EDUCATION LEADERS REPORT

Volume 2, No. 4

October 2016

School Surveillance: The Consequences for Equity and Privacy

BY J. WILLIAM TUCKER AND AMELIA VANCE

NASBE | National Association of State Boards of Education

Table of Contents

ABOUT THE AUTHORS

J. William Tucker is data and technology legal fellow for NASBE, and Amelia Vance is NASBE's director of education data and technology. She can be followed on Twitter at @ameliaivance.

The authors thank all of the amazing people who helped make this a better publication: Rachel Anderson, Claire Borthwick, Kimberly Charis, Brendan Desetti, Bill Fitzgerald, Erima Fobbs, Teddy Hartman, Elizabeth Laird, Reg Leichty, Brenda Leong, Kim Scardino, Jim Siegl, Steve Smith, Elana Zeide, and our editor, Valerie Norville.

Cover illustration: iStockphoto

School Surveillance: The Consequences for Equity and Privacy

By J. William Tucker and Amelia Vance

Schools watch their students. Nearly every responsibility that schools shoulder includes an element of surveillance—from ensuring that preschoolers do not wander off, to keeping third graders on task, to stopping bullying and sexting. These responsibilities are not new, but schools' increased ability to monitor students continuously is.

This capability—coupled with schools' adoption of surveillance technologies, concerns over student privacy, and increased research on major discipline disparities—makes it vital that state policymakers create guardrails around school surveillance to ensure equity and privacy are not undermined.

Schools typically watch students closely for a few key reasons: to keep students on task, for student and staff safety, and auditing and efficiency. In order to accomplish these goals, schools have supplemented traditional staff observations of students with a multitude of technologies, such as surveillance cameras, student internet use and device monitoring, and biometric scanners. By the 2013–14 school year, for instance, 75 percent of all K-12 schools in the United States were using security cameras.[1]

Districts generally get to decide which technologies to use and how intensive surveillance will be, but schools also have monitoring obligations under state and federal laws: Many states have laws imposing a duty of care on schools, there is a federal law requiring that schools filter certain inappropriate content, and almost all states have supplementary laws demanding that schools monitor cyberbullying or school violence. In addition, states and the federal government also require that some school surveillance result in written records, such as reports on disciplinary behavior, in order to identify when school climate needs to improve and whether minority students are disproportionately targeted for student discipline.

However, supplementing—and, in some cases, substituting—traditional human supervision with surveillance technology has not made school supervision fairer. Research increasingly points to an "uneven landscape of school discipline in which students of color are disproportionately impacted by discipline actions."[2] While technology may track students without regard to their varying physical characteristics, people, who may have conscious or subconscious biases, still interpret the results.

Few states have addressed the privacy or equity implications of ramping up surveillance technology in schools. But there are several significant ones: Surveillance can limit student creativity and learning by leading them to self-censor, compound the effects of existing discipline disparities and the digital divide by uncovering evidence of minor offenses that would otherwise have gone undetected, produce a disproportionate amount of data on those students who rely exclusively on school-provided devices that are most readily monitored, and create more data about students that could follow them long after schooling has ended.

While states have been working to protect student privacy—introducing more than 400 bills on the topic since 2014—few have addressed privacy protections for school surveillance. Similarly, many states have attempted to end disproportionate disciplining of minority students by eliminating zero-tolerance discipline policies or advocating for restorative justice practices, but none of these policies have addressed the inequitable effects of surveillance.

As more districts and schools adopt technologies that can surveil students on a second-to-second basis, state boards of education must be aware of the potential discriminatory effects of this surveillance and make key decisions about what technologies should be used, what data should be collected or retained, and what safeguards should be put in place to mitigate the discriminatory consequences.[3]

Six principles laid out below can usefully guide development of effective policies: minimization, proportionality, transparency, openness, empowerment, and equity.[4] In addition, staff training is critical to ensuring that policies reflecting these principles will be implemented appropriately.

WHY IS THERE SURVEILLANCE?

The growing presence of technology in US classrooms is no secret. Most educators welcome its presence: According to one survey, over two-thirds of teachers expressed a desire for more classroom technology.[5] In low-income schools, this support rises to three-fourths of teachers. Seventy-one percent of parents said in a 2015 survey that school tech has improved the quality of education.[6] US primary and secondary schools spent $4.9 billion on laptops, computers, and tablet devices in 2015.[7]

Internet monitoring is an example of school surveillance with which parents (and their students) are increasingly familiar. It is difficult to overstate the internet's potential as an educational resource. But while every page in a school textbook is selected to be age and educationally appropriate, the same cannot be said for every page on the web. Confronted with this reality, schools need ways to manage and curate the learning experience, prevent bullying and harassment, promote safety, meet federal obligations such as protecting children from pornography, and more. Keeping track of how students interact with the internet is a natural extension of this.

Almost all schools are required to engage in at least basic student internet filtering and monitoring to comply with the Children's Internet Protection Act (box 1). Eighteen states have also layered their own internet filtering laws onto CIPA protections (map 1).

Keeping Students on Task

Schools often monitor student devices to keep students on task—making sure they are using the web to research Poe and not promwear. In an interview with Scholastic, South Carolina teacher Lisa Carrigan said she uses a software program in her school's computer lab to help keep her students focused while they use the internet.[8] Such monitoring programs notify the teacher when students are browsing the wrong sites and allow her to redirect them from her own device. Essentially, these programs are a high-tech version of teachers walking around their classroom to check whether students are passing notes or reading comics (box 2)."The whole point of this software is to free up time for teachers to do what they do best, which is to teach," said Marcus Kingsley, NetSupport's CEO.[9]

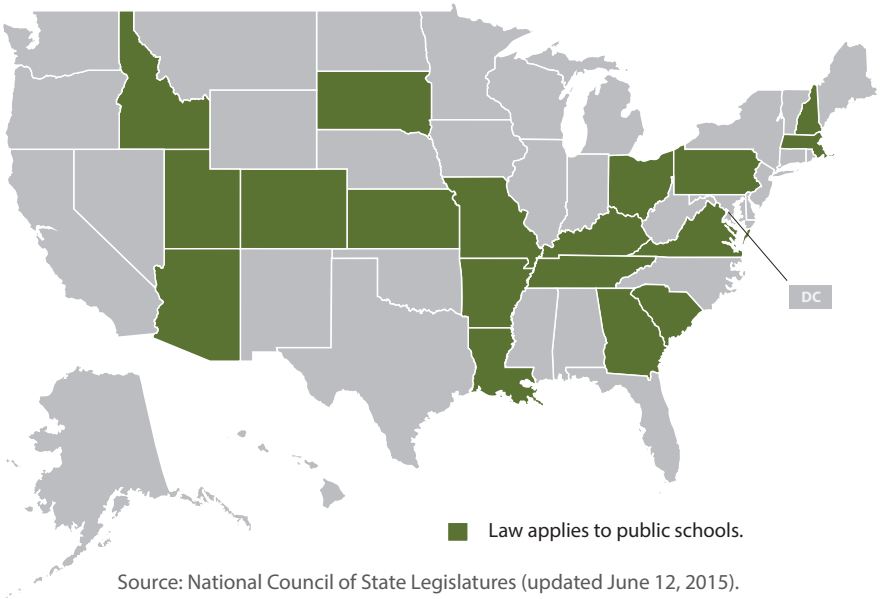
Such monitoring is not possible without digital devices for all students. "One-to-one" device programs provide each student their own laptop, netbook, tablet computer, or other mobile-computing device so they can engage regularly with digital and online resources. One-to-one (also seen as 1:1 or 1-to-1) devices can help serve school goals of student engagement and personalized learning, while also facilitating introduction of education technology into the classroom. According to one Market Data Retrieval survey, one-to-one device strategies are "substantially implemented" in 44 percent of district high schools, 36 percent of middle schools, and 20 percent of elementary schools across the country.[10]

While there is limited research on the efficacy of one-to-one device programs, one study of 5,000 Texas middle school students found that the students participating in one-to-one initiatives saw marked improvements in their technology skills and a drop in discipline problems.[11] One-to-one device programs may allow students to keep their devices with them throughout the day and even take them home, or the school may have a "cart model," in which students pick up a device from a cart when they enter the classroom (allowing schools to purchase a smaller number of devices). In this way, schools can transform the classroom learning experience while retaining control over device selection and bypassing equity issues that arise when you rely on students to supply their own devices.

However, not every school can afford one-to-one access. Bring-your-own-device (BYOD) initiatives are one solution for some districts. Not surprisingly, students have trouble focusing on teacher-assigned tasks when they are using their own devices just as much as when they are using a school device, and monitoring software also exists for the devices students are bringing from home.[12] A major distinction between the two is that in the first instance schools are monitoring student use of school property, which is more likely to be used mostly for schoolwork and stay on school grounds. When dealing with a

[MAP 1]

18 States Have Internet Filtering Laws That Apply to Public Schools



Source: National Council of State Legislatures (updated June 12, 2015).

BYOD program, schools are monitoring student property that is more likely to have noneducation-related materials and perhaps sensitive information, raising privacy concerns.[13]

Ensuring Student Safety

Perhaps the most compelling impetus for school surveillance is the desire to keep students safe, not only online, but also in the physical school environment. Broad "safety" and "security" concerns are cited as chief reasons for many school surveillance techniques. In 2012, 749,200 US students ages 12 to 18 were "victims of nonfatal school violence." Schools and districts naturally feel compelled to act. Numerous studies show that school-based violence harms students psychologically and compromises their "feelings of safety and connectedness."[14] The internet poses many dangers, as do malicious texts or malware that arrives on student devices.

Recently, one of the most legislated areas of student safety has been cyberbullying. Unlike traditional school bullying, where students could at least escape it by going home, cyberbullies can follow children via the device in their backpacks.

News reports relate numerous examples: A sixth grade boy came to school one day to find out that another sixth grader had posted a Facebook status the previous night asking his friends to "like" it if they hated the boy. As of that morning, 57 people had liked the status. A 13-year-old girl's Facebook photo was adorned with another girl commenting "hideous" and "this pic makes me throwup a lil." The girl stated that, if she had to choose between the life of an animal and that of the girl in the photos, she would choose the animal's because "yeah, at least they're worth something." A 12-year-old girl committed suicide in 2013 by jumping off a cement plant platform after being cyberbullied for over a year. A survey in 2011 found that while two-thirds of the teenagers surveyed were "mostly kind" to each other on social networks, 88 percent of them said they had witnessed "people being mean or cruel," and one in five said they had been one of

[BOX 1]

Filters and Monitoring

The Children's Internet Protection Act requires that all public libraries and schools receiving E-rate funds—approximately 95 percent of schools—implement an internet safety policy that includes "protection measures [that] must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors." While "child pornography" is fairly well-defined, what is "obscene" or "harmful to minors" will vary from community to community.[a] There is no preordained list of filters. Consequently, schools have been pinged for overfiltering student internet access, with some students unable to access websites for school projects on topics such as breast cancer.

