ACLU RESEARCH REPORT

Digital Dystopia

The Danger in Buying What the EdTech Surveillance Industry is Selling

ACLU

ACLU RESEARCH REPORT

Digital Dystopia

The Danger in Buying What the EdTech Surveillance Industry is Selling

Cover Photo © Shutterstock/MemoryMan

Contents

Acknowledgements 3

Executive Summary 4

Introduction 8

The EdTech Surveillance Industry’s Deceptive Marketing Practices 11

Surveillance Technology in Schools Is Hurting Kids, Not Helping Them 20

Efforts to Push Back Against Student Surveillance 31

Recommendations and Conclusions: How To Protect Students and Promote Better Student Surveillance Technology Decision-Making 39

Methods 43

Appendix 1: Ed Tech Surveillance: 10 Leading Products 46

Appendix 2. Model Legislation: Student Surveillance Technology Acquisition Standards Act 52

Endnotes 55

Acknowledgements

This report is a product of the American Civil Liberties Union (ACLU). Its principal author is Chad Marlow, senior policy counsel with the National Political Advocacy Department (NPAD). Significant portions of this report related to the ACLU's original research were authored by Emily Greytak, director of research, and former graduate research interns Katie Duarte and Sunny Sun. Major editing contributions and other critical guidance were provided by Allegra Harpootlian, communications strategist with the Communications and Marketing Department, and Jay Stanley, senior policy analyst with the Speech, Privacy, and Technology Project.

This report could not have been written without the many contributions of the journalists, academics, and advocates who have written and reported extensively on the use of surveillance in our schools and the impacts it has (and has not) had on our schools. Their works combined to create the palette from which we painted this report's picture, and we are extremely grateful to all of them.

This report also could not have been written without the skillful editing and thoughtful commentary of our many expert colleagues throughout the ACLU's nationwide organization. Thank you Kimberly Buddin (ACLU national), Sophie Cohen (NYCLU), Stefanie Coyle (NYCLU), Kade Crockford (ACLU-MA), Lea Despotis (ACLU national), Michael Hall (ACLU national), Beth Haroules (NYCLU), Sarah Hinger (ACLU national), Joe Johnson (ACLU-NJ), Harold Jordan (ACLU national and ACLU-PA), Ana Graciela Najera Mendoza (ACLU-SoCal), Michelle Morton (ACLU-FL), Dillon Reisman (ACLU-NJ), West Resendes (ACLU national), Daniel Schwartz (NYCLU), Hannah Stern (ACLU-RI) and Cody Venzke (ACLU national).

We are very grateful to former ACLU research interns and fellows who contributed directly to data collection, analysis, and research review. Specifically, to Roshni Saleem Chagan, Katie Duarte, Carly Evich, Eliot Lev, Cyrus O'Brien, Sarah Sakha, Sunny Sun, Kana Tateishi, Morre Taylor, Marcos Viveiros Cespedes, and Cynda Whitehouse We would also like to thank Eva Lopez, ACLU creative campaign strategist, Ana Graciela Najera Mendoza (ACLU-SoCal), and Alan Flores, co-chair of the Youth Advisory Board for ACLU's Youth Activism Research Collaborative, for additional moderation of focus groups. Along with our affiliate colleagues named above, we are also grateful to those affiliates who supported our focus group outreach: Molly Kennedy (ACLU-WV), Jake Martinez (NYCLU), Kenny Nguyen (NYCLU), and Keturah Herron (ACLU-KY). We especially want to thank the students who shared their experiences and feelings with us in our focus groups, it was an honor to learn from them and hear their stories. Not only are their contributions are not only reflected in this report, but they continue to inform ACLU's efforts to ensure schools are safe and equitable for all students.

We also appreciate the crucial support of the current and former program staff of the ACLU National Advocacy Institute: Andrew Domingue, Luke Sampson-Doyle, and Raquel Fossett (formerly ACLU). We also are grateful to Chris Re, associate director, public opinion Research, for his expert guidance and coordination of polling for this project. This report was copyedited by Tim Merrill and designed by Patrick Moroney, and we greatly appreciate their expertise.

Executive Summary

Over the last two decades, a segment of the educational technology (EdTech) sector that markets student surveillance products to schools – the EdTech Surveillance industry – has grown into a $3.1 billion a year economic juggernaut with a projected 8% annual growth rate.[1] *The EdTech Surveillance industry accomplished that feat by playing on school districts' fears of school shootings, student self-harm and suicides, and bullying – marketing them as common, ever-present threats.*

Capitalizing on its significant financial resources and political influence, the EdTech Surveillance industry has succeeded in shaping and controlling the narrative around its products. These companies flooded school officials with their own biased marketing materials, promoting their surveillance products as highly effective safety interventions that keep students safe, even though such claims lack independent, unbiased, substantiating evidence. The well-funded EdTech Surveillance industry has likewise benefited from its ability to drown out any discussion of the widespread harms their products cause students.

As a result, from student communications monitoring to facial recognition technology, school districts are rapidly deploying a huge array of surveillance technologies to spy on their students in the name of "safety." While buying these EdTech Surveillance products may make school districts *feel* safer, the reality is they do not keep students safe. In fact, student surveillance is not only ineffective as a safety measure, but it often harms students in the process and precludes schools from implementing more proven interventions.

Education officials and school administrators play a vital role in determining how best to keep students safe. But as long as school districts continue to make decisions based on information provided by the very same companies that are seeking to sell schools their EdTech Surveillance products, the EdTech Surveillance industry, and not their students, will be the biggest beneficiary.

"Digital Dystopia" is meant to equip school decision-makers, influencers, and community members with the full and reliable information they need to make the best decisions possible when it comes to student surveillance technologies and keeping students safe.

Methods

ACLU used the following methods to understand and uncover the current state of EdTech Surveillance in the United States: review of the existing empirical research, investigation into surveillance technology practices and products, an audit of school shooting incidents, a series of focus groups with over three dozen students from different regions and backgrounds as well as a nationally representative YouGov survey of 502 students aged 14-18.

Key Findings

While school violence and student mental health are critical issues that cause understandable concern amongst school community members, the EdTech Surveillance industry deliberately whips up fear around tragic, albeit uncommon events such as school shootings and suicides in order to drive demand for their products.

- EdTech Surveillance companies have focused on stoking fear around student self-harm, suicides, and bullying.
- Capitalizing on school safety concerns, lobbyists have secured over $300 million in federal funds, allegedly to improve school safety.[2] The EdTech Surveillance industry relies on these large pools of government funds to make their immediate monetary costs to schools either low or nonexistent.

The EdTech Surveillance industry aggressively promotes its products as a highly effective intervention to keep students safe; however, there is no independent, unbiased, data driven evidence that they do so. The methods the industry uses to make its efficacy claims are designed to mislead school districts into concluding their effectiveness as a student safety measure has been proven.

EdTech Surveillance companies provide specific data-driven assertions that are impossible to verify, such as Bark claiming its student surveillance software has "'prevented' 16 school shootings.[3]

- EdTech Surveillance companies make unsubstantiated overly broad and nonspecific claims. Gaggle, for example, asserts that its products are effective in "preventing suicides," "preventing school violence," "limiting bullying and harassment," "stopping child abuse and harassment," "stopping sexual abuse," and "stopping childhood predators.[4] NetTalon asserts that its surveillance cameras, coupled with the other school safety interventions it markets, will "dramatically improve school safety against active shooters or other terrorist attacks."[5] In-depth reviews of research literature, including those commissioned by the U.S Department of Justice,[6] and ACLU's review of the empirical evidence, consistently find a clear lack of evidence that surveillance technology makes schools safer.
- Surveillance cameras were in place during 8 out of 10 of the deadliest school shootings in the past two decades yet did not prevent those incidents.
- Social media monitoring had little role in thwarting planned school shootings, according to a U.S. Secret Service investigation,[7] as the vast majority were averted due to concerns raised by other students directly to school or local authorities.

While the effectiveness of student surveillance technologies is unproven, the harm they cause to students is not in doubt. While many student surveillance harms impact all students equally, there are a considerable number of specific harms that fall more heavily, if not exclusively, on already vulnerable students and groups of students.

- Student surveillance technologies harm all students by: (1) teaching students the wrong lessons about issues like authenticity, risk-taking, and the right to live free from surveillance; (2) undermining their privacy; (3) eroding student trust in teachers, school staff, and administrators; (4) inhibiting students' ability to engage in self-help; and (5) increasing student fear and criminalize youth
    - Approximately a third of 14-18 year old students in our national survey (32%) reported that surveillance makes them "always feel like I'm being watched."
    - Students in focus groups noted that, in reaction to surveillance, they limit discussing personal information with—or even around—educators, such as that they were in foster care, facing abuse, or struggling with mental health issues.
    - Nearly a quarter of the students we surveyed (24%) were concerned about how school surveillance limits the resources they feel they can access online.
    - Approximately 1 in 5 students surveyed reported concerns that surveillance technology could be used to identify students seeking reproductive health care, including abortion (21%) and seeking gender affirming care (18%).

