no contract conditioned a school's release of information to a third party on parent or student consent and only one district prohibited third parties from sharing information with other corporations absent parent or student consent.[52] The records show that contracts drafted by the *school districts* provide some privacy protection, while those drafted by the *partnering corporations* generally raise more concerns.[53]

Specific best practices present in the policies include:

- Limiting the use of student data to the purpose described in the contract.
- Prohibiting the receiving parties from re-disclosing or selling student data to any other entity.
- Requiring the deletion of all student data upon termination of the contract.

For example, Brockton and Worcester disclosed district-drafted standard and specific contracts to release student data to software providers, data analysts, and researchers. Importantly, all contracts drafted by Brockton and Worcester that we received describe a specific purpose for the information sharing, and prohibit the receiving entity from using student data for any other purpose without the district's permission. Under Brockton's standard release contract, the receiving entity may not re-share student data or use student data for monetary gain; must destroy all student data upon termination of the contract; and must comply with all federal and state laws.

In these ways, Brockton's and Worcester's standard release forms do a better job of limiting the release of student information than most corporate drafted contracts. Unfortunately, however, neither district's forms conditioned the school's release of information to a third party on parent and student consent. And while Brockton prohibited third parties from sharing confidential information with other corporations, Worcester authorized such disclosures upon school—not parent—consent.

Contracts and agreements with software providers that were drafted by the corporations were generally significantly laxer than those drafted by school districts. One exception is Brockton's contract with the Massachusetts Educational Financing Authority (MEFA), which explicitly stated that MEFA would not share spe-

cific student information "unless expressly directed to do so by the student or parent." Otherwise, the contracts written by corporations generally contain vague language or large loopholes opening up the possibility that student information could be used for a wide variety of purposes not explicitly disclosed in the contract or to parents.

For example, Chelsea's contract with SIS provider ShowEvidence permits the corporation to license student data to subcontractors and to use student data "to test . . . internal technologies and processes." It also contains broad language permitting ShowEvidence to use student data to provide non-specific services to the district. ShowEvidence agrees to comply with state and federal law, but does not mention student or parent consent. The contract also permits third parties that obtain student data through ShowEvidence to retain that data after the contract ends.

The Terms of Service between West Springfield and the corporation Clever are somewhat more privacy protective. Clever does not disclose student data to third parties without school authorization, and schools may revoke that authorization at any time. Clever also destroys student data within seventy-two hours of termination of the service. The Terms limit Clever's usage to data integration with other service providers. However, there's a large loophole: Clever retains the right to modify its Terms of Service at any time.

SCHOOL-CONTROLLED TECHNOLOGIES: Not the same as your own computer

School-controlled technologies provide students, especially low-income youth, with opportunities to use the latest devices at school and often at home. Without the proper policies in place, however, they also present serious privacy concerns. When it comes to privacy, a school's choice of device is less significant than the choices districts make about how they manage devices. Software installed on take-home laptops and tablets, what we call 'device control technologies,' can enable school officials to monitor extremely sensitive details about students, including their location, online activity, keystrokes, and even webcam activity, both at school and at home. Sixteen districts[54] responded to our request for information about school-controlled devices: ten offer iPads,[55] five offer Chromebooks,[56] and three offer MacBook Airs.[57]

The key questions related to school-controlled technologies are: What device control technologies are schools using, and what policies govern their use?

TRACKING THEIR TRACKING CAPABILITIES: Monitoring, filtering, and logging tools in use in Massachusetts schools

Device control technologies fall into three categories: application management software, content filtering software, and monitoring software. As described below, some applications provide both filtering and monitoring capabilities.[58]

Application management software, including Apple DEP, Chrome OS Management, and Casper JAMF, allows a district to remotely install, upgrade, or remove software on a school-controlled device. Because these technologies are limited to accessing a list of installed applications, and cannot access personal student information, they generally do not raise significant privacy concerns.

Content filtering software blocks students from accessing specific websites and applications and creates a

record whenever a student tries to access a blocked site. Some filters, like GoGuardian[59] and Lightspeed,[60] allow the option to record sites visited and searches, even those that are not blocked. All but one of the responding districts use on-campus filtering; at least eight also deploy *off-campus* filtering that operates regardless of where the school-controlled device is located.[61] At least four districts—Auburn, Natick, Wayland, and West Springfield—use off-campus filtering that also allows tracking of permissible Internet activity.[62]

Monitoring software tracks what students are doing with their devices. One common application, iCloud, can track the location of network-connected Apple devices such as iPads and Macbooks.[63] Another, Lightspeed, allows real-time reporting on network traffic, as well as filtering of off-campus traffic.[64] LanSchool allows staff to see students' browser histories, view their screens, take screenshots, log keystrokes, and even remotely control the device while connected to the school network.[65] Securly, a content filter, recently added a monitoring component that can scan students' social media posts for signs of bullying or self-harm.[66]

The most invasive monitoring software we found was the West Springfield school district's use of GoGuardian. This Chromebook application allows real-time and historical activity tracking. As of April 2015, GoGuardian's "theft recovery" tools let administrators track a device's location, take screenshots, log keystrokes, and even activate webcams. GoGuardian's features are available whenever the device is online, whether on campus or at home. 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."