In a report on the impacts of CIPA 10 years later, the American Library Association noted that "the over-filtering that occurs today affects not only what teachers can teach but also how they teach, and creates barriers to learning and acquiring digital literacy skills that are vital for college and career readiness, as well as for full participation in 21st-century society."[b] Another report on youth and the internet compared the internet to a swimming pool: "Swimming pools can be dangerous for children. To protect them, one can install locks, put up fences, and deploy pool alarms. All of these measures are helpful, but by far the most important thing that one can do for one's children is teach them to swim."[c] To help students learn how to navigate the internet, an amendment to CIFA in 2008 requires schools to address students' digital literacy.

CIPA also requires schools to monitor students' online activities, and how they do so must be referenced in schools' internet safety policies. Schools do not need monitoring software to fulfill the requirement—it can be satisfied through in-person supervision—but most schools use a "keyword" system, which flags certain inappropriate words used on a device or in student emails and sends an alert to school administrators. The Federal Communications Commission, which oversees CIPA compliance, has yet to offer guidance on schools' responsibilities to monitor student one-to-one devices, particularly when those devices are used at home.

a. The E-rate program provides participating schools and libraries with discounts on "telecommunications, telecommunications services and Internet access," as well as for "internal connections, managed internal broadband services and basic maintenance of internal connections." The discounts that libraries and schools receive are significant, ranging from "20 to 90 percent, with higher discounts for higher poverty and more rural schools and libraries." (FCC, "FAQs on E-Rate Program for Schools and Libraries," https://www.fcc.gov/consumers/guides/universal-service-program-schools-and-libraries-e-rate; John Harrington, "The Internet Is Speeding Up—and Schools Are Demanding Faster Connections," Commentary, Edscoop.com (August 2, 2016).

b. Kristen R. Batch, "Fencing Out Knowledge: Impacts of the Children's Internet Protection Act 10 Years Later," Policy Brief No. 5 (Washington, DC: American Library Association, June 2014).

c. Dick Thornburgh and Herbert S. Lin, eds., *Youth, Pornography, and the Internet* (Washington, DC: National Academies Press, 2002).

those mean people. Victims of cyberbullying tend to be more unwilling to attend school, are more likely to experience a drop in self-esteem, and are more likely to use drugs and alcohol.[15]

Forty-six states and the District of Columbia have passed laws prohibiting cyberbullying, many of which give schools responsibilities for identifying instances of bullying.[16] At a minimum, schools will face community criticism and scrutiny if they miss an instance of bullying that results in suicide or attempted suicide, particularly if the bullying occurred on their network or a school-owned device. They may also see federal consequences: A 2010 "dear colleague" letter from the Office for Civil Rights in the US Department of Education (ED) noted that bullying may, under certain circumstances, "trigger legal responsibilities for schools under the civil rights laws enforced by OCR and the Department of Justice that prohibit discrimination and harassment based on race, color, national origin, sex, disability, and religion."[17]

Another online area where student safety comes into play is sexting. Generally defined as "the sending of sexually explicit messages or images," sexting has increasingly become an issue in schools.[18] In a 2014 survey, 54 percent of respondents reported sexting as a minor, and 71 percent reported knowing others who had experienced negative consequences because of sexting.[19] Because the law considers sexting by children under 18 to be distribution of child pornography, sexting has serious consequences for the sender.

Some states have chosen to prosecute minors to the law's fullest extent, including registering those convicted as sex offenders for life.[20]As of 2015, 20 states had passed a law that addressed minors sending and receiving sexts,[21] but, in many other states, punishments are subject to a prosecutor's discretion (map 2).[22] Because students may use school networks or devices to send or receive these sexts, share photos during the school day with classmates, or take the photos while on campus, schools may choose to add keywords or use other methods that could identify sexts while monitoring student devices or internet access.

A third safety reason for monitoring online behavior is to predict and avoid school violence. Many school shooters telegraph their plans directly or indirectly through social media or on the internet sites they access. One district noted that their program "monitors keywords that could present threats, for example 'gun' or 'attack' or 'kill' or words of that nature."[23]

> "Administrators often hope that visible security measures, such as video surveillance, can be used to make students feel more secure and perhaps also deter bad behavior."

A January 2016 report from the FBI noted that "targeted violence is the end result after a process of thinking and behavior," and "[u]naccountable or unobserved space provides a window of opportunity for students engaging in activities contrary to their family norms or desires, thus creating additional vulnerabilities and opportunities for exposure to violent extremists or violent rhetoric."[24] Schools often use the same internet and device monitoring technologies to detect these behaviors that they use to keep students on task.

Some districts also monitor students' social media accounts. While some schools have employees "friend" students online to monitor their social media activity, a growing number of schools employ companies like Geo Listening to monitor their students' social media accounts.[25] Geo Listening aggregates and saves "a record of publicly available social media information," which it then "filters" and provides to "participating schools or school districts with an accurate and timely report of posts that can help them intervene on behalf of students with regard to their specific need."[26] The company collects "a username, date and timestamp, geolocation data and the full content of the public post" from Twitter, Facebook, Instagram, Vine, Ask.fm, YouTube, and Google+, and it provides the information it collects only to participating school or school district clients. Orange County Public Schools

[BOX 2]

Apple Classroom App for iPad

Many schools try to balance the need for device monitoring with the need to ensure privacy. Some companies are helping schools maintain this balance. Apple, for example, this year launched an app called Classroom, which allows teachers to "guide learning, share work, and manage student devices." There are two innovative privacy elements to the app. While in class, teachers can see any student's iPad screen from the teacher's device to ensure that students are on task. But once students leave the Bluetooth range of the teacher devices, they can no longer be monitored. In addition, students receive a notification at the top of their devices when teachers are looking at their iPads.

in California began using another social media monitoring company, SnapTrends, as an early-warning system after the 2012 Sandy Hook Elementary School shooting in Newtown, Connecticut.[27]

However, online surveillance may not be sufficient to keep students safe. Administrators often hope that visible security measures, such as video surveillance, will make students feel more secure and perhaps also deter bad behavior. Students who feel safe at school "have higher attendance rates, better academic performance, and may experience fewer classroom disruptions from other students."[28]

Most K-12 school districts around the country are employing some sort of video surveillance monitoring system to protect students and secure the campus.[29] By the 2013–14 school year, 75 percent of schools were using one or more security cameras to monitor in-school activity, up from 61 percent in 2009.[30] After the Sandy Hook shooting in 2012, state legislatures in 2013 introduced 62 school safety bills that included safety upgrades, including installation of video surveillance cameras,[31] and state laws passed in 2016 continue to authorize spending for a range of school security measures.[32] In one district, video surveillance was used when a student ran away, allowing the school to tell the police "every car she visited and every person she spoke with [after leaving her last class], up until she got into a car to leave the premises."[33]

Few districts have added cameras in classrooms versus school hallways, but the number is growing. Texas, for example, passed a law in 2015 mandating that all schools video- and audio-record classroom interactions between special education students and their teachers if requested to do so.[34] The primary purpose of the law is to protect special education students from abuse in the classroom, but advocates claim it should also be praised as a tool for both teachers and students who face false accusations of inappropriate conduct: They will be able to point to the camera recording as evidence.[35] For example, in one school, a music teacher who taught in a separate building from many of his colleagues requested the school install a camera in his classroom as a safeguard: "[E]ven an accusation, whether it's true or not, can end my career."[36]

In Iowa, one school district bought body cameras for administrators. Inspired by an incident where a principal was wrongfully accused of kicking a student, school administrators from this Iowa district asserted that recording can be a valuable tool for "personal accountability."[37]

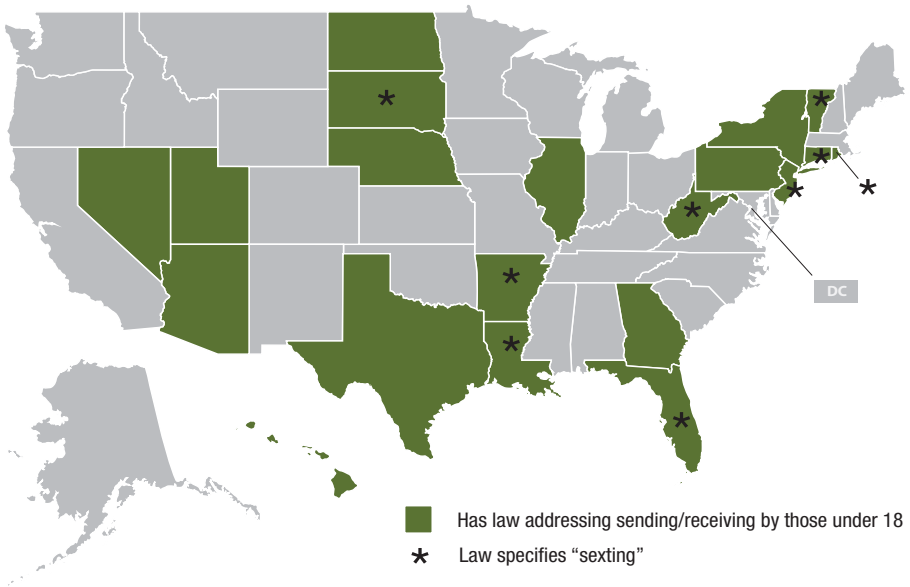
The utility for staff protection notwithstanding, advocates say student safety is the primary motivation for video recordings. However, some concerns have been raised about whether this is a step too far. One commentator asks, "If a principal is wearing a body camera, will a student be more or less likely to discuss abuse or bullying?. . . Students need to feel like they can confide in principals and vice principals without the conversation being recorded."[38]

Many schools also have video surveillance on school buses: As of 2015, two-thirds of school buses were equipped with interior surveillance systems.[39] Student safety is the primary purpose—25 percent of bullying is done on school buses—but bus cameras are also used to reduce student disciplinary incidents and protect staff. In Harford County, Maryland, a committee found that there was a 61 percent decrease in the number of referrals given to students for behavioral problems after surveillance was installed on some school buses in the district.[40] Video surveillance on buses can reveal staff malfeasance as well, as one New York school district discovered when a bus driver accused of slapping a student was caught on camera.[41]

Some school systems have installed audio recording devices in their buses as well.

[MAP 2]

20 States Have Laws Addressing Sexting by Minors



Source: Cyberbullying Research Center (updated July 2015).