    - EdTech Surveillance may provide students with a false sense of security — a portion of students surveyed reported the school surveillance made them feel "safe" (40%) and "protected" (34%). Among some students, surveillance have the opposite effect, stoking fear and promoting anxiety — a portion of students reported surveillance made them feel "anxious" (14%), "exposed," (15%), "paranoid" (13%), "violated (12%), with a smaller portion reporting that surveillance in schools made them feel "unsafe" (7%) and "scared" (5%).
    - Approximately a quarter of students surveyed were concerned about how surveillance could be used to discipline them or their friends (27%) and how it could be shared with law enforcement (22%).
    - Students in our focus groups reported that they or someone they know experienced being reprimanded or punished for personal social media posts outside of school time.
- Student surveillance technologies produce even greater harms for certain, already vulnerable groups of students. Namely: (1) students of color, particularly Black, Latine/x, and Indigenous students; (2) students with disabilities; (3) LGBTQ+ and nonbinary students; (4) undocumented students and students with undocumented family members; and (5) low-income students.

The opportunity costs of using surveillance technology include diverting monetary and human resources away from more effective school safety measures and educational technologies that support students' learning.

- EdTech Surveillance diverts financial and human resources from proven efforts that truly "work" to promote school safety and student wellbeing, such as school belonging, mental health supports, anti-bias initiatives, and even stronger building security.
- Using earmarked available for educational technology to purchase surveillance products instead of other more learning-focused technologies deprives students and schools of important benefits of truly effective and helpful educational technologies, such as those that promote accessibility or enhance remote learning.

Key Recommendations

Education surveillance technology is a multibillion-dollar industry that has seemingly unlimited resources to push biased and inaccurate marketing claims to increase their profits. However, school administrators and other school community members are not powerless. Through public education, robust, informed local decision-making processes, and state-level laws, each of us can promote smart student safety decisions and fight back against those seeking to make their fortunes selling abusive student surveillance technologies — and we must.

Educate Others and Advocate for Reform

For those who care about protecting our students' privacy and promoting better student surveillance technology decision-making, the most important action you can take is to help educate others about the suspect benefits and clear harms of student surveillance. Stressing the availability of such information will hopefully end decision-makers' and other community members' near exclusive reliance on self-serving information being provided to them by the EdTech Surveillance industry. Key points to highlight include:

- Do not let fear drive your decision-making;
- Do not rely on unsubstantiated efficacy claims offered by EdTech Surveillance companies who have a financial interest in the sale of the technologies — insist on proof of efficacy from unbiased, fully independent sources;
- Learn about the harmful impacts of surveillance technologies on students and other school community members, including their heightened adverse impact on already vulnerable groups; and
- Consider opportunity costs — what other options to keep kids safe will we be forgoing to use student surveillance technologies? In the end, if the school policymakers, influencers, and other community members you engage adopt these suggestions,

they will be much better informed and make wiser decisions when it comes to student surveillance technologies.

Adopt Best Practices For Decision-Making At Your School District Level

We advise adopting a school district policy that requires adherence to the following steps:

1. Define the precise problem your school district is seeking to solve;
2. Evaluate a student surveillance technology's actual benefits and costs/harms in light of the specific problem to be solved;
3. Seek input from your entire school community; and
4. Conduct a final benefits versus costs/harms analysis.

Ultimately, if the costs/harms of the student surveillance technology — including its opportunity costs — exceed its benefits, or where an alternative intervention has a better benefits-to-costs/harms ratio, the student surveillance intervention should be rejected.

Pass State Legislation Requiring All Schools/School Districts To Follow Best Practices For Student Surveillance Technology Decision-Making

For those who want to produce an even broader impact, rather than seeking to adopt best practices at just your school/school district, you can advocate for every school in your state to adopt these best practices. To facilitate the adoption of highly effective and consistent legislative standards, the ACLU drafted the "Student Surveillance Technology Acquisition Standards Act" model bill, which is provided in Appendix 2 of this report.

Advocate Against The Use of Student Surveillance Technologies

Consistently oppose the use of invasive and harmful student surveillance technologies in your school. At best, student surveillance technologies create the perception of improving student safety without actually moving us closer to that goal. In truth, the use of student surveillance technologies harms students and supplants measures that have a more positive, proven impact on students' safety and wellbeing.

Introduction

If you are a K-12 school administrator, school board representative, PTA member, or teacher at one of the 17,396 school districts in the United States,[8] chances are you have either been approached by a company looking to sell you a student surveillance technology product or your school is already using at least one such technology in its physical or virtual classrooms.[9]

Using sharp marketing materials, well-trained salespersons, and fanciful product efficacy claims, the Education Technology (EdTech) Surveillance industry has convinced thousands of school districts to buy their products. From communications monitoring to facial recognition technology, school districts are rapidly deploying a massive array of these surveillance technologies while paying far too little attention to whether they actually work and to the harms that accompany their use.

Two unrelated but highly impactful developments have led to schools' lightspeed adoption of student surveillance technologies. The first is the increased public attention on school shootings, suicides, and bullying. Certainly, among the many responsibilities of schools, protecting the physical and mental health of the children in their care is at or near the top of the list and, therefore, effective, properly tailored remedial measures are certainly appropriate. With respect to school shootings, in particular, the political unviability of gun control legislation in much of the country has placed even greater pressure on schools to find alternative approaches to keeping students safe.

The second development was the onset of the COVID-19 pandemic, which led to the physical shuttering of most of America's schools in March 2020. At the time, remote learning technologies were just beginning to gain a foothold in our schools. However, because of the emergency shift to remote learning, the use of remote learning technologies (quite a few of which were sold by rebranded student surveillance companies[10]) went from a limited to near total market penetration within a matter of weeks. Despite warnings,[11] the pressing need to educate America's students despite the loss of in-person instruction left little time to consider the long-term impact of adopting these remote-learning but also student-surveillance tools. Now that schools have re-opened, it is time to consider whether the urgent need to act inadvertently allowed a fox into the schoolhouse.

To convince schools to buy their surveillance tools, the EdTech Surveillance industry shifted its marketing machines into overdrive and frequently made claims about the efficacy of its products that were wholly unsubstantiated, impossible to verify, and/or flew in the face of the multitude of independent studies showing surveillance doesn't reduce incidents.[12] EdTech Surveillance companies counted on school decision-makers being unable to access reliable, independent information about their products' efficacy and having too little time to question their marketing claims.

And for those schools that might remain hesitant, the EdTech Surveillance industry's closing tactic was often enough to push even the most skeptical potential customer to relent: fear. On many levels, both subtle and explicit, their message to school districts was clear. Namely, your students are in danger and the risk to them is serious, imminent, and could manifest anytime and anywhere. Schools were told they had to take action to keep their students safe, and that the EdTech Surveillance industry had precisely the products they needed.

Despite the lack of unbiased, independent evidence that surveillance technologies produce meaningful improvements in student safety, the industry continues to make such claims. Not surprisingly, the EdTech Surveillance industry's marketing also fails to acknowledge the harm its products do. And by leveraging its power and substantial marketing budget, the EdTech Surveillance industry has largely drowned out advocates for nonsurveillance interventions. Fortunately, such mistakes need not be repeated going forward, and many past mistakes can still be undone.

"Digital Dystopia" is designed to empower decision-makers with the full and accurate information they need to protect all their students and keep them safe from invasive — and largely ineffective — surveillance products. The report begins with a discussion of 10 leading types of student surveillance technologies that are likely being marketed to your school district. We then engage in a deep-dive examination of the EdTech Surveillance companies' unsubstantiated and misleading marketing claims as well as the significant harms their products cause to students. After proceeding to highlight some important recent and ongoing fights against student surveillance, we conclude with recommendations on how readers can help promote better and more well-informed student safety and student surveillance technology decision-making.

The State of Ed Tech Surveillance Industry

Despite the near total absence of evidence that their products can play a meaningful role in keeping students safe, the EdTech Surveillance industry's marketing efforts have succeeded in diverting enormous amounts of education dollars into its questionable products. In 2021, K-12 schools and colleges in the United States spent an estimated $3.1 billion on security products and services (up from $2.7 billion in 2017).[13]

These dramatic annual expenditures on student surveillance technologies are made all the more troubling given that, as of the 2019-20 school year, 45% of K-12 public schools did not provide their students with any diagnostic mental health assessments to evaluate them for mental health disorders, and 58% did not offer any mental health treatments to lessen or eliminate student symptoms.[14] Likewise, while the School Social Work Association of America recommends that social work services should be provided at a ratio of 250 students to one social worker, ACLU analysis found that "less than 3 percent of schools nationwide, only about 3,000 schools, met [that] recommendation [and] more than 67,000 schools reported zero social workers serving their students."[15]

No conversation about surveillance in schools can take place without first understanding what technologies are currently being unleashed on elementary, middle, and high school students across the United States. As technology is constantly changing, so are the products available in the EdTech Surveillance marketplace. Though these technologies may continue to evolve, we have identified 10 leading surveillance technologies that are being sold to and used by school districts in 2023.[16]

- **Surveillance Cameras:** provide schools with the ability to watch students via live video feeds and to capture video recordings, sometimes with accompanying audio. Some cameras include police integration, which provides law enforcement with real-time access to the cameras, including the ability to control their operation and view their video feeds at any time.
- **Facial Recognition Surveillance:** Images captured by still and video cameras are run against photo databases using AI to identify persons in the images. Captured images can be analyzed either in real time or after the fact by applying the technology to pictures and video recordings. Technology can be used to document and analyze the movements and interactions of every student, teacher, staff member, and school visitor.
- **Access Control:** frequently combines the use of still or video cameras with facial recognition technology to screen visitors to schools.
- **Behavior Detection:** Artificial intelligence (AI)-driven technology watches and analyzes video subjects for behaviors it is either taught are problematic or which it concludes, via self-learning, may be "anomalous." Upon the observation of such behavior, the technology will issue a notification to school officials.
- **Social Media Monitoring Software:** scans students' public social media accounts for words and phrases that are designated by the school and/or the product provider to be problematic, even when they are off campus.[17] When the technology

scans a concerning post, it notifies the provider and/or school.