BE AWARE: Policies give administrators wide berth to snoop absent suspicion or consent

The bulk of disclosed policies dealt with issues of payment, distribution, maintenance, and liability. Policies directly addressing privacy—meaning access to the school-controlled device, its content and location, or its functionality—were brief and relatively uniform. For the most part, these policies offered little to no protection for student privacy:

- Two-thirds of the districts that produced a relevant document discussing administrator or teacher access to school-controlled devices—ten out of fourteen—reserved the right to search or inspect school-owned devices without notice or consent.
- Eight of the responding districts stated that students have "no expectation of privacy" in their school-controlled devices.
- Two districts permit random or periodic searches of school-controlled devices.
- Bedford and Hopkinton reserve the right to disclose information obtained from school-controlled devices to the police.

The only district that reported a more protective search policy was Uxbridge, which limits searches of school-controlled devices to physical searches "when a problem is brought to the attention of the building administration."

The privacy policies we reviewed were also notable for what they did *not* include. Specifically, some schools failed to disclose the full extent of their content filtering and monitoring software, or allow for an opt-out from this monitoring or filtering. For example:

Two-thirds of the districts that produced a relevant document discussing administrator or teacher access to school-controlled devices—ten out of fourteen districts—reserved the right to search or inspect school-owned devices without notice or consent.

- Auburn uses Lightspeed for off-campus filtering, but the district's parent presentation[73] does not reference this program. Instead, it only briefly mentions a management system that allows for "reporting on use and content," without describing what that means or providing an opt-out option.
- West Springfield's policies simply note that activities may be monitored and do not disclose that it is using the highly invasive GoGuardian application to monitor student Chromebooks; we only discovered this by examining the district's purchase orders.[74]

SURVEILLANCE CAMERAS, IN-SCHOOL NETWORK MONITORING, & CORPORATE ACCESS TO STUDENT DATA

While our research largely focused on the use of student information systems and school-controlled technologies, we also sought information on physical and electronic surveillance in Massachusetts schools, as well as corporate access to student data through software applications and email.

CAMERAS EVERYWHERE, but few public policies

We sent public records requests to eighteen school districts in Massachusetts seeking information about physical surveillance, including radio frequency identification (RFID) systems, biometric tracking devices, and cameras. None of the responding districts reported using biometric or RFID systems to monitor or track students.[75] But all fourteen responding districts use surveillance cameras, often in the absence of clear and publicly accessible privacy policies.

Nationally, the use of surveillance cameras in public schools is on the rise. In 2004, only thirty-three percent of public schools used surveillance cameras to monitor school grounds; by 2012, that number almost doubled, reaching sixty-four percent.[76] The Massachusetts Department of Elementary and Secondary Education (DESE) does not provide statistics on surveillance cameras in Massachusetts schools, but every district that responded to our public records requests uses them in at least one of their facilities.[77] Still, very few districts produced policies governing that use:

- Newton was the only district that provided a written surveillance camera policy.
- Lawrence, Salem, and Mystic Valley Charter School described their policies, but did not produce formal policies in written form.
- At the time of our request, Boston, Holyoke, Duxbury, and Springfield claimed not to have responsive policies. Nine months later, Holyoke adopted a camera policy.[78]
- The remaining six schools[79] neither provided nor denied having policies, although a policy for the Lynn school district was easily available on its website.

In total, at least three of the fourteen responding districts are using surveillance cameras in school without any privacy policy, and another eight are using cameras without publicly accessible, written privacy poli-

cies—if they have policies at all.

The policies in Newton, Holyoke and Lynn provide some privacy protections, although Newton's is strongest. They all require signage wherever cameras are placed and restrict cameras to public areas. Newton and Lynn limit footage access to the superintendent or principal, whereas Holyoke limits footage access to school administrators.[80] Newton further limits access to instances where a suspected crime has been committed on school grounds. Newton permits footage to be shared with the police only in accordance with a written Memorandum of Understanding,[81] whereas Lynn's policy merely states that surveillance cameras "may be monitored by . . . law enforcement personnel throughout the year,"[82] and Holyoke simply authorizes law enforcement access with "prior notice" to the school.[83] Finally, Newton's policy requires deletion of footage *after* fourteen days, while Lynn's only specifies that footage will be kept for *at least* thirty days. Holyoke does not specify a footage retention period.

'NO EXPECTATION OF PRIVACY': On-campus Internet monitoring

All fourteen responding districts use surveillance cameras, often in the absence of clear and publicly accessible privacy policies.

Acceptable Use Policies (AUPs) largely address school policies for safe and responsible network use, but also contain provisions related to privacy. We found that 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, Millis, Uxbridge, Lawrence and Shrewsbury[84] state that students do not have an expectation of privacy *and* reserve the right to monitor Internet use.
- Auburn, Hopkinton, Bedford, and Wayland permit school officials to share information obtained over the school network with law enforcement.
- Although Burlington and Douglas both state that students do not have an expectation of privacy, Burlington only permits electronic searches of school networks to substantiate inappropriate activity and Douglas states that it will conduct an individualized search only when a school official has a reasonable suspicion that a student has violated a law or school policy. Douglas also provides students with written notice of any suspected violation and an opportunity to present an explanation.