In 2014, for example, Boston equipped its 750 school buses with both cameras and microphones to address and investigate "reports of bullying, other disciplinary issues, and even traffic accidents."[42]

Allowing Auditing and Efficiency

Schools also use surveillance for auditing and efficiency. For example, surveillance is used to prevent or catch cheating or monitor for inappropriate content (such as looking at pornography on a school device). Tracking school buses (and those who ride them) not only increases student safety, it also improves efficiency. Tools with GPS capabilities and automated routing systems allow districts to streamline an often inefficient system by tracking how many students board buses at particular stops and comparing these numbers to bus route maps.

While transportation efficiency is the driving purpose, districts using these tools are not-so-incidentally tracking whether and where students are getting on buses.[43] Some schools employ radio-frequency identification technology (RFID) to document and manage student movement and campus access. Schools in Georgia, for example, are using RFID badges to track children as they board their bus and are informing parents of where and when their kids got on or off and whether they eventually made it into the school. The company providing the badges noted in a *Times Free Press* interview that the badges could be used to track student whereabouts during emergencies, such as the large snowstorm that stranded hundreds of Atlanta students on school buses one day in January 2014 as road conditions deteriorated.[44]

A few schools have begun to use biometric technologies to increase efficiency and protect students. The US Department of Education defines a "biometric record" as "one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual." For example, Blinkspot, a leading company in "pupil pupils," has developed iris scanners for school buses. The reader scans students' eyes and sounds an alert to indicate whether they got on the right bus. Blinkspot's scanner also syncs with a mobile app that updates parents. As with other tools used to track students' movements, biometric technology could be key to reassuring or aiding parents and school administrators, especially in emergency situations such as natural disasters or school shootings, or ensure student safety by, for example, keeping children from being accidentally left on a bus.

> "Surveilled students may feel they are in a less nurturing, comfortable learning environment."

POTENTIAL PRIVACY AND EQUITY CONSEQUENCES

Clearly, school districts are using surveillance for many good reasons. However, just as with surveillance measures in broader society, there are several ways that the technologies in schools can be abused. Speaking about the dilemma in society at large, two highly regarded privacy scholars noted, "There is a line between surveillance that is essential for the public good and invasive total-information awareness technologies, and that line is easy to cross if unattended."[45] If schools continue to embrace the potential benefits that accompany surveillance technology, state policymakers must be prepared to confront, and potentially regulate, the privacy consequences of that surveillance.

The Surveillance Effect

When Edward Snowden met with reporters to discuss the National Security Agency's public monitoring practices, he notoriously insisted on everyone putting their cellphones in the hotel fridge to block radio signals that could activate the devices' microphones or cameras.[46] While high school students are unlikely to take such extreme measures, decisions about whether to use surveillance should weigh the potential negative consequences of students becoming accustomed to surveillance or taking extreme measures to avoid it.

An obvious potential consequence is that surveilled students may feel they are in a less nurturing, comfortable learning environment. Security measures can interfere with the trust and cooperation learning requires by creating barriers among students, teachers, and officials, and casting schools in a negative light in students' eyes.[47]

As some commentators have pointed out, private is not the opposite of public.[48] For example, a bench in a city park may be "public," but the conversation you have with a friend while sitting on it may be considered "private." Likewise, while the typical school campus environment is considered public, many private moments occurred in the pre-surveillance age. But students' awareness of surveillance may make them act differently than they otherwise would in the absence of surveillance. Not everyone reacts to surveillance the same way, however: It "can evoke anger, embarrassment, guilt, shame, fear, but also a sense of security and safety."[49]

In some cases, the purpose of video cameras on buses or in school hallways is to have students act differently. They should, for example, be deterred from vandalizing property or bullying others. Several studies suggest that being aware of surveillance can improve behavior.[50] One study found that placing a mirror behind an unguarded bowl of candy led children to select fewer pieces of candy.[51] In another, a poster of staring human eyes in a cafeteria caused lunch-goers to clean up after themselves at twice the rate as before the introduction of the poster.[52]

Despite the potential benefit of deterring bad behavior, surveillance in schools also poses a threat to intellectual privacy and encroaches on the space to voice opinions and challenge convention. According to privacy expert and law professor Neil Richards, surveillance can cause "our thoughts and beliefs [to] get driven to the boring, the bland, and the mainstream."[53] When Ernest Hemingway discovered the FBI was monitoring him, he reportedly found it impossible to write.[54] Risk taking lies at the heart of inquisitiveness and creativity. If students feel as though they cannot step outside of the mainstream for fear of ridicule or are afraid to ask a question because their ignorance might be captured forever in the virtual cloud, then surveillance has gone too far.[55]

Furthermore, surveillance could alter or freeze a child's self-image. Bryan Warnick, a professor at Ohio State University who has written extensively about school surveillance, notes that educational environments are "meant to promote growth and change," but surveillance makes every moment static. For example, a video recording of an event in a student's past could bring up feelings of associated shame or regret any time it is replayed. "Places of human growth and development [like schools] need to be places that possess a certain type of forgiveness," Warnick says. "The presence of video cameras and recordings sends a message of neither forgiveness nor forgetfulness."[56]

Because surveillance in many contexts is focused on monitoring suspicious groups to prevent criminal activity, there is also a risk that surveilled children will view themselves as suspicious or delinquent.[57] "You want schools to be safe," said education expert Pedro Noguera, "but at the same time you want them to be places where kids feel as though they can learn and be supported." Bringing police onto campus and placing youth under continuous surveillance "begins to turn schools into institutions that are more like prisons," he said.[58]

> "Inherent or implicit biases may cause a principal or law enforcement officer to think that a black student reaching into someone's backpack is stealing when the same action by a white student fails to raise the same suspicion.

Edward Ward, a DePaul University honor roll student, attended one such school in Chicago's West Side, where most students were minorities: "From the moment we stepped through the doors in the morning, we were faced with metal detectors, x-ray machines, and uniformed security." Ward added that he "could slowly see the determination to get an education fade from the faces of [his] peers because they were convinced that they no longer mattered."[59]

The surveillance effect becomes especially pronounced when surveillance extends off-campus. When students know that their social media accounts and off-campus device use are being monitored, they may self-censor or otherwise limit their explorations.

While this is not always a bad thing—students' learning to censor their bullying impulses would generally be considered a good outcome—such surveillance can also create inequity: That is, students whose parents can afford to buy them nonschool devices will feel freer to communicate. Students who depend on school devices will be more likely to suppress outside-the-box impulses, or, if they do express them, they may be more likely to face negative consequences for these behaviors. In addition, certain types of surveillance, such as body cameras on school administrators or teachers, could inhibit student reporting of bullying or abuse situations.[60]

It is vital that policymakers consider how different types of surveillance may censor students' expressions and actions and weigh the costs and benefits before implementing a particular technology in their state or district (box 3).

Equity and the Digital Divide

Not all students can access the internet or use devices at home. As of 2012, 100 million US households still did not have high-speed internet access and almost half of the poorest households did not own a computer, according to a 2015 study.[61] In addition, lower income Hispanic and African American households were more likely to own only mobile devices, causing their internet viewing to differ from those with access to a laptop or desktop computer.

In 2015, the American Civil Liberties Union introduced model legislation on student data privacy, including language proscribing searches of one-to-one and BYOD devices, that was introduced in nine state legislatures in 2016 (box 4).

Chad Marlow, ACLU advocacy and policy counsel, said there should not "be two separate rules for two types of kids: one for the wealthy kids who could afford their privacy because they could say, 'I want to be private, so I will just bring my own device to school' and the kids who could not afford their own device who then [would] be forced to make the trade-off between getting a device that they really need for their education and giving up their privacy.… [P]rivacy protections are something that should be afforded to all students regardless of their economic circumstances."[62]

A 2015 report concluded: "If schools place constraints on what children can do with school-provided technologies,

the full range of digital possibilities is effectively reserved for more privileged students and families."[63]

The report detailed a one-to-one laptop program in a heavily Hispanic community in Arizona. While the district touted the benefit of giving technology to families who were unable to afford it, surveillance concerns hindered families from using it. Because they had to sign that they understood their school was monitoring the devices for inappropriate usage, families viewed the school devices as a threat to family privacy and security. Students therefore used the one-to-one devices only or primarily for schoolwork and "the subsidized laptops did not meet their full potential to connect families to online resources."[64]

The Effect on Discipline Disparities

Some advocates have expressed concern that if districts and states do not set policies limiting and describing the purposes for which surveillance will be used, surveillance could aggravate existing school discipline disparities between groups of students.

According to the most recent US Department of Education data, black K-12 students are suspended and expelled at a rate three times greater than white students.[65] During the 2013–14 school year, black males represented 19 percent of the national preschool enrollment but constituted 45 percent of male preschoolers receiving one or more out-of-school suspensions.[66] The rates are similar for black girls, who represent 20 percent of the total female enrollment but accounted for 54 percent of female out-of-school suspensions. While the same survey found that English learners and students with disabilities were not suspended at higher-than-expected rates in preschool, disparities in discipline rates did arise during the K-12 years.

Students with disabilities are as much as two times more likely to be suspended than their nondisabled peers.[67] One in five "multiracial" female students with a disability was suspended during the 2013–14 school year while only one in twenty white female students with disabilities faced similar suspensions.[68] Again, boys face even greater disparities: While one in ten white boys with disabilities saw out-of-school suspensions in 2013–14, that rate virtually

[BOX 3]

Student Surveillance and the US Constitution

School surveillance implicates two Constitutional rights: free speech under the First Amendment and freedom from unreasonable searches or seizures under the Fourth.

Generally, schools have not been found to violate rights to free speech when they surveil student speech on social media or while using the school internet or a school-owned device, and they may use that information to limit or stop inappropriate student speech. In *Tinker*, the Supreme Court held that student speech may be limited if it "materially disrupts classwork or involves substantial disorder or invasion of the rights of others." Many courts have held that even the risk of a substantial disruption may be sufficient to allow schools to limit or punish speech.[a] The Supreme Court has also found that schools are able to regulate lewd student speech and can punish off-campus speech that supports drugs at school-sponsored events.[b]

The Fourth Amendment does not allow the government, including public schools, to conduct unreasonable searches or seizures. The Supreme Court has held that school officials do not need a warrant or probable cause to search students in school. Instead, they must meet a lower two-part reasonableness standard. Courts have generally upheld that cameras placed in public locations—where students would not have a reasonable expectation of privacy—do not violate the Fourth Amendment and that classrooms are public places though a school restroom or locker room is not.[c] The combination of these tests—reasonableness of the search and whether a student had a reasonable expectation of privacy—tends to dictate how most courts decide student search cases.[d] Since most schools notify students (through device policies or network access policies) that they have no right to privacy while on the school network or while using a school-owned device, it is likely that the Fourth Amendment has not been violated. It is noteworthy, however, that monitoring student devices off-campus without cause could lead to charges that schools are violating the Fourth Amendment.

a. Caroline E. Mendola, "Big Brother as Parent: Using Surveillance to Patrol Students' Internet Speech," *Boston College Journal of Law and Social Justice* 35 (Fall 2015): n. 138.

b. In *Bethel School District v. Fraser* and *Hazelwood School District v. Kuhlmeier*, respectively.

c. *Brannum v. Overton County School Board.*

d. Emily F. Suski, "Beyond the Schoolhouse Gates: The Unprecedented Expansion of School Surveillance Authority under Cyberbullying Laws," *Case Western Reserve Law Review* 65 (Fall 2014).

doubles for minority and multiracial boys with disabilities.