- **Student Communications Monitoring:** scans private student electronic communications, such as emails and documents written on school accounts and software applications, for words and phrases deemed by the technology provider and/ or school to be problematic and shares concerning communications with the provider and/or school. While normally it is not constitutional to intercept private communications, that can change when students use school-provided equipment to communicate.
- **Online Monitoring and Web Filtering:** monitors what students search for online and what websites they visit, and flags concerning activities for the technology provider and/or school. Can block access to website content deemed by school to be inappropriate.
- **Weapon Detection:** claims to be able to analyze video from surveillance cameras to detect and warn schools about the presence of a weapon.[18]
- **Gunshot Detection and Analytics:** audio-based system which is used to detect and report gun shots (sometimes integrated with video).
- **Remote Video Monitoring /Proctoring:** Using the integrated video camera on a students' computers, schools can monitor a student's attendance, focus, and compliance with anti-cheating rules.

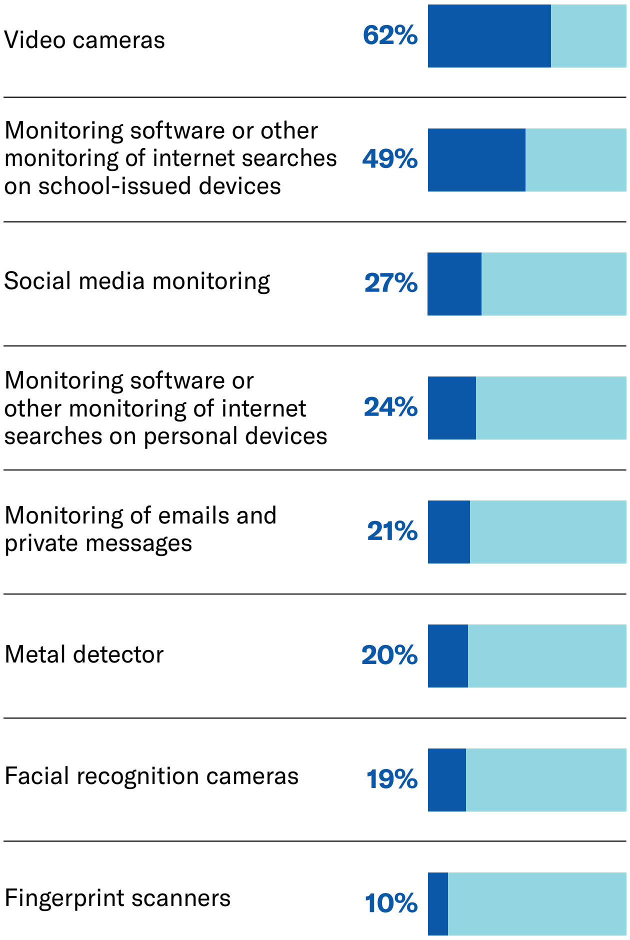
While the aforementioned surveillance technology descriptions detail each product's alleged capabilities, they should not be read to suggest the technology reliably functions as intended nor that it is capable of generating the advantageous results its operational capabilities might imply. In fact, many of the listed technologies are unproven, harmful, and flawed (see Appendix 1 for more detailed analysis of each type of technology, including its providers, stated capabilities, and harms).

Regretfully, these EdTech Surveillance products are increasingly becoming the norm in our nation's K-12 schools. A nationally representative sample of secondary school students (14-18 years of age) surveyed during the 2022-23 school year revealed that most students report the widespread use of these surveillance tools in their schools (see Figure 1).[19] Almost all (87%) of students claimed that their school used surveillance technology to monitor their behaviors — with most reporting multiple surveillance measures. During focus groups held by ACLU, a student described the varied types of surveillance in their school:

> "Our public WiFi in school is being restricted to monitor whatever we are doing. We are restricted to access certain sites to keep off bullying and entering some sites … we also have the cameras which are not everywhere but in certain areas like the hallway, entrance, strategic places. We also have tools that monitor our social media activities as well."
>
> — High school student, ACLU focus group participant

FIGURE 1

Portion of 14-18 Year Old Students Reporting Surveillance Technologies in their School



Source: YouGov. School Surveillance, fielded October 20-26, 2022. Commissioned by ACLU

The EdTech Surveillance Industry's Deceptive Marketing Practices

No Evidence of Efficacy

Despite industry claims, evidence establishing the EdTech Surveillance industry's products' effectiveness in meaningfully improving student safety is lacking. A pioneering Johns Hopkins study entitled "A Comprehensive Report on School Safety Technology" summed up the problem with the EdTech Surveillance industry's efficacy claims and its impact on school decision-makers:

> There is no national clearinghouse or center serving as an "honest broker" to test or recommend specific technologies or vendors to schools. As a result, many school officials rely on vendor-sponsored research, word of mouth, advice from police or security personnel, internal review, or grant funding criteria for making procurement decisions. Current evidence is limited on the success or cost effectiveness of technology in schools to prevent and mitigate crime, disorder, and catastrophic events.[20]

Our review of the existing research literature led to the same conclusions; namely, that there is little empirical evidence to support the claim that school surveillance technologies meaningfully increase safety or reduce violence in schools. With the exception of research on school surveillance cameras, which as discussed more fully below also does not support industry efficacy claims, there is scant published research on the impact of school surveillance technology at all.

Other independent journalists, academics, and researchers have likewise found that the EdTech Surveillance industry has failed to produce reliable data demonstrating its products work on a broad and consistent scale.[21] For example, as The 74 described a study of U.S. school districts from RAND: "From entry control equipment to video surveillance to violence prediction technology and software that scans students' social media profiles, [Heather Schwartz, lead author of the study] found independent research was surprisingly scarce on products' ability to prevent tragedies or mitigate risk"[22]

With respect to school surveillance camera companies, like Axis, NetTalon, and Avigilon, all have asserted, without providing solid evidence, that their cameras' can play a meaningful role in keeping K-12 students safe.[23] Yet, studies of video surveillance and crime prevention have found that cameras did not reduce violent crime,[24] and those findings are echoed in the research literature on school safety as well.

Multiple peer-reviewed studies of school safety measures, drawing from U.S. Department of Education's School Survey on Crime and Safety, have yielded similar conclusions: Surveillance cameras in schools do little to reduce violence or increase safety. Specifically, examining surveillance cameras have found little to no evidence that they reduce violence in schools. Specifically, one such study found that although use of multiple security measures may result in reduced property crime in high schools, none these measures, including surveillance camera, neither alone nor in combination – were related to decreased violence.[25] Another longitudinal study of a nationally representative sample of 850 school districts, Fisher and colleagues found no differences in outcomes related to school crime between schools with security cameras and schools without.[26]

Beyond these studies, general experience – of which we sadly have too much – demonstrates the limits of surveillance in keeping K-12 students safe. Our audit of K-12 school mass shootings over the past two-plus decades (1999 publication)[27] found that surveillance cameras were present in eight of the 10 schools that experienced these shootings.[28] That is a pretty poor deterrence record for a product being marketed as a tool for keeping students safe.

As for social media monitoring as a protective mechanism against mass violence, such as school shootings, the evidence just is not there. A 2021 in-depth examination by the U.S. Secret Service of planned, but thwarted, school shootings determined social media was implicated in a relatively small portion of the detection of these plots (16%), compared to the over 75% attributed to interpersonal communication.[29] In addition, in many of the 16% of cases, it was not social media alone that led to detection, but a combination of factors.

The U.S. Secret Service investigation focused on thwarted plots; other research on completed shootings identified at least one instance where a school shooting occurred despite the school district having social media monitoring in place prior to and during the incident.[30] Overall, the dearth of information about which surveillance technologies were in place when these horrific incidents occurred limits the conclusions that can be drawn about their efficacy, as research on efficacy is impossible to conduct without the data.