'FREE WITH ADS': Corporate access to student data through EdTech applications

The last trend we investigated was the widespread use of software that grants corporations access to student information and communications. A number of schools are using third-party commercial EdTech platforms for student email, file storage, testing, homework, lesson planning, and assessment. These applications give corporations access to huge quantities of information about students, from their names and grades to the content of their emails and even their study habits. There is a danger that corporations may seek to use this data to advertise products back to schools, teachers, or even students.

The most widely used EdTech service is Google Apps for Education. Google Apps for Education combines student email, document creation and storage, and scheduling—all linked to a student's Google account. About half of the twenty-nine districts that provided records for this report use Google Apps for Education.[85] In five districts, obtaining a Google account is required to participate in school-controlled technology programs.[86] Some schools assign Google mail accounts to all students. For years, Google was mining data from these accounts for targeted advertising purposes. Only in 2014, after facing legal action, did Google modify its privacy policy to prohibit scanning student emails and files for advertising purposes.[87]

But Google is far from the only player in the EdTech arena. Other EdTech applications that have access to student data include:

> Lynn's policy states that surveillance cameras "may be monitored by . . . law enforcement personnel throughout the year."[82]

- **MyHomework**, a digital planner that tracks students' schedules and homework assignments. Shrewsbury uses a paid version of this application without advertisements; the other option is a "free" version that shows ads to students.
- **Schoology,** a Facebook-like application for managing classes, assignments, grades, and communications. Sudbury uses this application.

Applications like these may provide benefits to schools. But they also present the risk that corporate partnerships and consumer profiling will become determining factors in how students are educated, with lower-income school districts and students facing the stark reality that they cannot afford to pay for the privacy protections effectively purchased by wealthier communities.[88]

VII. CONCLUSION: Rethinking our approach to student privacy in the 21st century

The records we reviewed highlighted four general areas of concern with regard to student privacy: risk of improper use of student data, suspicionless searches, surveillance, and lack of transparency.

RISK OF IMPROPER USE OF STUDENT DATA

The first threat to student privacy is the risk that schools and corporations will use student data inappropriately, or will improperly disclose it to unaccountable third parties. Schools routinely create and obtain detailed information on individual students. Corporations also generate data on students who have accounts with them. In both the corporate and government realms, without the proper policies in place, there is a very real risk of the misuse of student information.

The most likely misuse of student data is improper data mining. "Data mining" (or "data analytics") uses computer algorithms to sort through large amounts of information, with the goal of producing new insights.[89] When corporations use data mining tools to target students with advertising, schools undermine their own

efforts to train the next generation of independent thinkers.[90] And corporations that do not mine student data for advertising purposes might share it with companies that do.[91] Moreover, as student data spreads from corporation to corporation, students, parents, and even schools have less and less control over sensitive personal information, and the ability to correct inaccurate information becomes increasingly remote.

The risks posed by schools misusing student data are also grave. Particularly dangerous is the prospect that schools will offer special opportunities to some students and deny them to others, based on information gleaned from computer algorithms and imperfect data inputs.[92]

Unfortunately, these potential problems are not getting the careful attention they deserve. Many of the school districts we surveyed did not have a clear policy governing the transfer of student information to third parties. Other schools adopted data policies written by for-profit corporations, offering protections substantially weaker than those offered in districts that wrote their own policies. While all disclosures of student data raise privacy concerns, disclosures made on terms dictated by private companies are cause for serious alarm. EdTech corporations have a fiscal interest in mining, sharing, or even reselling student data, and often use vague contractual terms to leave those possibilities open. For-profit corporations are fundamentally only responsible to their boards of directors and shareholders. Public schools are meant to serve the public good.

When public schools outsource central school management and educational practices to private companies, what's best for students can get left behind.

SUSPICIONLESS SEARCHES

The second threat to privacy we identified is suspicionless searches, where school officials claim authority to access a student's physical or digital possessions without even reasonable suspicion that the student has violated a law or school policy. As the Supreme Court recently noted, Internet-enabled devices store vast amounts of personal information [93]—far more than a book bag or a locker. With the advent of school-controlled technology programs, students are encouraged to use school-monitored devices as if they are their own, often both on campus and at home. Some districts, like Bedford and West Springfield, even allow students to install their own software or let parents get their own account on the device. It is inevitable that these devices will, even a few weeks into the school year, contain large quantities of sensitive personal information.

Before searching a student's backpack or notebook, a school official needs "reasonable suspicion"—a specific, articulable reason to believe the student has broken a law or school rule.[94] But when it comes to school-controlled devices, which contain much more information than any notebook or backpack could, nine out of fourteen districts either ignore students' privacy interest or explicitly allow for suspicionless searches.