Schools often suspend students in response to relatively petty infractions. While suspensions triggered by safety concerns are infrequent, "students are routinely removed from school for minor offenses like tardiness, truancy, using foul language, disruption, and violation of the dress code." [69] According to former US education secretary Arne Duncan, 95 percent of all suspensions are attributable to such nonviolent offenses.[70] Moreover, black students during 2013–14 were 2.3 times more likely than white students to be referred to law enforcement or arrested as a result of a school incident.[71]

Some studies find correlations between high levels of school security and a higher percentage of minorities being suspended.[72] Further, schools serving primarily students of color are more likely to rely on intense surveillance methods such as surveillance cameras and x-ray machines than other schools, according to a 2016 study by Jason P. Nance. These disparities persist even after controlling for school or neighborhood crime rates and rates of other incidents such as bullying.

Meanwhile, 62 percent of major incidents of school violence occur in schools that serve primarily white students. Nance thus concludes that the disparity is rooted in implicit bias—that is, "unconscious biases that people are unaware they hold but influence their perceptions, behaviors, and decision-making." Such bias provides "a powerful explanation for the persistence of many societal inequities, even among individuals with egalitarian intentions."[73]

One extensive study of Texas school and juvenile justice records found that African American ninth grade students were 31 percent more likely to be disciplined in school than their white and Hispanic peers. Strikingly, the authors found that African American students were actually less likely than their white or Hispanic peers to commit the disciplinary infractions that trigger mandatory school suspensions.

The authors postulated that adult subjectivity explained the disconnect: "High rates of disciplinary involvement among African-American students were driven chiefly by violations that are subject to the discretion of school employees. It is important to explore, with educators, parents, students, and others, what might be contributing to this disproportionality."[74]

Someone who exhibits implicit bias may not be inherently prejudiced. "One can have a positive attitude towards African-Americans but still associate them with weapons [or] may associate Asian-Americans with high achievement … but still feel poorly towards this group."[75]

Teachers often display such implicit bias, by holding lower academic expectations for minority students or by being more likely to support punishment when an African American student has a second disciplinary incident as compared with a white student.[76]

According to Steve Smith, chief information officer for Cambridge Public Schools in Massachusetts, the issues with surveillance in schools are a microcosm of the issues nationally. The problem, he says, is not with the technology itself but with how people use it.[77] Inherent or implicit biases may cause a principal or law enforcement officer to think that a black student reaching into someone's backpack is stealing when the same action by a white student fails to raise the same suspicion. According to Teddy Hartman, privacy officer for Howard County Public Schools in Maryland, surveillance produces "the potential that some biases may be reinforced, depending on who or what people are looking for as suspicious, or not suspicious."[78]

Another reason to be concerned about

[BOX 4]

ACLU Model Bill

The ACLU student privacy model legislation was the first such effort to address privacy of one-to-one devices and BYOD surveillance. However, many organizations and districts have argued that the ACLU went too far in restricting school surveillance, potentially inhibiting efforts to curb cyberbullying as well as potentially violating schools' CIPA obligations.[a]

In a DC Council hearing, Friendship Public Charter Schools' founder Donald Hense argued against a model ACLU bill that would require DC schools to bring in law enforcement before they searched a student device for a violation of school policy that could also be illegal. Hense said that involving law enforcement could further stoke the school-to-prison pipeline. For example, it is easy to imagine a scenario in which a school administrator wants to search a student's device for evidence of sexting but without involving law enforcement.

However, the ACLU argues that the bill actually reduces the school-to-prison pipeline by encouraging administrators to contact parents instead of conducting device searches (with or in lieu of law enforcement) and by requiring administrators to document the "reasonable suspicion" that induced them to pursue a device search in the first place.[b]

a. Education Public Hearing on B21-578, "Protecting Students Digital Privacy Act of 2016," Council of the District of Columbia, March 21, 2016.

b. Chad Marlow, interview by Amelia Vance, October 7, 2016.

increases in suspensions stoked by surveillance practices is the inseparable consequence of missing school time. Actual time spent in school is "one of the surest and most consistent predictors of academic success," while school suspensions have been linked with academic disengagement, delinquency, and school dropouts.[79] An eight-year study of Florida high school students found that a single suspension was associated with a dropout increase of 16 percent; students who were suspended twice in ninth grade were found to have a 42 percent chance of dropping out of school.[80] In addition to the personal, social, and professional consequences for these children, dropout rates are also linked to significant economic costs for the nation at large in terms of missed tax revenue and lost productivity.[81]

Increased surveillance in schools can exacerbate the disparities in disciplinary actions simply by uncovering more instances of minor infractions.[82] While internet monitoring software and body cams can help deter and capture evidence of serious safety concerns, they also provide evidence of less serious violations, like using a cellphone when not permitted. By capturing more instances of such behaviors, surveillance can have an exaggerated effect on suspension rates, particularly in schools with zero-tolerance policies, where discretion is taken out of the hands of teachers and administrators.[83] When schools criminalize typical adolescent behavior, pushing and shoving becomes battery and speaking disrespectfully to a teacher becomes disorderly conduct.[84]

There is also the danger of technology turning tattle-tale, as opposed to being a passive record of activity. For example, device monitoring technologies can send emails to administrators, teachers, or parents to report, for example, that a student is visiting an inappropriate webpage. Future technology could go further: Video surveillance may soon be able to automatically analyze the footage recorded and, using facial recognition technology, note breaches of school policy in each student's record.

> "Failure to address the disparate use of surveillance practices sends a signal that 'white students are privileged and have greater privacy rights while students of color cannot be trusted.'"

The problem of bias, coupled with the increased presence of school resource officers and surveillance technology, heighten concerns that school discipline is increasingly shifting toward involving students with the justice system—stoking what has been termed the school to prison pipeline. Indeed, 43 percent of US public schools have school resource officers.[85] As more police are required to wear body cameras, new records of student interactions may be created that are not subject to privacy regulations.[86]

It is possible that, by allowing schools to monitor and track students in a more objective way, surveillance technology could be used to produce more egalitarian discipline or encourage better self-discipline as students become aware their actions are being monitored. The existence of surveillance records could empower students accused of infractions to request that administrators view footage to see what actually happened and thereby clear up misunderstandings. For example, one district used surveillance to determine that a student had not violated school policy by leaving the campus to buy fast food for lunch: The camera showed that his brother had dropped off food for him.[87]

Yet the disproportionate use of intense surveillance methods on students of color presents a profound problem. Failure to address the disparate use of surveillance practices sends a signal that "white students are privileged and have greater privacy rights while students of color cannot be trusted."[88] It is essential that any discussions about surveillance take into account how it may further discipline disparities and find ways to mitigate and avoid them.

The Permanent Record

A fear often expressed in the public discourse on student surveillance is that a "permanent record" will haunt students for the rest of their lives.[89] The specter of permanent records is in many ways an old trope with new energy: In the 1986 movie *Ferris Bueller's Day Off*, a menacing principal threatens students with poor marks on their permanent record. At its core, the worries surrounding the permanent record reflect fears of future failure and a lack of trust. That is, students and parents fear that an inescapable shadow of past judgments and unflattering evaluations by school officials and teachers will stifle human potential. They also fear that no one can be entrusted long-term with student data. Asked to describe the informational profile of a typical American college student, Joel Reidenberg, director of the Center on Law & Information Policy at Fordham Law School, responded, "We're in an environment of surveillance, essentially. [You can expect] an extraordinarily rich data set of your life."[90]

A 2015 survey conducted by the Future of Privacy Forum found that "68 percent of parents are concerned that an electronic record would be used in the future against their child by a college or an employer."[91] As two legal scholars note, "Video surveillance 'sees all and forgets nothing,' and it is the responsibility of today's school officials to determine if the level of intrusiveness is justifiable 'in light of the purpose of the policy being carried out.' "[92]

Just as the increasing omnipresence of

surveillance means that there are more opportunities for students to be "caught" misbehaving, inexpensive digital storage methods have diminished the previous incentive for not keeping a record: lack of space in the filing cabinet. In essence, data storage capacity is nearly infinite. "If storage is free but analysts' time is costly," says Princeton computer science professor Edward Felten, "then the cost-minimizing strategy is to record everything and sort it out later."[93] If adequate safeguards are not put in place, the data collected through surveillance could become "permanent" by default (box 5).

The prospect of enduring, accessible, essentially free storage amplifies the potential for abuse that accompanies permanent records. Society recognizes that children do not possess the wisdom and experience that come with maturity and adulthood and formalizes this view through laws that void contracts made with minors and expunge court records of juveniles. Digital data storage, conversely, fosters an environment where memories are long. Without proper deletion requirements, employers or college admissions staff are free to determine which data represent a student's character versus which were learning moments, and they may erroneously proceed to do so on the assumption that the records are accurate and still applicable. This is troubling, especially since most adolescents, despite incidents of juvenile delinquency, mature into law-abiding individuals, so that "yesterday's record does not accurately describe today's individual."[94]

Yet surveillance policies and laws infrequently list what information becomes part of the student record and even more rarely discuss when surveillance must be deleted. The Texas 2015 law requiring video and audio recordings of special education classrooms requires only that recordings be retained for at least six months; it does not include a maximum retention time.[95]

WHAT STATE POLICYMAKERS SHOULD CONSIDER IN RESPONSE

Figuring out how to balance surveillance's pros and cons is not limited to the education context; many of these debates are going on in broader society. Most citizens recognize that some degree of surveillance is useful. Few, for example, would characterize internet monitoring that identifies child predators or bank surveillance cameras as unconscionable invasions of privacy. On the other hand, many express alarm at the idea of the government indiscriminately spying on phone conversations and messaging. Similarly, most seem to accept a measure of surveillance in schools to promote safety while rejecting monitoring when they feel it becomes too invasive.

A sensible policy response is to come up with guardrails that ensure that surveillance, whether on- or offline, helps children rather than posing obstacles to their progress. There are many options state policymakers can consider in order to create these guardrails.

One of the strongest powers that policymakers have is the public platform they are granted when they assume office. State board of education members can use this platform to ask three questions about surveillance in their state:

- Which types of surveillance does our state employ?
- What is the purpose for their use?
- Are there policies in place to ensure surveillance is used equitably and respects privacy?