Fearmongering and False Advertising

In order to maximize demand for their products, the EdTech Surveillance industry's marketing efforts needed to secure the widespread acceptance of two narratives: (1) that there is a significant school safety problem that urgently needs to be addressed and (2) that their products are effective and the best available option for improving school safety. Because the EdTech Surveillance industry recognizes that the greater the school safety risk is perceived to be, the greater the demand for its products will be, the industry has strongly integrated fear-evoking narratives into its marketing efforts.

Not surprisingly, the "fear of school shootings has turned school security into a booming industry."[31] As Kenneth Trump, president of the National School Safety and Security Services, told The 74 in 2018, these high-profile shootings have created a climate that is "ripe for exploitation." Speaking about companies, like those in the EdTech Surveillance industry, that use school tragedies to market its products, he said, "It's not that they're villains ... but they're certainly opportunistic. At the end of the day, they're looking for new revenue streams."[32] Or as Jim Dearing, a senior analyst at the market-research firm IHS Markit, succinctly put it, "anxiety can be good for business."[33]

In their marketing materials, companies are capitalizing on schools' fears of violence and mass shootings in an effort to promote their products. As Image 1, online graphic from Gaggle, demonstrates,[34] some even use it to claim competitive advantages over other EdTech Surveillance companies — despite offering no evidence of actual efficacy.

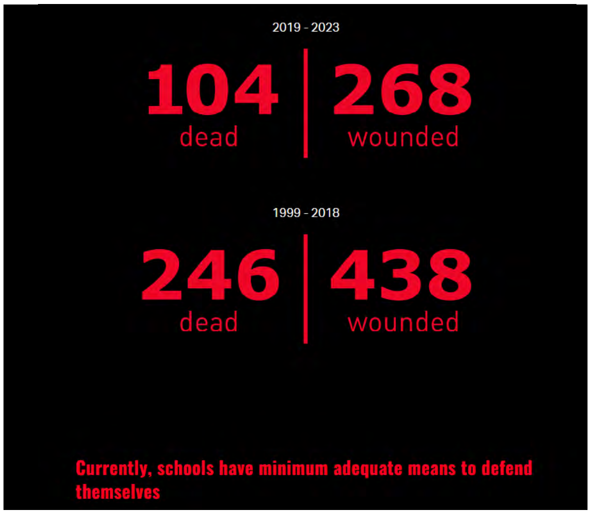
EdTech Surveillance companies further inflame schools' fears by presenting the false narrative that life-threatening violence in schools is common and

IMAGE 1

Gaggle ranked higher than its competitors in:
PREVENTING SCHOOL VIOLENCE

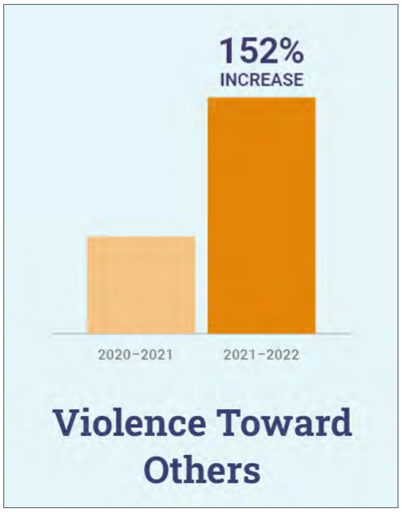
"School violence" marketing graphic from Gaggle website

IMAGE 2


2019 - 2023
104
dead
268
wounded
1999 - 2018
246
dead
438
wounded
Currently, schools have minimum adequate means to defend themselves

"Minimum adequate means to defend themselves" marketing graphic from NetTalon website

IMAGE 3



"Violence towards others" marketing graphic from Gaggle website

growing worse at astronomical rates, as the Gaggle[35] and NetTalon[36] in Images 2 and 3 seek to represent.

What is conveniently missing from the EdTech Surveillance companies' marketing narrative is the larger context. According to David Ropeik, a consultant on the psychology of risk perception, the likelihood of a K-12 public school student being shot and killed at school is roughly 1 in 614 million.[37] That is more than twice as unlikely as winning the top prize in the Powerball or Mega Millions lotteries.[38] In fact, data shows schools are a particularly safe environment for children.[39] Nevertheless, as the EdTech Surveillance industry well knows, the emotional impact of fear can override the intellectual impact of statistics, which is why, according to the professional educators' association Phi Delta Kappa International, a third of parents still fear for their child's safety at school.[40]

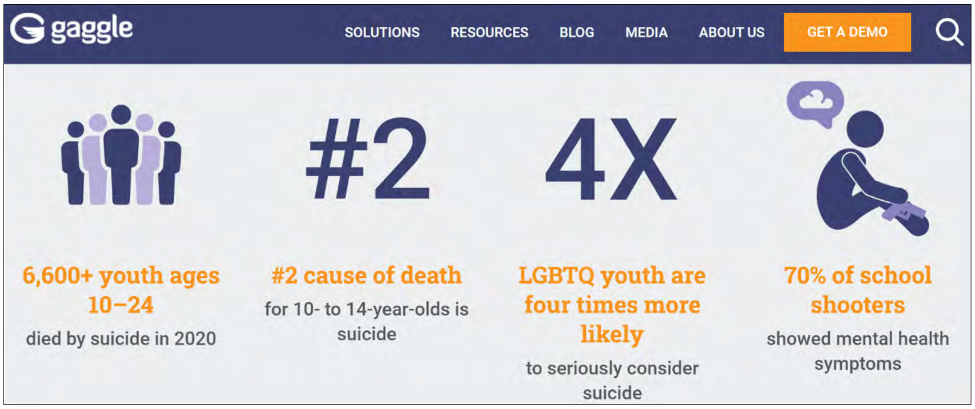
Recognizing that the more fear they can generate, the greater the demand for their products will be — and perhaps also recognizing that their efficacy claims around preventing school shootings are demonstrably weak — EdTech Surveillance companies have also focused on stoking fear around student self-harm, suicides, and bullying, as images 4, 5, and 6 from Gaggle,[41] GoGuardian,[42] and Securly[43] reflect.

There is no question that self-harm, suicide, and bullying are serious issues and worthy of schools' attention. But to fully capitalize on school districts' fears, the EdTech Surveillance industry not only needed to maximize the perception that these crises were real and worsening, but also that its products were able to identify and positively address large numbers of problematic scenarios well before any other available intervention could.

And if some had to play fast and loose with the facts to make such claims, so be it.

The marketing efforts of Bark, an app that monitors millions of kids' internet activity, provides a stark example of the ethical lines the EdTech Surveillance industry seems willing to cross in pursuit of profits. While promoting its surveillance tools to North and South Carolina school districts, Bark wanted it to appear like there was an epidemic of cyberbullying and death by suicide in the region. The company pushed out questionable statistics to local TV stations, telling them it had identified 14,671 instances of students expressing a desire for self-harm or suicide, as well as 88,827 instances of cyberbullying, in the Carolinas alone.[44] A subsequent Vice News investigation concluded that Bark was clearly inflating these "self-harm or suicide" Carolina-based numbers, as they were greater than the total numbers Bark reported nationwide for the same time period. Similarly, the number of reported cyberbullying cases in the Carolinas would have constituted 65% of the total 135,984 cases Bark detected nationwide that year. According to Vice News, "the rest of the data shared with the Carolina TV stations [was] similarly disproportionate."[45]

IMAGE 4



6,600+ youth ages 10–24

died by suicide in 2020

#2 cause of death

for 10- to 14-year-olds is suicide

LGBTQ youth are four times more likely

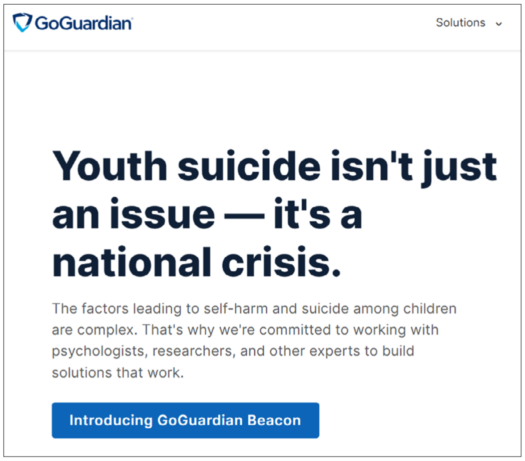
to seriously consider suicide

70% of school shooters

showed mental health symptoms

“Suicide/mental health” marketing graphic from Gaggle website

IMAGE 5

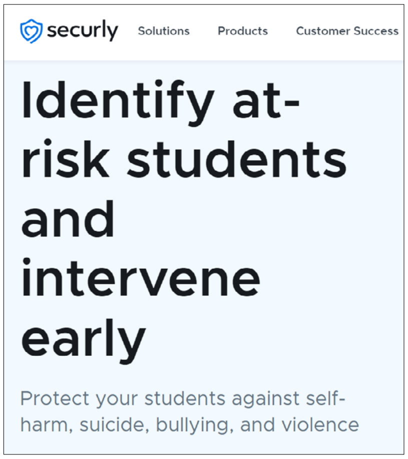


Youth suicide isn't just an issue — it's a national crisis.