The legality of suspicionless searches of school-controlled devices is still being worked out in the courts, but it is clear that explicitly denying students any privacy in such devices is a terrible policy—in no small part because suspicionless searches increase the risk that student discipline will be outsourced to the criminal justice system. Districts like Bedford and Hopkinton, which both state that students have no expectation of privacy and reserve the right to disclose the result of searches to police, potentially enable law enforcement agencies to bypass the constitutional requirement of finding probable cause before rifling through a student's

sensitive information. In addition to exposing students to potential criminal charges—a life-altering event—a policy of suspicionless searches teaches students that their Fourth Amendment rights can be summarily discarded simply by participating in school programs. This decidedly anti-democratic message is the exact opposite of what students should be learning in schools in a free society.

SURVEILLANCE

The third threat to privacy is the use of surveillance cameras. Surveillance cameras in schools provide the illusion of security while normalizing ubiquitous monitoring. Despite rare and high profile incidents of extreme violence, students in the United States are safer at school than at any point since 1993.[95] And while there is no empirical evidence to suggest cameras stop violence at schools or protect youth, there's a very real danger that their widespread deployment in institutions of learning sends the wrong message to students: You are not safe at school, and you must be watched at all times for your own good.[96]

> Only one district surveyed, Uxbridge, had a policy requiring suspicion of a violation before conducting a search of a school-controlled device.

As an organization that defends civil rights and civil liberties, the ACLU is concerned about the rapid expansion of school surveillance systems. But what do students think? In 2013, a group of Walpole High School students formed Students Opposing Surveillance, or SOS, to make their concerns known. SOS argued that the cameras invaded student privacy, created a sense of distrust between the student body and the administration, and cost money that could be spent elsewhere.[97] One student, Jon Kelland, responded to claims that cameras would protect students in the event of a shooting: "These cameras will not stop bullets from flying [or] put Kevlar in front of the students," he said.[98]

Students at North High School in Worcester had a similar reaction when the school announced that it would share real-time surveillance video with the local police. While some students agreed with heightened surveillance, others saw increased police involvement at schools as an unnerving violation of privacy.[99]

Much like cameras, many types of electronic monitoring enable schools to surveil their students. Location tracking software embedded in school-controlled devices can track students' physical movements, while filtering software can track students' digital lives, including browsing habits, communications, and social media use. These technologies undermine students' control over their information by eliminating private spaces, both online and in the real world.

For the most part, school policies do little to mitigate this harm. Most schools did not produce policies limiting the district's power to conduct physical surveillance. Of the schools that provided policies about Internet monitoring, the vast majority did not limit what schools can do.

Visible surveillance—like cameras—normalizes the idea that students are, and will be, continually watched. Ubiquitous spying through school Internet and devices can also give the impression that students are violating laws and policies more frequently than in the past, when in fact there is simply more information about potential violations. This can lead to over-disciplining students, including more frequent involvement of law

enforcement in disciplinary issues. Enhanced surveillance capabilities can thus exacerbate the school-to-prison pipeline, undermining the students' opportunities, especially for students of color and those with developmental or learning disabilities.[100]

> While there is no empirical evidence to suggest cameras stop violence at schools or protect youth, there's a very real danger that their widespread deployment in institutions of learning sends the wrong message to students

LACK OF TRANSPARENCY

Finally, we saw an overall lack of transparency from the districts we contacted. Seven school districts either did not respond to our request for records, or charged fees that were beyond what the ACLUM, let alone a student or parent, could reasonably afford. Among the districts that did respond, many failed to produce important documents.

The documentation schools did disclose raised a different set of transparency concerns. Over a dozen districts released purchase records for school-controlled technologies, which showed that some schools are installing highly invasive filtering and monitoring software on students' devices. However, students and parents are not always told about the full capabilities of these applications, and in some cases are not even told which proprietary software is being used.

We saw the same problem with disclosures of student information. The records we obtained show that several schools are disclosing student information to third-party researchers, analysts, and developers. Because they are not publicly posted, these information-sharing agreements are not always available to students and parents without going through the lengthy and sometimes expensive process of making a public records request.

Lack of transparency shrouds privacy violations in secrecy, making it difficult for parents and students to understand or change bad policy and giving the upper hand to corporations intent on harvesting and profiting from student information. Lack of transparency does not always mean that a district is trying to hide information from the public. But whether the failure to be transparent with parents and students is intentional or accidental, it obstructs the democratic process.

Without an open exchange of information about current and possible future policies and practices, districts may believe that students and parents do not value privacy, while students and parents may not know that their privacy is at risk. The result is a system that does not reflect the values of the community. An informed public is essential for a properly functioning democracy—a maxim that does not cease to be relevant at the schoolhouse gates. By failing to make important information about privacy practices available to the public, districts undermine both the participatory nature of our government and student rights.

APPENDIX 1
SPECIFIC FINDINGS ON MASSACHUSETTS SIS

Here in the Commonwealth, our research showed that most schools use commercial Student Information Systems to manage student data. Fewer districts use custom-built SIS platforms.