State boards of education are also positioned to identify and convene key stakeholders to answer these questions and determine what policies may need to be created, reformed, removed, or replaced. Key stakeholders will likely include superintendents, principals, teachers, legislators, the governor's office, state education agency staff, parents, and students.

[BOX 5]

Is Surveillance Part of the "Education Record"?

Students have certain rights when something is considered to be part of their education record. Under the Family Educational Rights and Privacy Act (FERPA), students or their parents can review the record and appeal to change inaccurate or misleading information. However, surveillance video or information obtained through surveillance may or may not be considered part of the education record, and the US Department of Education's Family Policy Compliance Office has not yet offered formal guidance on how to determine this. But they have consistently given this informal guidance to school districts: While video surveillance in general is not considered an education record, a video showing a student committing such acts as breaking into a locker or getting into a fight will become an education record if the school uses it for disciplinary purposes.[a] In the absence of formal guidance, state courts have ruled in opposite ways.[b]

a. Upton & and Hatfield, "FERPA—The Family Education Rights and Privacy Act," Memo, (Hillsborough, NH, September 2013), **http://www.nhsba.org/documents/kidderdocs2013/4AFERPA.pdf.**

b. Brad Banasik, "Students, FERPA and Videotape," Michigan Association of Secondary School Principals blog, March 12, 2008, **http://mymassp.com/content/students_ferpa_and_videoptape_0**.

Finally, most state boards have rulemaking or policymaking authority, whether in general or on student privacy in particular (map 3). Once state boards have obtained answers to the key questions and discussed the issue with stakeholders, they can suggest or adopt rules to ensure privacy and equity.

Education professor Bryan Warnick suggests five principles for regulating surveillance in schools: minimization, proportionality, transparency, openness, and empowerment.[96] To those, we add equity. In addition, staff training will be essential to ensure that policies reflecting these principles are faithfully implemented.

Minimization

"[S]urveillance practices should only be used when there is evidence of a clear and immediate danger to student safety or to the conditions necessary for student learning," Warnick advises.[97] Further, they should be discontinued if the reason for adopting surveillance subsides.

Protecting privacy requires limiting how much data are collected in the first place as well as limiting data that are retained. The Student Data Principles, a list of 10 fundamental values on student privacy that over 40 education organizations (including NASBE) signed in 2014, includes a minimization provision: "Educators and their contracted service providers should only have access to the minimum student data required to support student success."[98]

The principle of minimization asks policymakers to consider whether surveillance is the answer to the problem. In the case of the 2015 Texas law on recording special education classes, one could argue that, given the high costs of installing audio-video cameras, money would be better spent on additional on-the-job training and better salaries to attract more-skilled practitioners. However, at least one teacher that testified in support of the Texas law noted that her reports of teachers' abuse of students were ignored and that cameras would create more of a deterrent.[99] State policymakers could easily come down on either side, but it is important that the potential consequences of surveillance technologies be weighed and other options considered.

Creating state and district-level data governance policies is the first step in ensuring minimization (box 6). This policy encompasses not only the data collected through surveillance but all other student data collected by schools, such as grades, test scores, personalized learning plans, medical information, disciplinary records, and social-emotional indicators. Data governance policies spell out answers to parents' key questions on student data collection:

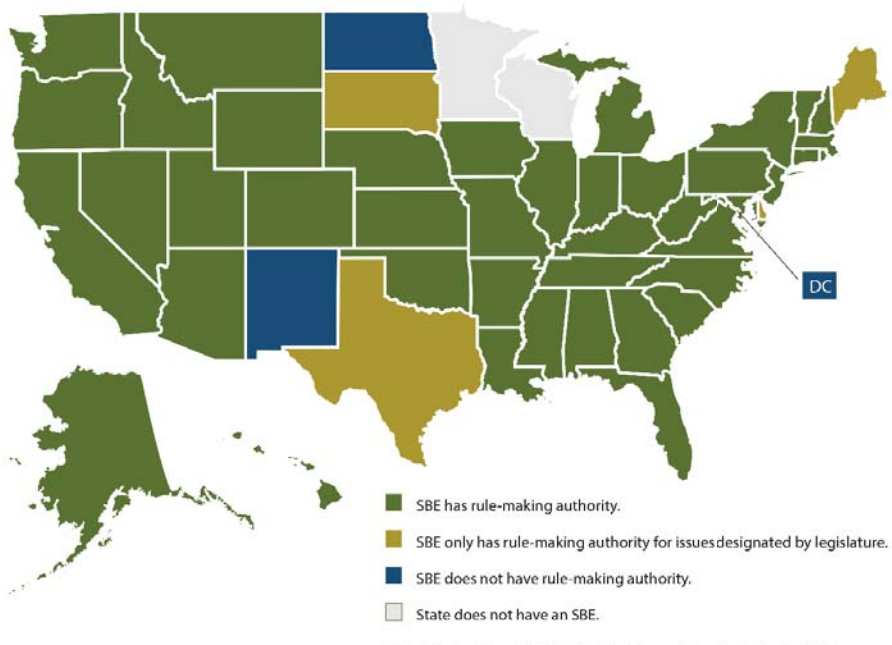
- What data are being collected? What protections are in place to protect it?
- For what purposes are data collected? Are they necessary? (This question addresses minimization specifically.)
- Who holds what student data? (school, district, state, and/or third parties)
- Who can access that data?

In order to determine what data should be collected, state board members may find it useful to start with their questions about education in general—how many state students do not graduate or how efficacious is education technology in the classroom, for example—and then create a governance body or study committee to determine what data (gathered by surveillance technology or otherwise) are needed to answer those questions.

In addition to creating or enhancing data governance policies, policymakers should also audit their surveillance programs to make sure they are noninvasive. As one expert said, "The easiest way to limit harms caused by [surveillance] is to not gather the information in the first place."[100] Whether the purpose is efficiency, performance auditing, or safety, the tools and technologies used to achieve a school's aim

[MAP 3]

SBEs with Rule-Making Authority



should neither compromise nor detract from the goal of creating supportive, nurturing, and safe learning environments. In practice, this principle may mean opting against technologies where parents or school board members determine that the costs to privacy or perceptions outweigh marginal benefits. Creating a lean monitoring system will also make it easier to manage the privacy implications and create workable, efficient policies.

Minimization also encompasses policies that require deletion of surveillance data, another element that should already be part of state or district data governance policies. Such requirements are essential to combating the prevalent fears over students' "permanent record." While some data are useful to keep from preschool to employment, audiovisual records and iris scans could be deleted as soon as a student graduates or leaves the school. Schools and the contractors that help them with surveillance should commit to storage time limits. Proper deletion requirements increase security of private information: Data that do not exist cannot be compromised. Deletion requirements also foster trust and transparency because students and their parents will not feel they are being monitored arbitrarily. In sum, deleting information that no longer serves an immediate goal is a simple way to combat the harms created by permanent records.

States would be wise to follow the example of New Jersey. New Jersey regulations mandate that student records contain only information relevant to a student's education.[101] The regulations also specify that student records must be inspected annually to ensure the data in those records are still relevant, and they require that all irrelevant information be deleted. Having this type of annual review—either mandated through law or regulation or suggested as best-practice guidance from the state education agency or state board—could help mitigate potential harms from surveillance data.

State boards should discover if their state has limitations or guidance on how long surveillance information is kept (such as whether there is a deletion requirement for video surveillance or data collected from a student device). If there are no limitations, state boards should use their rule- or policymaking authority to create time-specific limitations or other types of privacy-protective limitations.

Proportionality

Warnick argues that "the use of surveillance practices should be proportional to the severity of the problem and to consequences for the student."[102] That is, the invasiveness of a search must be balanced against "the degree and immediacy of the danger or distraction," and the justification required to perform a search should be proportional to the consequences for students. Districts or schools should have data governance policies that cover their current surveillance practices, plus contingency plans to address potential privacy violations. The data governance policy can also address when surveillance should occur in the first place. States can recommend or mandate such policies, which, when faithfully implemented, can go a long way toward building proportionality, as well as trust and transparency.

[BOX 6]

State Policy Examples

State education agencies, legislatures, or state boards of education have taken the lead in forming data governance policies:

- West Virginia Department of Education, under the authority of the West Virginia Board of Education, created a data governance policy that covers state, district, and school responsibilities, data destruction, and third-party contracts.[a]
- Idaho's state board created a model data governance policy for all districts that aligns with legislative guidance.[b]
- Louisiana released a data governance guide in order to clearly lay out districts' responsibilities and highlight best practices.[c]

Unfortunately, no data governance policies that we discovered incorporate privacy measures for data collected through surveillance. This is a great opportunity for state board members to step up to create a data governance policy in their state or add surveillance data protections to preexisting policies.

a. West Virginia Department of Education, "Data Access & Management Guidance," (January 21, 2014), **http://static.k12.wv.us/tt/2014/datamanagement_guidance%20FINAL%201-21-14.pdf**.

b. Idaho State Board of Education and the Data Management Council, Model Student Data Privacy and Security Policy, August 14, 2014, **https://boardofed.idaho.gov/policies/documents/policies/Student%20Data%20Model%20Policy%200814.pdf**.

c. Louisiana Department of Education, Louisiana's Plan to Protect Student Privacy, November 2015, **http://www.louisianabelieves.com/docs/default-source/data-management/2015-student-privacy-planning-guide-(web).pdf**.

The proportionality principle is especially important in the context of one-to-one devices. State policymakers should recommend or adopt rules on when one-to-one devices should be searched or monitored and how. Every school district should also have a policy on how and when searches occur for devices students own or use for more than educational activities. State policymakers can create or highlight model policies for districts or require that all districts follow one policy.

Transparency

Without transparency, there can be no trust. Parents and other stakeholders have doubted whether to trust schools with their child's privacy. Partly, this distrust stemmed from the dearth of answers from many states, districts, and schools on what data were being collected, how they were used, and how they were protected.

Warnick's transparency principle mandates informing the population under surveillance of the practices and the policies that govern its use. Transparency respects the "personhood of those within the population" but also "prevents feelings of betrayal when a violation of privacy is unexpected, and thus allows for a greater degree of trust between students and schools."[103]

Biometric systems consultant Bob Marotta, who has worked with police departments, federal law enforcement, and US Central Command, explained that "fear of the technology stems from not understanding it."[104] In an age where technology is becoming as prevalent in the classroom as desks and chairs, schools must teach students data literacy. Without data literacy, giving students and parents technical data policies is insufficient. If students do not understand the consequences of web browser monitoring or GPS tracking, they cannot give informed consent to surveillance. And if students and parents do not understand the degree to which they are being monitored, learning of it after the fact will likely lead to confusion and outrage.

> "Policymakers can require that surveillance disclosures list data that will be collected, how they will be used, and how they will be protected."