The factors leading to self-harm and suicide among children are complex. That's why we're committed to working with psychologists, researchers, and other experts to build solutions that work.

“Youth suicide” marketing graphic from GoGuardian website

IMAGE 6



Identify at-risk students and intervene early

Protect your students against self-harm, suicide, bullying, and violence

“Identify at-risk students” marketing graphic from Securly website

Comparing the data reported by Bark with the data from Securly, a similar student surveillance company responsible for monitoring 10 million students during that time period, illustrates how EdTech Surveillance companies can manipulate data to feed the narratives they are using to target school districts. Despite monitoring two and a half times as many students, Securly reported detecting only five cyberbullying incidents, compared to Bark’s 135,984. Similarly, Securly reported detecting 400 discussions of interest in self-harm or suicide during the same period that Bark reported 11,548.[46]

While some fraction of this discrepancy could result from the companies having different definitions of “self-harm” or “cyberbullying,” school districts must be wary of self-reported (and self-serving) numbers and insist on independent verification of any EdTech Surveillance marketing claims.

Claiming Success Without Real Evidence

Even with a highly motivated, fear-driven customer base, the booming EdTech Surveillance industry marketplace would not exist if its companies had not succeeded in convincing school districts that its products are effective at reducing school shootings, student self-harm, suicides, and bullying. And so, despite the absence of reliable, independent data supporting their case, that is exactly what the EdTech Surveillance companies claimed.

The EdTech Surveillance industry has relied on five methods to misleading school districts about the efficacy of their products: (1) providing specific, unsubstantiated success metrics, (2) making claims of general efficacy, (3) insinuating effectiveness, (4) treating opinions like facts, and (5) highlighting one-off success stories.

Providing Specific, Unsubstantiated Success Metrics

Many unsubstantiated efficacy claims asserted by EdTech Surveillance companies present what appear to be precise, data-driven assertions but are actually impossible to verify. For example, Gaggle claims that "during the 2021-2022 academic year, [it] helped districts save the lives of 1,562 students who were planning or actively attempting suicide."[47] Similarly, Bark claims its student surveillance software has "'prevented' 16 school shootings."[48] Aside from a total absence of publicly shared details substantiating these claims, the claims themselves are impossible to accurately make or verify because, as The New York Times correctly observed, "calculating figures like suicide prevention is a murky science at best."[49] Proving precise suicide prevention figures is self-serving and irresponsible; it is virtually impossible to say that an action would have been taken if not for a specific intervention (e.g., students may talk about suicide or violent acts but have no real intention to act), and it is similarly impossible to rule out if an alternative intervention — like a friend reporting a troubling text or an interaction with a school counselor — would have had a similar impact.

Another related, deceptive marketing tactic is to support one's efficacy claims with specific data points that are vague and ill-defined. Securly, for example, claims its products "helped school officials intervene in 400 situations that presented an 'imminent threat.'"[50] Referencing a precise number suggests its impact claim is reliable and data-driven, but "intervene" does not necessarily suggest a positive outcome, "helped" does not mean the same intervention or outcome would not have occurred without its "help," and whether something is an "imminent threat" is subject to interpretation and manipulation. What is not vague is the message schools were intended to take away from the marketing statement: Securly averted 400 tragedies and if you buy our product, we can do the same for you.

By pushing out precise but unsubstantiated and unverifiable efficacy claims to promote their products, EdTech Surveillance companies are counting on school district officials accepting their efficacy claims without asking too many questions. To borrow the converse of the slogan for the old retail clothing store Syms,[51] for the EdTech Surveillance industry, "an educated consumer is its worst customer."

Making Claims of General Efficacy

To avoid making efficacy claims using specific figures it cannot verify, the EdTech Surveillance industry frequently pivots to asserting strong but general claims of efficacy that are untethered to any specific data points. Gaggle, for example, asserts that its products are not only effective in "preventing suicides," "preventing school violence," "limiting bullying and harassment," "stopping child abuse and harassment," "stopping sexual abuse," and "stopping childhood predators," but also that Gaggle is "ranked higher" at doing so than its EdTech Surveillance industry competition.[52]

The technique of using general efficacy claims seems to be particularly popular amongst EdTech Surveillance companies marketing surveillance cameras. Axis claims its surveillance cameras "deter illegal, illicit, or otherwise unwanted behaviors — during and after school hours" and that its "audio-equipped cameras can distinguish aggression."[53] NetTalon, asserts that its surveillance cameras, coupled with the other school safety interventions it markets, will "dramatically improve school safety against active shooters or other terrorist attacks."[54] As discussed elsewhere in this report, these claims are particularly fanciful given that existing research and actual school experience shows surveillance cameras are generally ineffective in deterring bad conduct.

Insinuating Effectiveness

Many of the EdTech Surveillance industry's misleading claims fall under the category of insinuation. Here, rather than overtly stating its products are effective, the industry invites school districts to connect closely aligned — but ultimately fallacious — marketing dots. For example, at the very top of its website, surveillance camera company Avigilon states that "safety for students, staff, and faculty is our top priority." The clear insinuation is that its camera products, which its website markets, will provide those things, and it can make such an insinuation without providing proof that it is true.

Social Sentinel, which relies on black box algorithms to monitor digital conversations and detect "threats", makes numerous bold insinuations about the effectiveness of its student surveillance products. These include stating that its products are "the smartest way to stay ahead of harmful intentions," asking potential school district customers "if you could prevent someone from harming themselves or others would you?" and concluding the text on the front page of its website with "Improve Violence Prevention Today."[55]

Social Sentinel conveniently does not mention that it is often, as The Verge points out, "mining shallow insights from available data, [while] providing few benefits to outweigh the privacy harms."[56]

Treating Opinions Like Facts

Oftentimes, companies recognize that stating their own subjective opinions would appear self-serving. To get around this, the EdTech Surveillance industry prefers carefully curating reviews from school administrators and staff, which it then uses to convince its peers in other school districts.

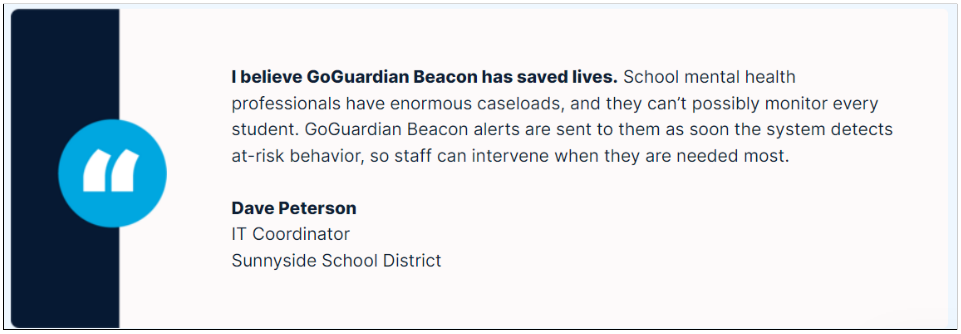
One such example comes from the GoGuardian graphic (see Image 7).[57] It is enough to note how different the statement would read if it said "GoGuardian Beacon has saved lives" instead of "I believe GoGuardian Beacon has saved lives." The former statement is one of fact; the latter, which GoGuardian uses, is merely an unsupported statement of opinion.

Another such example comes from the Gaggle graphic shown in Image 8.[58] While the graphic leads with a statement, in bold font, that "Gaggle Is Saving Lives," the rest of the graphic supports that statement with nothing but subjective opinions; to wit, that the positive evaluations of Gaggle's products are based on "feedback," as to what educators "indicated," "believe," "said," and "reported."

These kinds of statements are more a commentary on how effective the products' marketing is in influencing educators' opinions than how effective their products actually are — they simply show that the quoted or surveyed school officials have internalized the EdTech Surveillance companies' marketing claims despite the absence of hard, factual evidence.

As reported by Vice.com, Michael Fox, the superintendent of the Demarest School District in Bergen County, New Jersey, sent emails to fellow New Jersey school district administrators promoting the products of Verkada — a rapidly growing surveillance camera company that is active in the EdTech Surveillance market. Fox sent out dozens of emails to fellow administrators containing statements like, "In the fall we upgraded all of our security cameras and added vaping sensors in the bathrooms.... [Verkada was] excellent to deal with throughout the process making it seamless. The products are incredible and everyone we worked with was outstanding. My

IMAGE 7

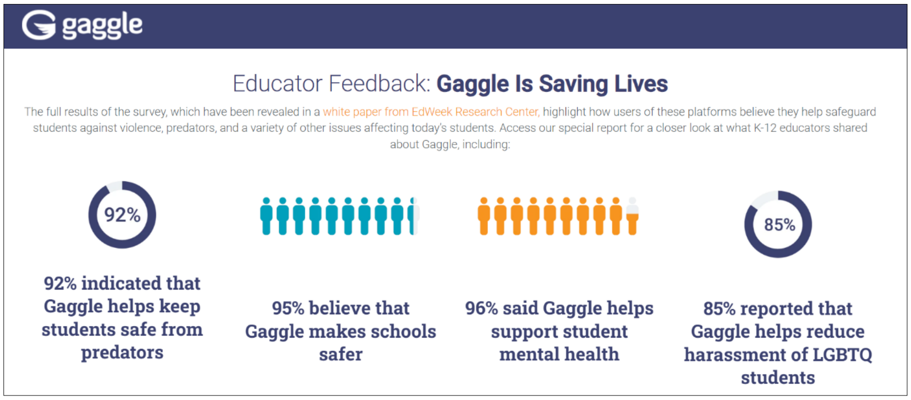


I believe GoGuardian Beacon has saved lives. School mental health professionals have enormous caseloads, and they can't possibly monitor every student. GoGuardian Beacon alerts are sent to them as soon the system detects at-risk behavior, so staff can intervene when they are needed most.