Thirteen school districts in Massachusetts provided us with information about which SIS they use to manage student information. The five largest school districts in Massachusetts[101] all use different SIS platforms—Boston uses Aspen, Springfield uses Powerschool, Brockton uses Infinite Campus, and Lynn uses eSchoolPlus, while Worcester uses a custom-built system.[102] In North America, PowerSchool is the most widely used platform, and it reaches more than fifteen million students worldwide as of June 2014.[103]

Records show schools in Massachusetts are sharing information with third-party entities. Worcester school district provided contracts releasing student data to twenty different entities, including private software vendors, consultants, and researchers. Brockton released student data to two special education management services, eSped[104] and EasyIEP,[105] as well as one analytics service and one research group. Chelsea produced a contract with ShowEvidence, an online student assessment tool.[106] Shrewsbury, a PowerSchool district, is using a curriculum management application called Schoology[107] – one of 140 private "Independent Software Vendor" partners that can access data directly from the PowerSchool SIS.[108] Holyoke, Lynn, Salem, and West Springfield all produced contracts or purchase orders for online special education management platforms.[109] West Springfield is using a "middleware" platform called Clever to connect its SIS to Google's Apps for Education service.[110]

ENDNOTES

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 Westin, Alan F. *Privacy and Freedom*, pg 7New York: Atheneum, 1967.

6 The right to autonomy, sometimes called the right to self-determination, is recognized as a basic human right. See Part 1, Article 1 of The United Nations International Covenant on Civil and Political Rights, available at http://www.hrweb.org/legal/cpr.html.

7 *NAACP* v. Alabama (357 U.S. 449, 1958) was a landmark case in which the U.S. Supreme Court recognized freedom of association as a right protected by the First Amendment.

8 Warren, Samuel, and Louise Brandeis. "The Right to Privacy." *Harvard Law Review*, 1890, 275; and *Olmstead v. United States*, 277 U.S. 438, 478 (1928).

9 See the U.S. Senate's 2013 report on the multi-billion dollar a year data brokering industry, at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577. Siciliano, Robert. "Data Brokers: What Are They; How to Get Control of Your Name." *The Huffington Post*. TheHuffingtonPost.com, 21 Apr. 2014. Web. 23 Sept. 2015. <http://www.huffingtonpost.com/robert-siciliano/data-brokers-what-are-the_b_5185127.html>.

10 Singer, Natasha. "InBloom Student Data Repository to Close." *The New York Times*, April 21, 2014, Technology sec. <http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/?_php=true&_type=blogs&_r=0>.

11 For a detailed discussion on the ethics of using data mining and analytics in education policy, see Jeffrey Alan Johnson, "The Ethics of Big Data in Higher Education," International Review of Information Ethics, Volune 7, 2014, available at http://www.i-r-i-e.net/inhalt/021/IRIE-021-Johnson.pdf. See also Alacorn, A., Zeide, E., Rosenblat, A., Wikelius, K., boyd, d., Gangadharan, S. & Yu, C. (2014). *Data & Civil Rights: Education Primer.* See http://www.datacivilrights.org/pubs/2014-1030/Education.pdf.

12 The movement of students from school disciplinary system to the criminal justice system is called the school-to-prison pipeline. Both in Massachusetts and nationwide, it is a burden disproportionately borne by students of color or other minorities, students living in poverty, and students with developmental and learning disabilities. See: https://www.aclu.org/issues/racial-justice/race-and-inequality-education/school-prison-pipeline. For a discussion of how school surveillance can exacerbate the school-to-prison pipeline, see Raible, John, and Jason G. Irizarry. "Redirecting the Teacher's Gaze: Teacher Education, Youth Surveillance and the School-to-prison Pipeline." *Teaching and Teacher Education*: 1196-203. See http://youthjusticenc.org/download/education-justice/suspension-and-expulsion/Redirecting%20the%20Teacher's%20Gaze:%20Teacher%20Education,%20Youth%20Surveillance%20and%20the%20School-to-Prison%20Pipeline.pdf.

13 Roessler, Beate, and Dorota Mokrosinska, eds. *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge University Press, 2015. 228-230.

14 *SafeGov Global School Internet Privacy Survey*, SafeGov and Brunswick Group, 2014, safegov.org, cited by McKinsey & Company at http://mckinseyonsociety.com/protecting-student-data-in-a-digital-world/.

15 Future of Privacy Forum. "New Future Privacy Forum Survey Shows Parents Overwhelmingly Support Using Student Data to Improve Education; Concerns About Privacy and Security Remain." Future of Privacy Forum. 21 Sept. 2015. Web. 23 Oct. 2015. <http://www.futureofprivacy.org/2015/09/21/new-fpf-survey-shows-parents-overwhelmingly-support-using-student-data-to-improve-education>

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

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

18 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>.

19 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.

20 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.

21 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.

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

23 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.

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

25 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>.

26 The findings in this report are largely based on the records provided to the ACLU in response to these records requests, which are available at https://aclum.org/student_privacyreportdocuments. All other external sources are cited in the endnotes.

27 Read the public records requests at https://aclum.org/student_privacyreportdocuments.

28 Ibid.

29 The Lexington and West Springfield school districts received both requests.

30 In order of response, these districts were Millis, Revere, Douglas, Brockton, Franklin, Sudbury, Burlington, Hopkinton, Wayland, Worcester, Natick, Auburn, West Springfield, Duxbury, and Lawrence.