An absence of transparency can bite states and districts. For example, the Massachusetts ACLU found that only one of fourteen districts reviewed in a 2015 study could provide a written policy governing the use of in-school surveillance cameras, and at least four used cameras without any policy at all.[105] When it came to uploading spyware and device monitoring software onto one-to-one devices, the ACLU found that as many as eight districts were using such software, with at least four monitoring off-campus internet browsing, but these schools were often not upfront with students and parents about the extent of potential surveillance. This survey not only cast the surveyed districts in a bad light in the media, it also sparked the introduction of the ACLU model bill on one-to-one device monitoring, which some advocates said went too far (box 4). It is both smart and efficient for states and districts to preempt such negative attention with a healthy dose of transparency.

Claire Borthwick, associate product manager and counsel at GoGuardian, a software company that provides schools with Chromebook management and web filtering, also emphasizes the importance of transparency. She advises that schools "engage directly with parents about their technology procedures and monitoring policies. This might mean including information in the back-to-school newsletter, sending instructional guides home throughout the year, obtaining permission forms, or discussing practices during parent and teacher meetings. [GoGuardian's] job is to give them the tools they need to implement a safe, successful technology program and to protect their data, while the school's role is make choices on how, when, and where they wish to use it."[106]

State policymakers can require schools to post surveillance policies on their webpages or to send them to parents in an easy-to-understand format annually. Some districts have an annual training for parents to learn about their child's one-to-one device, students' responsibilities, and what surveillance will occur. Similar to best practice on student data privacy, policymakers can require that surveillance disclosures list data that will be collected, how they will be used, and how they will be protected.

Openness

"The question of whether to use surveillance practices, and of the conditions that will govern such surveillance, should be open to continuous public debate and scrutiny, and students should have a say in this discussion," according to Warnick.[107] Situations change: A major bullying problem that justified intense one-to-one device monitoring in 2013 may have since been addressed through a new digital citizenship program that reduced bullying. Community attitudes change: After an act of violence, the public may want increased security, including increased surveillance, to prevent copycats from committing similar acts.

US schools serve a great variety of people with different perspectives, values, and concerns. Inevitably, an approach to surveillance, privacy, and transparency that works in one community will not work in another. Whether auditing an existing policy for a surveillance tool or creating one from scratch, the policymaker will therefore first need to weigh local attitudes and needs. Armed with that information, schools can tailor uniform requirements that best fit community needs.

Once there is transparency about surveillance and the policies that regulate it, community members can openly discuss what surveillance practices should be used and how to regulate that surveillance. State policymakers, especially state boards of education, can highlight these topics for the general public and call for community input. They can ensure that policies are reviewed on an ongoing basis. They can specifically request that students be part of decision making. When there were questions about student data privacy practices in West Virginia, state board members and state education agency staff held meetings around the state to answer the general public's questions and hear from all stakeholders. Other states could follow this example.

States also can require better data collection on school security measures: how often officials search or direct searches of individual students, and how often they conduct random searches of groups of students. Reporting these data may encourage school officials to rely on "concrete data to make security decisions and perhaps more carefully consider whether they should implement alternative measures to create safer environments," suggests Jason P. Nance.[108]

Empowerment

The surveillance effect can undermine the perception of safety that administrators try to foster in their students by instead making them feel powerless and continually judged. "Surveillance technology should work to benefit everybody and not only school authorities," Warnick suggests, adding, "Students, teachers, parents, and staff need to be able to access the information garnered from surveillance practices to defend their rights and to advance their own legitimate ends."[109]

Surveillance policies that serve only to punish or judge students are likely to undermine trust. For example, video surveillance should be available not only to support punishment of a student for violating school policy but also for that student to review and to challenge. Surveillance should not be exempt from student or parent viewing because a school labels it as a "law enforcement record" instead of a "student record."

> "Video surveillance should be available not only to support punishment of a student for violating school policy but also for that student to review and to challenge."

When feasible, allowing students and parents to give or refuse permission to have their information collected as part of a surveillance technology—when, for example, there are iris scanners for buses—can enhance empowerment.

State policymakers can ensure that policies include equitable principles on which records are available to students, how they can access them, due process protections for when surveillance technologies are used to punish, and allowing opt-ins or opt-outs where feasible.

Equity

Fixing the broader inequities in school discipline can address many surveillance concerns. As one step in this direction, state board members may want to consider instituting restorative justice techniques and other nonpunitive alternatives to zero-tolerance policies.[110] In the context of schools, restorative justice is an approach to reducing suspensions, expulsions, and disciplinary referrals with two primary elements: "(i) a nonadversarial and dialogue-based decision making process that allows affected parties . . . to discuss the harm done to victims, while considering needs of all participants; and (ii) an agreement for going forward based on the input of all stakeholders about what is necessary to repair the harm directly to the persons and community."[111]

Highlands Middle School, in Jacksonville, Florida, is one school that has piloted such an approach. The school relies on support circles and student accountability boards to respond to student misbehavior. One Highlands Middle School student said Highlands' accountability board gives students who get in trouble alternatives to suspension, such as in-school suspension, support circle attendance, or cafeteria clean-up duty. Once the board assigns a punishment, it usually does not see the same student again.[112]

While the effectiveness of restorative justice has yet to be borne out through large empirical studies, it has attracted state and federal interest. At least two states, Florida and Colorado, have included restorative justice as an alternative to zero-tolerance policies in state legislation. At least 14 more states have some sort of restorative justice practice in school settings.[113] Congressional Representative Cohen (D-TN) and Senator Harkin (D-IA) each introduced legislation in 2013 sanctioning the use of restorative justice.[114] State boards may wish to create task forces to explore restorative justice and other practices to reduce inequities in their state.

Training

In order to implement these principles, everyone who will be dealing with surveillance or other student data should be trained. State board members and other policymakers can create all manner of policies around surveillance, but they can never be implemented with fidelity unless staff members, administrators, and teachers receive training in data, equity, and privacy. Training to minimize implicit bias can be folded into teacher and leader

preparation programs and professional development. Appropriate data literacy training covering how to collect, interpret, use, and protect data can be included in educator prep programs and professional development and can also help avoid disciplinary inequities.[115]

Teaching administrators about good data governance helps get at data minimization, transparency, and larger questions about what data schools should collect and why. "As states and districts increasingly ask educators to use data as a tool to inform their professional judgement, these states and schools also have a responsibility to ensure that their educators have the skills and supports they need to meet this profound responsibility," said Rachel Anderson, associate director for federal policy and advocacy at the Data Quality Campaign.[116]

State boards can require or recommend that administrators and teachers be trained in data literacy, privacy, and implicit bias by state colleges of teacher education or as part of their certification processes or professional development. For example, North Dakota passed a law in 2015 requiring the statewide longitudinal data system (SLDS) committee to provide annual data protection training to any staff with access to SLDS data.[117] Many organizations—including the US Department of Justice and many police departments—now require all employees to receive implicit bias training.[118] State policymakers could require that educators and administrators undergo this training, too.

Training is just as critical for the students who will be placed in the surveillance environment. State boards can use their authority over graduation requirements to encourage students to attend classes aimed at making them better digital citizens. Their education should include digital literacy, not only to ensure they are safe online but also so they understand the real-world consequences of digital posting. Students' online posting "creates a lasting digital footprint, even after it is deleted—a point students often have trouble fully comprehending," said GoGuardian's Borthwick. "When a student spends time on noneducational, 'inappropriate' material online, or makes 'anonymous' comments online in a way that can be hurtful, it offers teachers a unique opportunity to help students learn digital responsibility."[119]

CONCLUSION

At its core, surveillance technology has the potential to channel both positive and negative outcomes. Parents, students, state board members, and other stakeholders are not wrong to view new, potentially invasive technologies with a skeptical eye because there is the potential for abuse. A laissez-faire attitude toward surveillance can hamper student creativity and freedom of expression and undermine equity through furthering preexisting discipline disparities and the digital divide. The creation of more data about students through surveillance could also aid in creating the feared "permanent record" that could follow students long after school has ended.

At the same time, the technologies that monitor children might also hold the key to unlocking their individual promise and protecting them from dangers on- and offline. Consider the benefits: instructors spend less time staring over student shoulders or monitoring school hallways and more time in the classroom; students are kept safe from bullies, inappropriate content, and activities like sexting that could ruin their futures; and there is a more efficient learning environment that locates students and reports whether they are safe in the case of disaster.

Eliminating surveillance entirely is unlikely to be the answer. Instead, policymakers should create guardrails that realize the positive effects of surveillance while protecting privacy and equity in a deliberate, responsible, and measured way. Such guardrails should reflect the principles of minimization, proportionality, transparency, openness, empowerment, and equity. Training will be an indispensable component of such policies.

State boards of education have the authority—and the responsibility—to ensure surveillance is implemented responsibly so that the privacy and equitable treatment of all students are ensured. In their unique position as developers of policy, standards, and rules and regulations, state boards can introduce and manage surveillance tools intentionally. But they can also be advocates and trusted counselors in explaining the value of surveillance to parents and reassuring them that the benefits of surveillance will not come at the expense of students' well-being. Through rule making, privacy policies, convening, and questioning, state boards can ensure that policies on student surveillance incorporate privacy protections and that the fruits of surveillance technologies do not do the most harm to the students who need the most help.

NOTES

1. US Department of Education, National Center for Education Statistics, "Public School Safety and Discipline: 2013–14," NCES 2015–051 (Washington, DC, 2015); NCES, "Fast Facts: School Safety and Security Measures," **https://nces.ed.gov/fastfacts/display.asp?id=334**.

2. See, for example, Cheryl Staats, "Implicit Racial Bias and School Discipline Disparities: Exploring the Connection," Kirwan Institute Special Report (May 2014), **http://kirwaninstitute.osu.edu/wp-content/uploads/2014/05/ki-ib-argument-piece03.pdf**.

3. For the purposes of this report, we limited our discussion to technology that enables surveillance, since the storage capacity and nonstop surveillance capabilities of this technology are especially likely to create privacy and equity dangers for students. We have also limited our scope to school or district surveillance of students, as opposed to third-party school services that may have access or tracking features.

4. The first five come from Bryan Warnick, *Understanding Student Rights in Schools* (New York: Teachers College Press, 2013). We add equity.

5. PBS, "PBS Survey Finds Teachers Are Embracing Digital Resources to Propel Student Learning," press release (February 4, 2013).

6. Marketplace and Lieberman Research Worldwide, "Parents Attitudes toward Education Technology," APM Marketplace Report (May 2015), **http://cms.marketplace.org/sites/default/files/Education%20Technology%20-%20APM%20Marketplace%20Report.pdf**.