Dave Peterson
IT Coordinator
Sunnyside School District

"Saved lives" testimonial marketing graphic from GoGuardian website

IMAGE 8



Educator Feedback: **Gaggle Is Saving Lives**

The full results of the survey, which have been revealed in a white paper from EdWeek Research Center, highlight how users of these platforms believe they help safeguard students against violence, predators, and a variety of other issues affecting today's students. Access our special report for a closer look at what K-12 educators shared about Gaggle, including:

92% indicated that Gaggle helps keep students safe from predators

95% believe that Gaggle makes schools safer

96% said Gaggle helps support student mental health

85% reported that Gaggle helps reduce harassment of LGBTQ students

“Saving lives” marketing graphic from Gaggle website

IT and Principals rave about the system. … I highly recommend a zoom or in person meeting.”[59] As reported by Vice, Fox failed to mention was that he was apparently coordinating his efforts with Verkada sales representatives, who were copied on his emails.[60]

The EdTech Surveillance industry’s efforts to enlist validators from schools and other educational organizations have been fairly relentless, especially after school tragedies present an opportunity it can capitalize on. Amanda Klinger, director of operations at The Educator’s School Safety Network,[61] told Education Week that after the Uvalde school shooting, requests from EdTech Surveillance companies to have her organization partner with them rose significantly. Klinger was surprised by the volume of requests, given that her nonprofit has been “pretty consistent in terms of our hesitancy and concern about some of the costs and the limited efficacy of some of these measures … Yet I cannot keep people who are developing these things from banging down our door.”[62]

Highlighting One-Off Success Stories

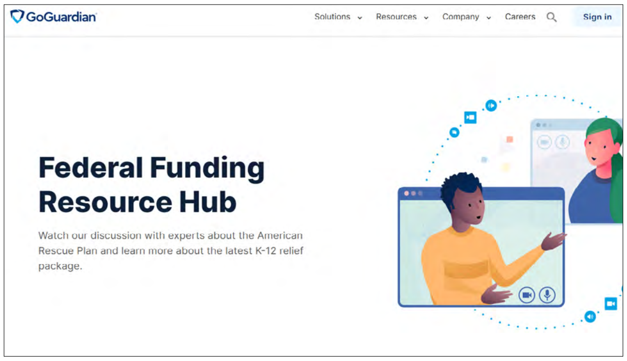
Companies selling education surveillance technology often use stories that tug at administrators’ heart strings, presenting one-off success stories as the rule, instead of the exception. One such example comes from a December 2022 Vice News report on the EdTech Surveillance company Gaggle. In that story, Vice News interviewed a student from school in Burien, Washington, that Gaggle had referred Vice News to. The student was flagged by Gaggle for writing a document titled “Essay on the Reasons Why I Want to Kill Myself/Didn’t.” While the student acknowledged that Gaggle had led to adult intervention she believes would likely not have happened if not for Gaggle, her overall reaction to Gaggle’s monitoring was mixed. The student stated that Gaggle might be helpful “in some ways, but I also kind of think that it’s — I wouldn’t say an invasion of privacy — but if obviously something gets flagged and a person it wasn’t intended for reads through that … that’s kind of uncomfortable.”[63]

The student’s discomfort with Gaggle is understandable. Having a school-retained EdTech Surveillance company read through a student’s private, personal documents is essentially the digital equivalent of thumbing through a student’s paper diary. The Burien student told Vice News that she was embarrassed by having her private thoughts read, but that the embarrassment did go away “after two years.”[64]

Such one-off success stories are not cultivated to highlight how the technology may have harmed other students nor do they offer space to examine if other interventions could have achieved similar success without their products’ accompanying harms. Rather, they cherry pick stories to suggest their outcomes are the norm. But finding a handful of positive stories to highlight is hardly a tall task given that the EdTech Surveillance industry’s products monitor millions of students. After all, even a broken clock can be made to appear to be working well twice a day.

And of course, nowhere in the EdTech Surveillance companies’ marketing materials can school districts learn about harmful incidents their surveillance products failed to prevent, or about vulnerable students who were unfairly targeted by surveillance technology in their schools, or about students who were afraid to talk to their teachers or school counselors when they needed help because the unease and betrayal they felt being spied on by their schools eroded their trust.

IMAGE 9

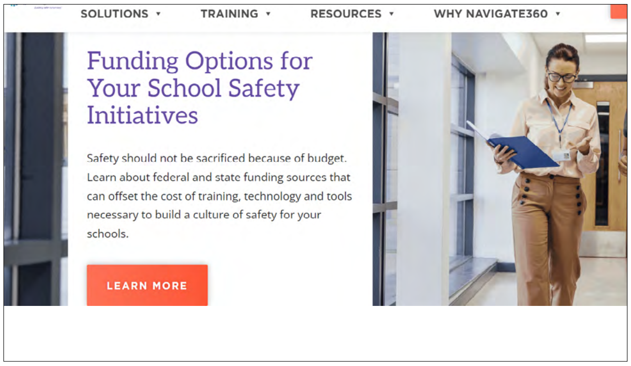


Federal Funding Resource Hub

Watch our discussion with experts about the American Rescue Plan and learn more about the latest K-12 relief package.

“Federal funding” marketing graphic from GoGuardian website

IMAGE 10

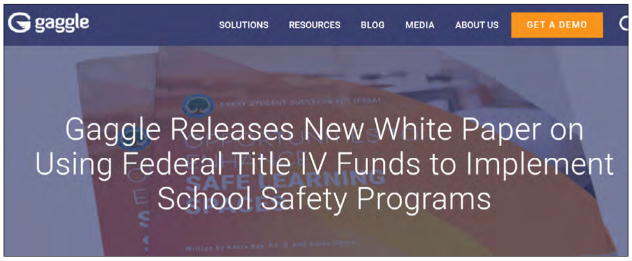


Funding Options for Your School Safety Initiatives

Safety should not be sacrificed because of budget. Learn about federal and state funding sources that can offset the cost of training, technology and tools necessary to build a culture of safety for your schools.

“Funding options” marketing graphic from Navigate360 (Social Sentinel) website

IMAGE 11



Gaggle Releases New White Paper on Using Federal Title IV Funds to Implement School Safety Programs

“Federal Title IV funds”” marketing graphic from Gaggle website

We Can’t Prove It Works, But At Least Your School Won’t Have To Pay For It!

As The 74 observed in 2018, “Security trade groups have lobbied for hundreds of millions of dollars in ... funding for school safety measures. The gun legislation that Congress passed last week [in June 2022] includes an additional $300 million to bolster school security.”[65] And their lobbying has had equal success generating hundreds of millions of dollars in grant funding from individual states as well.[66] These lobbying efforts were all designed to maximize the EdTech Surveillance industry’s revenues by making its products much cheaper — and sometimes even free — for schools to acquire.

The EdTech Surveillance industry’s strategy here appears pretty clear: convince schools that, even if the benefits of its products are speculative, large pools of industry-driven, government-funded grants have often made its immediate monetary costs to schools either low or nonexistent.[67] With that being the case, the argument follows, there is little to no risk in schools acquiring them. As the three EdTech Surveillances company website screenshots below illustrate, they will even tell you where and how to get the money.

Given this approach, it should come as no surprise that when EdTech Surveillance company Verkada enlisted the help of the Demarest, New Jersey, school superintendent to sell its products to other school districts, part of his efforts was to offer to “coach[] them how to use federal COVID funds to pay for the upgrades.”[68]

Schools Must Remain Vigilant … Against the EdTech Surveillance Industry

The $3.1 billion EdTech Surveillance industry, which is expected to grow by more than 8% annually on average,[69] is not primarily in the business of keeping kids safe. Its industry is not comprised of nonprofit companies, and it is not driven by the pursuit of the public good above all else. Its primary goal is to make money. Lots of it. And that means the information it provides to schools is designed to drive interest in purchasing its products, not to provide an honest analysis of its benefits and drawbacks.