31 In order of response, these districts were Uxbridge, Lynn, Shrewsbury, Salem, Holyoke, Springfield, Wellesley, Methuen, Boston, Chelsea, the Mystic Valley Regional Charter School, New Bedford, and Bedford.

32 https://aclum.org/app/uploads/2015/08/Attorneys-Fees-state-statutes-chart.pdf

33 34 CFR § 99.30, available at http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33.

34 34 CFR § 99.31(a)(1)(i), available at http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33.

35 Barnes, Khaliah. "Amassing Student Data and Dissipating Privacy Rights." *Amassing Student Data and Dissipating Privacy Rights*. EDUCAUSE. Web. 23 Sept. 2015. <http://www.educause.edu/ero/article/amassing-student-data-and-dissipating-privacy-rights>.

36 34 CFR §§ 99.30, 99.31(a)(3), 99.35, available at http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33. See also "EPIC - EPIC v. The U.S. Department of Education." *EPIC - EPIC v. The U.S. Department of Education*. Web. 23 Sept. 2015. <https://epic.org/apa/ferpa/default.html>.

37 603 CMR 23.02, 23.07 (4), Access to Student Records, Student Records, Education Laws and Regulations, Massachusetts Department of Elementary and Secondary Education, available at http://www.doe.mass.edu/lawsregs/603cmr23.html?section=07.

38 603 CMR 23.02,Definition of Terms, Student Records, Education Laws and Regulations, Massachusetts Department of Elementary and Secondary Education, available at http://www.doe.mass.edu/lawsregs/603cmr23.html?section=02.

39 Ibid.

40 Ibid.

41 603 CMR 23.00, 23.01, Application of Rights, Student Records, Education Laws and Regulations, Massachusetts

Department of Elementary and Secondary Education, available at http://www.doe.mass.edu/lawsregs/603cmr23.html?section=01.

42 34 CFR §§ 99.30, 99.31(a)(3), 99.35, available at http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33. See also Strauss, Valerie. "Lawsuit Charges Ed Department with Violating Student Privacy Rights." *Washington Post*. The Washington Post, 13 Mar. 2013. Web. 23 Sept. 2015. <http://www.washingtonpost.com/blogs/answer-sheet/wp/2013/03/13/lawsuit-charges-ed-department-with-violating-student-privacy-rights>. (Note: Massachusetts state privacy regulations are more protective than FERPA.)

43 Kharif, Olga. "InBloom Shuts Down Amid Privacy Fears Over Student Data Tracking." *Bloomberg.com*. Bloomberg, 1 May 2014. Web. 23 Sept. 2015. <http://www.bloomberg.com/bw/articles/2014-05-01/inbloom-shuts-down-amid-privacy-fears-over-student-data-tracking>.

44 Singer, Natasha. "Deciding Who Sees Students' Data." *The New York Times*. The New York Times, 5 Oct. 2013. Web. 23 Sept. 2015. <http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html>.

45 For a complete list of fields inBloom proposed to track, see http://www.classsizematters.org/wp-content/uploads/2013/04/inBloom-Data-Fields-excerpts.pdf.

46 "Student Privacy Pledge – Hits 150!" *Future of Privacy.* 15 June 2015. Web. 23 Sept. 2015. <http://www.futureofprivacy.org/2015/06/15/student-privacy-pledge-hits-150>.

47 Most SIS platforms allow schools to insert custom fields, potentially expanding the amount of student data tracked. Additionally, some districts use ancillary SIS platforms to supplement their core SIS, adding more detail to certain types of records. For example, Salem school district uses HealthMaster, a medical records system capable of tracking detailed information about students' mental and behavior health and special education needs.

48 We didn't specifically ask Shrewsbury for these records, instead asking for information about school-controlled technologies, but the district volunteered that it shares information with private companies.

49 603 CMR 23.07, available at http://www.doe.mass.edu/lawsregs/603cmr23.html?section=07.

50 Ibid.

51 This particular example is taken from the 2014-15 Salem High School student handbook.

52 The reason for this discrepancy isn't laid out in any school policies or contracts, but probably results from the deregulation of FERPA to allow schools to treat contracting corporations as "authorized representatives." Therefore, even when a school's general policy requires that they obtain parental consent before sharing student information with outside entities, this requirement may be ignored if a school designates a contractor as an authorized representative.

53 One exception is Brockton's contract with the Massachusetts Educational Financing Authority.

54 More than sixteen technologies are listed because some districts offer more than one option.

55 Auburn, Bedford, Burlington, Douglas, Methuen, Millis, Revere, Shrewsbury, Uxbridge, and Wellesley.

56 Douglas, Franklin, Sudbury, Wayland, and West Springfield.

57 Hopkinton, Natick, and Wayland.

58 For example, GoGuardian. https://www.goguardian.com/.

59 https://www.goguardian.com/.

60 http://www.lightspeedsystems.com/products/web-filter/.