7. Jim Kerstetter, "Tech Makes Its Pitch to the Education Community," *New York Times* (June 29, 2016).

8. Calvin Hennick, "I Spy: What's Happenig on All Those Student Devices," Scholastic.com (Summer 2014).

9. Ibid.

10. Steve Zurier, "5 Devices for K–12 One-to-One Initiatives," EdTechMagazine.com (June 26, 2015).

11. K. Shapley, et al., "Evaluation of the Texas Technology Immersion Pilot: Final Outcomes for a Four-Year Study (2004–05 to 2007–08)" (Austin, TX: Texas Center for Educational Research, 2009). The scores of students in the study improved so much that "after three years, low-income students in the laptop schools displayed the same levels of technology proficiency as wealthier students in the control schools." Bryan Goodwin, "One to One Laptop Programs Are No Silver Bullet," *Educational Leadership* 68, no. 5 (February 2011), paraphrasing Shapley et al.

12. Using tools like NetSupport, AirWatch, Stoneware, and others, schools are able to manage individual, personal devices students bring to class. Hennick, "I Spy."

13. Schools seeking to monitor devices their students bring from home have several options. One way to track student device activities is through controlled network access. Derry Township School District in Hershey, Pennsylvania, uses a third-party tool to manage its network authentication by proving two network options: a "throttled-down" and "heavily filtered" guest network and the main school network. If students elect to join the much faster main network, they must enter a username and password and receive a device certificate from the server, which authorizes their access for an established period (five years in this case) and allows the network to associate the device with that particular student for the duration of the certificate. Student with access to the main network are then subject to the networks filtering settings. Such vendors as Extreme Network and Ruckus Wireless also include features that let schools see who is connected to the network and what type of device they are using. Dennis Pierce, "6 IT Solutions to BYOD Challenges," TheJournal.com (October 22, 2015), **https://thejournal.com/articles/2015/10/22/6-it-solutions-to-byod-challenges.aspx**.

14. See, for example, Matthew J. Cuellar, "School Safety Strategies and Their Effects on the Occurrence of School-Based Violence in US High Schools: An Exploratory Study," *Journal of School Violence* (2016) **doi: 10.1080/15388220.2016.1193742**, who here is paraphrasing Kristin D. Eisenbraun, "Violence in Schools: Prevalence, Prediction, and Prevention," *Aggression and Violent Behavior* 12, no. 4 (2007): 459–69.

15. Sameer Hinduja and Justin W. Patchin, "2015 Cyberbullying Data," Cyberbullying Research Center (May 1, 2015), **http://cyberbullying.org/2015-data**; Emily Layden, "On Facebook, Bullies 'Like' if You Hate," *New York Times* (September 9, 2012); Jan Hoffman, "As Bullies Go Digital, Parents Play Catch-Up," *New York Times* (December 4, 2010); Lizette Alvarez, "Girl's Suicide Points to Rise in Apps Used by Cyberbullies," *New York Times* (September 14, 2013); Somini Sengupta, "Teenagers Tell Researchers It's a Cruel, Cruel Online World," *New York Times* (November 9, 2011); Philip T.K. Daniel and Scott Greytak, "A Need to Sharpen the First Amendment Contours of Off-Campus Student Speech," *Education Law Reporter* 273: 21, 42 (WL 6960849 December 22, 2011); Amanda Lenhart et al., "Teens, Kindness and Cruelty on Social Network Sites," Pew Research Center (November 9, 2011), **http://www.pewinternet.org/2011/11/09/teens-kindness-and-cruelty-on-social-network-sites**.

16. Sameer Hinduja and Justin Patchin, "State Cyberbullying Laws," Cyberbullying Research Center (January 2016), **http://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf**.

17. National Forum on Education Statistics, "Forum Guide to Crime, Violence, and Discipline Incident Data," NFES 2011–806 (Washington, DC: US Government Printing Office, 2011).

18. Emma Morris, "Sexting: Felony or Flirting?" Family Online Safety Institute (Washington, DC: FOSI, October 14, 2014), **https://www.fosi.org/policyresearch/sextingfelonyorflirting/**.

19. Heidi Strohmaier et al., "Youth Sexting: Prevalence Rates, Driving Motivations, and the Deterrent Effect of Legal Consequences," *Sexuality Research and Social Policy* 11 (2014): 245.

20. Morris, "Sexting: Felony or Flirting?"

21. Sameer Hinduja and Justin Patchin, "State Sexting Laws," (Cyberbullying Research Center, 2015), **http://cyberbullying.org/state-sexting-laws.pdf**. See also Julia Halloran McLaughlin, "Crime and Punishment: Teen Sexting in Context," *Penn State Law Review* 115: 135 (2010), which provides numerous examples of sexting incidents and prosecutions.

22. However, a 2013 survey of state prosecutors who filed charges in juvenile sexting cases found that only 16 percent of the cases resulted in the defendant being registered as a sex offender, and only 4 percent led to a criminal trial. NASBE was unable to find a similar survey of district prosecutors. Wendy Walsh, Janis Wolak, and David Finkelhor, "Sexting: When Are State Prosecutors Deciding to Prosecute? The Third National Juvenile Online Victimization Study," (Crimes against Children Research Center, January 2013), **http://www.unh.edu/ccrc/pdf/CV294_Walsh_Sexting%20%26%20prosecution_2-6-13.pdf**.

23. Eun Kyung Kim, "Safety or Snooping? Schools Start Monitoring Social Media Accounts of Students," (Today Parents, September 3, 2015), **http://www.today.com/parents/schools-use-program-monitor-kids-**

social-media-accounts-t42221.

24. Office of Partner Engagement, Federal Bureau of Investigation, "Preventing Violent Extremism in Schools," (January 2016), **https://info.publicintelligence.net/FBI-PreventingExtremismSchools.pdf**.

25. Benjamin Herold, "Schools Weigh Access to Students' Social-Media Passwords," *Education Week* (February 17, 2015); Somini Sengupta, "Warily, Schools Watch Students on the Internet," *New York Times* (October 28, 2013); Jeff Matsuura and Craig Blakeley, "School Surveillance of Student Social Media Raises Privacy Concerns," *Law and Technology Blog*, ThomsonReuters.com (May 2, 2016).

26. Geo Listening, "Privacy Policy," **https://geolistening.com/privacy-policy/** (accessed August 31, 2016).

27. Karen Turner, "Schools Are Helping Police Spy on Kids' Social Media Activity," *Washington Post* (April 22, 2016).

28. Emily E. Tanner-Smith and Benjamin W. Fisher, "Visible School Security Measures and Student Academic Performance, Attendance, and Postsecondary Aspirations," *Journal of Youth Adolescence* 45 (2016): 195, 210.

29. For an interesting discussion of the purposes and pros and cons of surveillance, see Tim Walker, "Cameras in the Classroom: Is Big Brother Evaluating You?" NEA Today (January 23, 2015), **http://neatoday.org/2015/01/23/cameras-in-the-classroom-big-brother-evaluating**.

30. US Department of Education, National Center for Education Statistics "Public School Safety and Discipline: 2013–14," NCES 2015–051 (Washington, DC, 2015); NCES, "Fast Facts: School Safety and Security Measures," **https://nces.ed.gov/fastfacts/display.asp?id=334**.

31. Education Week, "School Safety Legislation since Newtown," (April 24, 2013), **http://www.edweek.org/ew/section/multimedia/school-safety-bills-since-newtown.html**.

32. Jason P. Nance, "Student Surveillance, Racial Inequalities, and Implicit Racial Bias," *Emory Law Journal* 66, forthcoming, **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830885**.

33. Genetec, "Raytown Quality Schools Unifies Video Surveillance and Access Control System," (accessed August 31, 2016), **http://www.genetec.com/solutions/resources/raytown-quality-schools-upgrades-video-and-access-control-systems**.

34. The requirement is triggered when a parent, trustee, school board member, or staff member on the campus requests that audiovisual monitoring equipment be installed. Texas Senate Bill 507 § 29.022(a).

35. Ryan Schuette, "Coming to Texas: Special-Ed Cams to Protect Students from Their Own Teachers," NPR.org (December 15, 2015).

36. Peter Pochowski, interview by Neil Conan, "Security Cameras in School: Protective or Invasive?" Talk of the Nation (Sept. 4, 2012).

37. Matthew Feeney, "Why We Don't Need Body Cameras in Schools," CATO Institute (July 20, 2015), **http://www.cato.org/publications/commentary/why-we-dont-need-body-cameras-schools.** Also see Conor Friedersdorf, "Keep Body Cams off Public-School Educators," TheAtlantic.com (July 10, 2015).

38. Feeney, "Why We Don't Need Body Cameras in Schools."

39. Thomas McMahon, "School Bus Contractors Equipment Survey 2015," *School Bus Fleet* (September 2015): 5.

40. David Anderson, "Harford Says School Buses with Onboard Surveillance Cameras Have Reduced Disciplinary Problems," *Baltimore Sun* (October 27, 2015).

41. Kathy Welsh, "School Bus Monitor Arrested for Slapping Student," HVNN.com (January 5, 2015).

42. James Vaznis, "Boston Adds Security Cameras to School Buses," *Boston Globe* (July 21, 2014).

43. Kate Schimel, "Meet the Modern Bus," EducationDive.com (August 24, 2015).

44. Tim Omarzu, RFID Chips to be Used on Chattooga County Buses to Track Students, TimesFreePress.com (July 14, 2014).

45. Danielle Keats Citron and David Gray, "Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards," *Harvard Law Review* 126, F. 262 (May 2013).

46. Andy Greenberg, "Snowden Designs a Device to Warn if Your iPhones Radios Are Snitching," Wired.com (July 21, 2016).

47. Nance, "Student Surveillance," 25.

48. danah boyd, "Making Sense of Privacy and Publicity," SXSW (Austin, Texas, March 13, 2010), **http://www.danah.org/papers/talks/2010/SXSW2010.html**.

49. Kirstie Ball et al., "The Problem of Surveillance and Gender," *Routledge Handbook of Surveillance Studies* (London: Routledge, 2012): 51.

50. Several are referenced in Jason G. Goldman, "How Being Watched Changes You—Without You Knowing," BBC (February 10, 2014); see also Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," *Scientific American* (May 3, 2011).

51. Arthur L. Beaman et al., "Self-Awareness and Transgression in Children: Two Field Studies," *Journal of Personality and Social Psychology* 37, no. 10 (October 1979): 1835–46.

52. Max Ernest-Jones et al., "Effects of Eye Images on Everyday Cooperative Behavior: A Field Experiment," *Evolution and Human Behavior* 32 (2011): 172–78.

53. Neil Schoenherr, "Intellectual Privacy Vital to Life in the Digital Age," TheSource.com (February 2, 2015).

54. A. E. Hotchner, "Hemingway, Hounded by the Feds," *New York Times* (July 22, 2011).

55. See T.A. Ridout, "Surveillance and the Creative Mind," The Huffington Post (October 26, 2014) for an essay elaborating this point.