Questionable statistics, unsupported efficacy statements, and heart-warming stories may make you feel like buying its products will make your schools safer, but "feeling safer" is not the goal — "being safer" is. School districts should not view EdTech Surveillance companies as their allies, partners, or saviors in pursuing that goal. Each is simply a company trying to sell you a product. No more and no less. Accordingly, the best way for school districts to achieve their goal of truly improving school safety is to be savvy, well-educated consumers, who think long and hard before making any decisions about acquiring and using student surveillance technologies.

Surveillance Technology in Schools Is Hurting Kids, Not Helping Them

"I feel like I like this school has my fingerprints on file, they have my face, just like back off … just give me room to breathe."

— High school student, ACLU focus group participant

School districts' embrace of student surveillance technologies comes with substantial hidden costs — costs that are far more significant than mere financial ones, because these costs come at the expense of the very students the products are claiming to protect. In short, in their quest for safety, school districts are inadvertently exposing their students to harm.

The harms of surveillance technology have been well documented by journalists, scholars, think tanks, and by students themselves.[70] Along with a recognition of those harms, our research also revealed students' complex feelings about school surveillance. Facing concerns about their own safety, which have been amplified by the extensive and sensational coverage incidents of school violence often receive, students may arrive at the conclusion that being under constant surveillance is the price they must pay for security. At least in part, this belief appears to stem from the fact that students — like their school districts — have been bombarded by unsubstantiated claims that surveillance will keep them safe. The EdTech Surveillance industries' largely unsubstantiated talking points are not only influencing school districts, they are also impacting students and others in the school community.

A few students in our focus groups were able to point to individual incidents of surveillance being used to identify bullying and reduce student misconduct. However, while these specific outcomes were viewed positively, any mention of these potential benefits were generally countered with descriptions of the damage caused by surveillance, often by the same students.

Students surveyed and those participating in focus groups identified numerous dangers presented by surveillance technologies. These generally centered around lack of privacy, limits on free expression, erosion of trust, and unfair treatment (see Table 1). They also complained that surveillance impacts their interactions with educators, administrators, and their peers in a negative or restrictive way. As one student explained,

> "I can imagine a lot of single case scenarios in which school surveillance can have positive impacts … but I think that the majority effect of it would just be increased paranoia for students because the vast majority of students have no ill intent, so while it could be advantageous to weed out those who have malicious intent, I think the majority of students would just feel violated."

Students' complicated, and sometimes seemingly contradictory, feelings about school surveillance are not unique to students in our research. A growing body of research on youth perspectives has, not surprisingly, documented tensions between privacy and security as related to surveillance technologies, both in and out of school.[71] Notably, although students may initially express more positive or neutral feelings about surveillance, when conversations progress beyond the surface level, students reveal more misgivings and concerns.[72]

Furthermore, students' beliefs about school surveillance must be considered in the context of their awareness and understanding of the technologies themselves. Prior research has revealed ways in which students' beliefs about school surveillance are not always accurate, particularly when they are left in the dark about the purpose and placement of such surveillance.[73] Similarly, our research indicated that students have varying degrees of knowledge not only of what is being used in their schools, but also about the possible impacts of these technologies.

TABLE 1

Students' Concerns About School Surveillance

I always feel like I'm being watched	**32%**
How it could be used to discipline me or my friends	**27%**
What your school and companies they contract with do with the data (such as sell it, analyze it, etc.)	**26%**
How it limits what resources I feel I can access online	**24%**
Could be shared with law enforcement	**22%**
Could be used against me in the future by a college or an employer	**21%**
Could be used to identify students seeking reproductive health care (such as contraception or abortion care)	**21%**
Could be used to identify students seeking gender-affirming care (such as transgender students seeking hormones)	**18%**
Could be used against immigrant students, especially those who are undocumented	**18%**
How it limits what I say online	**17%**
Could be used to "out" LGBTQIA+ students	**13%**
I have no concerns regarding surveillance in my school	**27%**

Source: YouGov. School Surveillance, fielded October 20-26, 2022. Commissioned by ACLU

Regardless of whether the harms of surveillance experienced by students come with mixed feelings does not, in any way, lessen the impact of those harms. And as with surveillance in general, while student surveillance has widespread negative impacts, not all students and student groups are impacted the same.

Teaching Students the Wrong Lessons

The harms of student surveillance manifest themselves in many ways. The first category of harm that surveillance causes is particularly troublesome because it is antithetical to our schools' educational mission; to wit, those who have been trusted to educate our children — to help them grow intellectually, socially, and emotionally — are inadvertently teaching them the wrong lessons by bringing surveillance technologies into their schools.

As one expert, University of North Carolina law professor Barbara Fedders, put it, "research demonstrates the damaging effect of surveillance on children's ability to develop in healthy ways. Pervasive surveillance can create a climate in which adults are seen as overestimating and overreacting to risk. Children, in turn, cannot develop the ability to evaluate and manage risk themselves in order to function effectively."[74] Beyond that, "social science also suggests that children experience surveillance as a form of control that limits their choices and inhibits their ability to act autonomously. Surveillance shapes behavior through the threat of punishment for bad actions, which troublingly means that children may make decisions based on the potential for negative consequences instead of as an expression of their own values and beliefs. This in turn can diminish children's ability to self-regulate, to navigate personal boundaries, and to learn to assess risk and reward on their own."[75]

And the more student surveillance technologies a school district acquires, the worse the damage becomes. As Chris Gilliard, writing in Wired explained, "if society were to deploy every surveillance and analytical tool available, schools would be hardened to a point where even the most anodyne signs of resistance or nonconformity on the part of young people would be flagged as potentially dangerous — surely an ongoing disaster for the physical, social, and emotional well-being of children, for whom testing boundaries is an essential element of figuring out both themselves and the world they live in."[76]

Teaching children to fear risk taking, acting upon their own values and instincts, and developing into a person that is uniquely their own has no place in a constitutional democracy that is grounded in civil rights and liberties like the United States. Instead of relying on surveillance to protect students, it is becoming increasingly important for our schools to protect our students *from* surveillance.

Everybody Hurts: How Surveillance Undermines Privacy, Erodes Trust, Inhibits Self-Help and Increases Fear

While surveillance technologies threaten the civil liberties and well-being of all students, they do not impact every student and group of students in the same way. We begin our discussion of student surveillance harms with those that apply universally to all students.

EdTech Surveillance Undermines Privacy

No civil liberty is more directly threatened by student surveillance than the right to privacy. While today's students may increasingly feel like they live in a society where privacy is more of an aspirational goal than a reality, the truth is that privacy is as important as ever, although it requires more work than ever to protect it.

Although privacy is properly framed as a right in and of itself, it is perhaps more importantly viewed as an essential gateway to other civil rights and liberties. Privacy protects the right to explore and investigate new ideas, to think innovative and controversial thoughts, to associate with unpopular groups, and to communicate groundbreaking ideas your community or the world at large may not yet be ready to hear. It protects a person's right to keep an electronic diary on their home computer as much as it protects their right to keep a paper diary under their bed. It protects the right to ask questions and obtain treatments related to health care. It protects a person's right to have thoughts and ideas that are purely their own. Student surveillance not only undermines all of these privacy rights for students, it also teaches them to fear and even expect the unveiling of their private thoughts and actions.

These are not imagined concerns. According to a national poll by YouGov commissioned by ACLU, nearly a third of students (32%) survey reported that school surveillance made them feel like they are being watched. As one student in our focus groups explained,

> "You know, it always keeps me in check that I have to be cautious of myself, that someone is monitoring me. And it's not entirely cool. Yes, I know it's for my protection, all the stuff still, but it's not entirely cool."

The concern about being watched is clearly limiting some students' ability to express themselves, even outside of the school environment, as one student mentioned in our focus groups when discussing their school's social media monitoring: "I feel on social media is my safe space where I can just do my name my way but when we are being monitored, I feel scared somehow."

Students are feeling the impact of their schools' prying eyes and they do not like it. As one student in our focus group noted, "things are meant to be personal, and my inbox should be one of those." Another described how surveillance impacted them: "I feel uncomfortable. I feel very uncomfortable being watched. I don't, I don't feel like myself." This discomfort may result in students feeling they must engage in proactive measures to protect their privacy, as a high school junior complained at an October 2018 Woodbridge, New Jersey, school board meeting: "We have students so concerned about their privacy that they're resorting to covering their [computers'] cameras and microphones with tape."[77]

For that reason, it is critical school districts learn to "understand privacy as a child's welfare or developmental right, rather than only a negative right against governmental intrusion, [because then] it is easier to see how that right is worth protecting against the emerging student surveillance regime.

“Things are meant to be personal, and my inbox should be one of those.”

— ACLU student focus group participant

Child development scholars argue that surveillance does not allow students to practice acting and reasoning independently and thus keeps them from developing the skills and habits of mind they will need to one day exercise the liberty rights we afford adults. What is more, as a new generation of learners becomes acculturated to and accepting of surveillance, children may be more likely to become adults who do not value their own privacy — or that of others.”[78] In short, not only do student surveillance technologies threaten students’ own privacy and related civil rights and liberties, their use also teaches students to undervalue the privacy and constitutional rights of others.