61 Auburn, Burlington, Douglas, Franklin, Natick, Sudbury, Uxbridge, Wayland, Wellesley, and West Springfield.

62 Auburn, Natick, and Wellesley use Lightspeed; Wayland uses Securly; and West Springfield uses GoGuardian.

63 https://www.apple.com/icloud/find-my-iphone.html. Bedford, Millis, and Natick reported using this feature. Wellesley reported that location tracking is disabled on all devices issued to students. Auburn, Burlington, Douglas, Hopkinton, Methuen, Revere, Shrewsbury, Uxbridge, and Wayland also use Apple products but did not include a policy on location tracking.

64 http://files.lightspeedsystems.com/pdfs/collateral/Features-Checklist_WF.pdf. Auburn, Natick, and Wellesley reported using the Lightspeed to filter web content. Other Lightspeed products allow location tracking, but does not appear to be deployed in any of the responding schools.

65 http://lanschool-docs.s3.amazonaws.com/ls78/ls78datasheet.pdf. Wayland school district produced a purchase order for LanSchool in response to our public records request.

66 http://blog.securly.com/2015/08/05/bullying-and-self-harm-detection/. Wayland uses Securly to filter off-campus traffic for middle school students. The monitoring functionality was added after Wayland responded to our public records request, so we do not have any information on whether the district is using this feature.

67 https://www.goguardian.com/student-engagement-analytics-offers-visibility-to-user-behavior-metrics-to-help-improve-student-engagement.html.

68 https://www.goguardian.com/anti-theft-provides-chromebook-recovery-and-protection-wherever-the-device-is-located.html; http://www.edtechroundup.org/reviews/goguardian-chromebook-monitoring-filtering-and-anti-theft-for-schools.

69 Of the sixteen responding schools, fourteen produced their privacy policies for school-controlled devices. Auburn and Shrewsbury did not include privacy policies in their responses. Auburn school district requires parents to attend a training session or view a training video that describes the district's policies. The video version, which was included in Auburn's response, did not address the district's privacy policies. Shrewsbury's privacy policy appears to require a parent or student account to view.

70 Sudbury, West Springfield, Burlington, Revere, Bedford, Douglas, Franklin, Hopkinton, Millis, Natick, Methuen, Uxbridge, Auburn, Wayland.

71 Bedford, Burlington, Douglas, Franklin, Hopkinton, Sudbury, and West Springfield.

72 Bedford, Millis, and West Springfield.

73 Available at https://www.youtube.com/watch?v=nYNL4LH4H1c.

75 Our independent research showed the same.

76 "Indicators of School Crime and Safety." *National Center for Education Statistics*. Institute for Education Sciences, 1 July 2015. Web. 23 Sept. 2015. https://nces.ed.gov/programs/crimeindicators/crimeindicators2014/figures/figure_20_2.asp

77 Brockton, Lawrence, Newton, and Salem school districts and the Mystic Valley Charter School affirmatively reported using surveillance cameras. Boston, Chelsea, Lynn, and New Bedford did not, but mention cameras on their website or in their student handbooks. Duxbury, Springfield, and Worcester school surveillance systems have been in the news recently. See: Waterhouse, Gail. "Duxbury Coach Accused of Assaulting Two Students." *MyFoxBoston.com*. Fox News, 10 Sept. 2014. Web. 21 Oct. 2015. < http://www.myfoxboston.com/story/26495241/duxbury-coach-accused-of-assaulting-two-students>. McKay, David. "Public Schools Show Increase in Security Measures." *WWLPcom*. 21 May 2015. Web. 23 Sept. 2015. <http://wwlp.com/2015/05/21/public-schools-show-increase-in-security-measures>. O'Connell, Scott. "Worcester School Board OKs Grant Application for School Security System." Telegram.com. 30 Apr. 2015. Web. 23 Sept. 2015. <http://www.telegram.com/article/20150430/NEWS/304309506>. Finally, we found minutes from the Holyoke school committee describing the use of 60 cameras in Holyoke High School and a DESE report referring to West Springfield's school surveillance cameras. See: "School Committee Agenda." Http://*www.hps.holyoke.ma.us*. City of Holyoke, School Committee, 1 Aug. 2011. Web. 23 Sept. 2015. <http://www.hps.holyoke.ma.us/pdf/sc_agendas/PacketRegular 8-1-2011.pdf>. "West Springfield Public Schools District Review." Http://*www.doe.mass.edu*. Massachusetts Department of Elementary and Secondary Education, 1 Feb. 2013. Web. 23 Sept. 2015. <http://www.mass.gov/edu/docs/ese/accountability/district-reports/nolevel/2012-0332.pdf>.

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

79 Brockton, Chelsea, Lynn, New Bedford, West Springfield, and Worcester.

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

81 We obtained a copy of the prior Memorandum from the City Solicitor's office. While we were relieved to see that Newton had a written data sharing policy, the Memorandum in many ways typifies the school-to-prison pipeline. For example, it requires the district to involve the police in incidents involving the possession of drugs or alcohol, threats, bullying, and hazing, regardless of severity. Moreover, school officials are tasked with securing evidence and turning over written reports to the police.

82 http://www.lynnschools.org/documents/district/policies_codes_guidelines/School%20Security%20Camera%20Policy-%20ECA_B%20-%202-12-15.pdf.