56. Warnick, *Understanding Student Rights in Schools*, 128–64.

57. Ball et al., "The Problem of Surveillance and Gender."

58. Melinda D. Anderson, "When School Feels Like Prison," The Atlantic (September 12, 2016).

59. Ward's testimony at a hearing on Ending the School-to-Prison Pipeline before Senate Subcommittee on the Constitution, Civil Rights, and Human Rights, 112th Cong. 1 (2012), cited in Nance, "Student Surveillance."

60. Feeney, "Why We Don't Need Body Cameras in Schools."

61. Vikki S. Katz and Michael H. Levine, *Connecting to Learn: Promoting Digital Equity among America's Hispanic Families* (New York: Joan Ganz Cooney Center at Sesame Workshop, 2015).

62. Interview with ACLU's Chad Marlow by Amelia Vance on January 29, 2016.

63. Katz and Levine, *Connecting to Learn*.

64. Ibid.

65. US Department of Education, "Data Snapshot: School Discipline," Issue Brief 1, School Rights Data Collection (March 2014).

66. US Department of Education, Office for Civil Rights (OCR), "2013–2014 Civil Rights Data Collection: A First Look," (June 7, 2016), **http://www2.ed.gov/about/offices/list/ocr/**

docs/2013-14-first-look.pdf.

67. ED, "Data Snapshot: School Discipline."

68. OCR, "2013–2014 Civil Rights Data Collection."

69. Dan Losen et al., "Eliminating Excessive and Unfair Exclusionary Discipline in Schools: Policy Recommendations for Reducing Disparities" (Bloomington, IN: The Discipline Disparities Research to Practice Collaborative, March 2014), **http://www.indiana.edu/~atlantic/wp-content/uploads/2014/04/Disparity_Policy_031214.pdf**.

70. Arne Duncan, "Rethinking School Discipline," remarks of US Secretary of Education Arne Duncan at the Release of the Joint DOJ-ED School Discipline Guidance Package (January 8, 2014), **http://www.ed.gov/news/speeches/rethinking-school-discipline**.

71. OCR, "2013–2014 Civil Rights Data Collection."

72. Jeremy D. Finn and Timothy J. Servoss, "Security Measures and Discipline in American High Schools," in Daniel J. Losen, ed., *Closing the School Discipline Gap* (Los Angeles: Civil Rights Project, 2015).

73. Staats, "Implicit Racial Bias," 1–2.

74. Tony Fabelo et al., "Breaking Schools' Rules: A Statewide Study of How School Discipline Relates to Students' Success and Juvenile Justice Involvement," (New York: Council of State Goverments Justice Center and The Public Policy Research Institute, Texas A&M University, 2011), 46, **https://csgjusticecenter.org/wp-content/uploads/2012/08/Breaking_Schools_Rules_Report_Final.pdf**.

75. Nance, "Student Surveillance," 61–62.

76. Linda van den Bergh et al., "The Implicit Prejudiced Attitudes of Teachers: Relations to Teacher Expectations and the Ethnic Achievement Gap," *American Education Research Journal* 47 (2010); Jason A. Okonofua and Jennifer L. Eberhardt, "Two Strikes: Race and the Disciplining of Young Students," *Psychological Sciences* 26, no. 1 (2015).

77. Steve Smith, interview by J. William Tucker, August 10, 2016.

78. Teddy Hartman, interview by J. William Tucker, August 10, 2016.

79. Losen et al., "Eliminating Excessive and Unfair Exclusionary Discipline."

80. Robert Balfanz et al., "Sent Home and Put Off-Track: The Antecedents, Disproportionalities, and Consequences of Being Suspended in the Ninth Grade," paper presented at the Closing the School Discipline Gap: Research to Practice conference, Washington, DC (Los Angeles: Civil Rights Project, 2013).

81. Henry M. Levin and Cecilia E. Rouse, "The True Cost of High School Dropouts," op-ed, *New York Times* (January 26, 2012). According to the authors, reducing high school dropout rates by 700,000 students would produce an economic benefit of $90 billion per year.

82. See, for example, David Osher et al., "Avoid Simple Solutions and Quick Fixes: Lessons Learned from a Comprehensive Districtwide Approach to Improving Conditions for Learning," (January 2, 2013), **https://civilrightsproject.ucla.edu/resources/projects/center-for-civil-rights-remedies/school-to-prison-folder/state-reports/avoid-simple-solutions-and-quick-fixes-lessons-learned-from-a-comprehensive-districtwide-approach-to-improving-conditions-for-learning/osher-avoid-simple-solutions-ccrr-conf-2013.pdf**.

83. For a definition of zero-tolerance policies, see Russell J. Skiba and Gil G. Noam, "Zero Tolerance: Can Suspensions and Expulsions Keep Schools Safe?" *New Directions for Youth Development: Theory, Practice, Research* 92 (Winter 2001): 20; see also Motoko Rich, "Administration Urges Restraint in Using Arrest or Expulsion to Discipline Students," *New York Times* (January 8, 2014).

84. Aaron Kupchik, "The School-to-Prison Pipeline," in Franklin E. Zimring and David S. Tenenhaus, eds., *Choosing the Future for American Juvenile Justice* (New York: NYU Press, 2014).

85. Nathan James and Gail McCallion, "School Resource Officers: Law Enforcement Officers in Schools," Congressional Research Service (June 26, 2013), **https://www.fas.org/sgp/crs/misc/R43126.pdf**; Greg Botelho and Ralph Ellis, "Police in Schools: Why Are They There?" CNN (October 30, 2015).

86. See Evie Blad, "Body Cameras on School Police Spark Student Privacy Concerns," *Education Week* (March 3, 2015).

87. Genetec, "Raytown Quality Schools."

88. Nance, "Student Surveillance," 39.

89. For example, see Elana Zeide, "The Proverbial Permanent Record," New York University Information Law Institute (October 9, 2014), **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2507326**.

90. Valerie Strauss, "The Astonishing Amount of Data Being Collected about Your Children," WashingtonPost.com (November 12, 2015).

91. Kade Crockford and Jessie J. Rossman, "Back to the Drawing Board: Student Privacy in Massachusetts K-12 Schools," (Boston: ACLU Foundation of Massachusetts, 2015).

92. Kevin P. Brady and Cynthia A. Dieterich, "Video Surveillance of Special Education Classrooms: Necessary Protections of Vulnerable Students or Intrusive Surveillance of Select Student Populations?" *Education Law Report* 325 (Feb. 25, 2016). Quoting, successively, "Constitutionality of Secret Video Surveillance," 91 A.L.R. 5th 585, § 2 (2001), and *Brannum v. Overton County School Bd.* 516 F.3d 489, *Education Law Report* 229: 402 (6th Cir. 2008).

93. David Von Drehle, "The Surveillance Society," Time.com (August 1, 2013).

94. Lapp, "Databasing Delinquency."

95. Texas Senate Bill 507 § 29.022(a).

96. Warnick, *Understanding Student Rights*.

97. Ibid., 162.

98. The Student Data Principles, **http://studentdataprinciples.org**.

99. Brady and Dieterich, "Video Surveillance," n. 27.

100. Lapp, "Databasing Delinquency."

101. New Jersey Administrative Code § 6A: 32-7.1 (i).

102. Warnick, *Understanding Student Rights*, 162.

103. Ibid., 163.

104. James L. Rosica, "Biometrics May Be Banned in Florida Schools but Flourish Elsewhere," TBO.com (March 9, 2014), **http://www.tbo.com/news/politics/biometrics-may-be-banned-in-florida-schools-but-flourish-elsewhere-20140309**.

105. Crockford and Rossman, "Back to the Drawing Board."

106. Claire Borthwick, interview by J. William Tucker, August 19, 2016.

107. Warnick, *Understanding Student Rights*, 163.

108. Nance, "Student Surveillance."

109. Warnick, *Understanding Student Rights*.

110. For example, another alternative approach is MyTeachingPartner, a program developed by the University of Virginia that provides resources and individual coaching for teachers

to aid and support their interactions with students. The program has been found to reduce racial disparities in student discipline. Anne Gregory et al., "How Educators Can Eradicate Disparities in School Discipline," in Russell Skiba et al., eds., *Inequality in School Discipline* (New York: Palgrave Macmillan, 2016). Other evidence-based alternatives are documented in Christopher Boccanfuso and Megan Kuhfeld, "Multiple Responses, Promising Results: Evidenced-Based, Nonpunitive Alternatives to Zero-Tolerance," (Washington, DC: Child Trends, 2011).

111. Mara Schiff, "Dignity, Disparity and Desistance: Effective Restorative Justice Strategies to Plug the School-to-Prison Pipeline," (Los Angeles: The Civil Rights Project, UCLA, 2013), citing G. Bazemore and M. Schiff, " 'No Time to Talk': A Cautiously Optimistic Tale of Restorative Justice and Related Approaches to School Discipline," in Richard Rosenfeld et al. eds., *Contemporary Issues in Criminological Theory and Research: The Role of Social Institutions* (Belmont, CA: Wadsworth and Cengage Learning, 2010).

112. Tessa Duvall, "School Restorative Justice Program Allows Peers to Support, Hold One Another Accountable," *Florida Times-Union* (November 24, 2015).

113. California, Colorado, Florida, Georgia, Illinois, Maine, Maryland, Michigan, Minnesota, Missouri, New York, Texas, Pennsylvania, and Connecticut. Schiff, "Dignity, Disparity and Desistance," 7.

114. Restorative Justice in Schools Act of 2011, H.B. 415, 112th Congress, Congressional Record H4059; Successful, Safe, and Healthy Students Act of 2011, S. 919, 112th Congress, Congressional Record S2794–2797.

115. State policymakers seeking to improve teacher data literacy should seek this resource: Data Quality Campaign, "Teacher Data Literacy: It's About Time: A Brief for State Policymakers," (February 2014), **http://dataqualitycampaign.org/resource/teacher-data-literacy-time/**.

116. Rachel Anderson, interview by Amelia Vance, August 31, 2016.

117. North Dakota, Senate Bill No. 2326 (2015), **http://www.legis.nd.gov/assembly/64-2015/documents/15-0956-05000.pdf**.

118. Nance, "Student Surveillance," 75–76.

119. Borthwick interview.

NASBE | National Association of State Boards of Education

333 John Carlyle Street, Suite 530
Alexandria, VA 22314

The National Association of State Boards of Education represents America's state and territorial boards of education. Our principal objectives are to strengthen state leadership in education policymaking, advocate equality of access to educational opportunity, promote excellence in the education of all students, and ensure responsible lay governance of education.
Learn more at www.nasbe.org.