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

84 The Shrewsbury Acceptable Use Policy for high school students states, in part: "I understand that…there is no expectation of privacy when I use the school district's network, and anything I do can be viewed by administration at any time." The policy is available here: http://schools.shrewsbury-ma.gov/itams/documents/1241563252_192138.pdf.

85 Some districts only use specific features, like file storage, while disabling others, such as email. A few districts, like Auburn, assign every student a Google account but only enable email for older students.

86 Douglas, Franklin, Hopkinton, Natick, and Sudbury.

87 Williams, Lauren C. "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>.

88 Hill, Adrienne. "A Day in the Life of a Data Mined Kid." *Marketplace.org*. American Public Media, 15 Sept. 2014. Web. 23 Sept. 2015. <http://www.marketplace.org/topics/education/learningcurve/day-life-data-mined-kid>.

89 See Chideya, Farai. "No Child Left Un-Mined? Student Privacy at Risk in the Age of Big Data." *The Intercept*. First Look Media, 27 June 2015. Web. 23 Sept. 2015. <https://firstlook.org/theintercept/2015/06/27/child-left-un-mined/>; and Simon, Stephanie. "The Big Biz of Spying on Little Kids." *POLITICO*. 15 May 2014. Web. 23 Sept. 2015. <http://www.politico.com/story/2014/05/data-mining-your-children-106676.html>.

90 See "Advertising in Schools," Campaign for a Commercial Free Childhood. http://www.commercialfreechildhood.org/issue/advertising-schools.

91 A 2013 study of district-corporate contracts from twenty schools around the country found that only 7% of these contracts restricted the sale or marketing of student information. Reidenburg, Joel. "Privacy and Cloud Computing in Public Schools." *Fordham Law Archive of Scholarship and History*. Fordham University School of Law Center on Law and Information Policy, 13 Dec. 2013. Web. 23 Sept. 2015. <http://ir.lawnet.fordham.edu/clip/2>.

92 See, e.g., Hill, Adriene. "A Day in the Life of a Data Mined Kid." Marketplace.org. American Public Media, 15 Sept. 2014. Web. 23 Sept. 2015. <http://www.marketplace.org/topics/education/learningcurve/day-life-data-mined-kid>.

93 *Riley v. California*, 134 S.Ct. 2473, 2490 (2014).

94 This constitutional rule was established in the Supreme Court case *New Jersey v. T.L.O.*, 469 U.S. 325, 341 (1985).

95 Neuman, Scott. "Violence In Schools: How Big A Problem Is It?" *NPR*. NPR, 16 Mar. 2012. Web. 5 Oct. 2015. <http://www.npr.org/2012/03/16/148758783/violence-in-schools-how-big-a-problem-is-it>.

96 See, e.g., National Association of School Psychologists, http://www.nasponline.org/advocacy/schoolsecurity.pdf.

97 Seltz, Johanna. "Walpole Students Petition against Surveillance Cameras in Schools Students Oppose Adding Cameras Students Fight Plan to Add Cameras Students Fight Plan to Add Cameras." *Boston.com*. The New York Times, 14 Mar. 2013. Web. 23 Sept. 2015. <http://www.boston.com/news/local/massachusetts/2013/03/13/walpole-students-petition-against-surveillance-cameras-schools-students-oppose-adding-cameras-students-fight-plan-cameras-cameras-students-fight-plan-add/GjxmVgguxho7WOfdlqkTqN/story.html>.

98 See ibid.

99 Allen, Samantha. "North High Students Have Mixed Reactions to School Surveillance." *Telegram.com*. 3 Mar. 2015. Web. 23 Sept. 2015. <http://www.telegram.com/article/20150303/NEWS/303039549/1116>.

100 https://www.aclu.org/issues/racial-justice/race-and-inequality-education/school-prison-pipeline.

101 District populations based on 2014-15 enrollment data, available at http://profiles.doe.mass.edu/state_report/enrollmentbygrade.aspx.

102 Worcester is the only responding district that uses a custom-built SIS; the other twelve use commercial, off-the-shelf products.

103 "Pearson to Sell PowerSchool to Vista Equity Partners." Pearson.com. 17 June 2015. Web. 23 Sept. 2015. <https://www.pearson.com/news/announcements/2015/june/pearson-to-sell-powerschool-to-vista-equity-partners.html>.

104 https://www.esped.com/.

105 http://www.publicconsultinggroup.com/education2/products/easyiep/index.html.

106 http://www.showevidence.com/.

107 https://www.schoology.com/home.php.

108 http://www.powerschool.com/powerschool-partner-program/.

109 Holyoke and Salem reported using eSped, Lynn uses EasyIEP, and West Springfield uses SEMSTracker (http://excent.com/Products/SemsTracker).

110 Middleware is software that acts as a bridge between two or more otherwise incompatible applications. Usually this is done by converting data from the two end-point applications into a common format that can be read by both systems. In the case of Clever, the converted information is stored online, allowing SIS platforms (including Aspen, PowerSchool, and many more) to connect to over 200 different applications. https://clever.com/.


ACLU
AMERICAN CIVIL LIBERTIES UNION
of MASSACHUSETTS
FOUNDATION