Over a quarter of the students we polled (26%) reported concerns about what their school and any Ed Tech Surveillance companies they contract with would do with the surveillance data they collect, whether it be how the school uses it themselves or how it might be sold by the companies. And it should be noted that the more surveillance data a school district collects, the greater the risk hacking presents to students’ privacy. A 2017 review of privacy policies of over 100 educational technology products by the Electronic Frontier Foundation revealed that the vast majority of policies failed to include key elements, such as encryption or de-aggregation of data.[79] They found that some products even provided schools the opportunity to determine their own policies to govern personal student data that was collected by these products. And we have already seen these types of privacy and security gaps exploited — as numerous hackers and even school officials improperly use student surveillance technologies to intrude on students’ lives in and outside of school.[80]

Ultimately, a discussion of how the loss of privacy threatens the very foundations of a free society is a subject worthy of entire books, rather than a single subsection of a report on student surveillance. Luckily, every K-12 school district already has access to a resource that can educate them on how privacy-infringing, government surveillance has generated fear, stifled free thought, and oppressed entire populations.[81] That resource is its history teachers.

EdTech Surveillance Erodes Trust

Another general harm the use of student surveillance technologies creates is a breakdown of trust between students and adults. Although studies of the impact of school surveillance technologies are few and far between, the existing research highlights this erosion of trust.[82] As Vice News reported, “The few published studies looking into the impacts of [student surveillance] tools indicate that they may have the ... effect [of] breaking down trust relationships within schools and discouraging adolescents from reaching out for help.”[83] Ironically, the same tools the EdTech Surveillance industry is promoting as a means for identifying students in need of help may actually be discouraging those students from reaching out to school officials and other adults for help when they need it.

The ACLU researchers heard this directly from the high school students in our focus groups. Nearly all participants indicated that school surveillance would negatively impact their interactions with school staff, their communications with friends, what they do online and on social media, what groups or clubs they might join, and how they feel at school. Students with surveillance in their schools were cognizant of being monitored, sharing that they would alter what they say around teachers, avoiding private conversations to prevent “getting in trouble” or having a negative outcome (e.g., telling parents). For example, students discussed consciously refraining from sharing experiences of abuse or that they were in foster care or struggling with mental health issues, all because they were being surveilled. Furthermore, almost 1 in 5 students (17%) in our nationwide poll had concerns about school surveillance limiting what they say online.

Aside from the direct harm this loss of trust causes students, its secondary effects might be even more problematic. Maintaining student trust may be a central component of keeping students safe because the information sharing that trusting student-teacher/administrator relationships foster can allow for adults to respond appropriately and take action in face of potential threats to student safety. As the ACLU of Pennsylvania noted:

> School shootings and bombings have been prevented when a student shared a concern with a trusted school staff member. … For example, a student may overhear a discussion about a possible act of extreme violence by a current or former student and report it to a teacher. Researchers call these situations "averted violence." Students are more likely to come forward with information that will prevent major acts of violence when they feel supported, respected, and valued.[84]

By eroding students' trust in their educators and schools, student monitoring technology can undermine the safety of an entire school community.

EdTech Surveillance Inhibits Self-Help

When a student in need of help or information is inclined to try to help themselves, their school's actual or perceived use of student surveillance technologies may discourage them from doing so. The erosion of student trust may not only prevent students from reaching out directly to teachers, counselors, or nurses for support or information, but it may also impede students' ability to seek it out elsewhere. Nearly a quarter of the students we surveyed (24%) were concerned about how school surveillance limits the resources they feel they can access online. Believing their conversations are being recorded or their electronic communications are being monitored may lead students to limit their outreach for information or requests for help.

This may be particularly damaging for students who do not feel they can turn to their parents or communities for certain information. As Barbara Fedders wrote, "Contemporary student surveillance regimes can sometimes function to keep students from obtaining important, age-appropriate reproductive health and sexual orientation/gender identity information that they need from their schools — especially if they cannot get it from their parents."[85]

Many students are strongly aware of the danger surveillance may present to those in need of certain types of critical health care. Approximately 1 in 5 students surveyed indicated that they were concerned surveillance could be used to identify students seeking care; specifically, those seeking reproductive health care, including abortion (21% of students reported), and seeking gender affirming care (18%).[86] Given the current political climate, where abortion care is being criminalized[87] and laws are being passed to ban even the discussion of transgender health care,[88] the consequences of being identified by such surveillance are becoming increasingly serious.

In a world turned upside down, schools' use of surveillance technologies is transforming America's school system, which was developed to promote and advance learning, into one that discourages or even prevents it.

EdTech Surveillance Increases Fear and Criminalizes Youth

Like the EdTech Surveillance industry's marketing itself, the use of surveillance technologies increases fear amongst students and other school community members (which in turn, may further drive demand for surveillance technologies). In the case of visible surveillance measures, like security cameras, such technologies increase fear by serving as a constant reminder of the threats they are allegedly in place to address.

While threats like mass shootings are actually quite rare,[89] in many schools these reminders are omnipresent, as is the fear they may induce in some students. ACLU's polling of students found evidence that at times, students may believe surveillance to be a potential balm for these real or propagated threats, with a substantive minority reporting that surveillance in schools made them feel "safe" (40%) and "protected" (34%). And yet, more than 1 in 10 students reported surveillance as a mechanism that made them feel quite the opposite: "anxious" (14%), "exposed" (15%), "paranoid" (13%), and "violated (12%), with a smaller portion directly reporting that thinking of surveillance in schools made them feel "unsafe" (7%) and "scared" (5%).

Students in our focus group explained how surveillance can have the dual effect of making

> “It’s the same kind of thing, you know, we treat kids like monsters and like criminals, then … it’s kinda like a self-fulfilling prophecy.”
>
> **— ACLU student focus group participant**

them feel protected, but uncomfortable or even unsafe at the same time:

> “Well, when it comes to surveillance in school, quite a lot of it makes me feel more scared because I believe everything I do, I’m being watched and monitored so I’m not free to express myself freely, you know … I feel someone is watching me, monitoring me, so it makes me feel unsafe at times, although it’s for my own security but still I feel unsafe.”

While surveillance technologies may provide a false sense of security to students, there is little empirical evidence that they actually reduce violence or increase school safety (see the previous section, No Evidence of Efficacy). Furthermore, a 2018 survey of over 50,000 students across the state of Maryland found that security cameras inside schools were actually associated with lower feelings of safety and equity. The results of the study led the researchers to conclude that consistent surveillance may result in students feeling as if they are being treated like criminals.[90] A substantiative portion of students in our national survey shared these concerns — approximately a quarter reported concerns about how surveillance could be used to discipline them or their friends (27%) and how it could be shared with law enforcement (22%). Social media monitoring was a particular concern among focus group participants, as students shared examples of peers being reprimanded or punished for posts, including one who was suspended for a personal Instagram post that showed alcohol in the background.

This sentiment was also raised by several students in the ACLU’s focus groups as well, with one student claiming, “it’s the same kind of thing, you know, we treat kids like monsters and like criminals, then … it’s kinda like a self-fulfilling prophecy.”

The Disparate Harms of Surveillance on Marginalized Students

For a number of already vulnerable groups of students, the harms caused by student surveillance technologies may be even greater than for the average student. These vulnerable groups include students of color, students with disabilities, LGBTQ+ and nonbinary students, undocumented students/students with undocumented family members, and low-income students.

Students of Color

School surveillance can intensify the well-documented racially discriminatory impacts of the school-to-prison pipeline — the unequal and discriminatory system of school disciplinary rules, procedures, and spending priorities that frequently substitute law enforcement for school and family involvement — particularly when students of color are accused of wrongdoing.[91] According to the Department of Education’s most recently available Civil Rights Data Collection, Black students face suspensions at rates two times that of white students, while Indigenous and bi/multiracial students were also disciplined at higher rates.[92]

The way student surveillance technologies operate, and are integrated into already inequitable school disciplinary systems, threatens to make attending school even more risky for many students of color, and especially Black and Brown students. Not only are these surveillance technologies more likely to cause harm to these students as compared to their white peers, but “schools with a preponderance of students of color within the school building [are] more inclined to adopt strict surveillance practices”[93] in the first place. Prior research using data from the

U.S. Department of Education confirms that schools in communities of color are more likely to have surveillance measures, such as cameras, despite their not necessarily facing greater safety risks.[94]

Recall that the student communications-, document-, and social media-monitoring products sold by the EdTech Surveillance industry operate by flagging what the surveillance provider and/or school district deem to be problematic words and actions by students. But as Priyam Madhukar wrote for the Brennan Center for Justice, "When schools introduce these technologies, they open the door to labeling students' normal thoughts, words, and movements as dangerous — and potentially involving law enforcement. As a former teacher in a 99 percent Black, low-income neighborhood, I am terrified for my former students whose natural speech patterns or movements were often wrongfully perceived as problematic by those unfamiliar with the community."[95]

In turns out, these fears are not unfounded. Upon examination, "natural language processing algorithms have been shown to be worse at recognizing and categorizing African American dialects of English. And popular tools used to screen online comments for hate speech and cyberbullying tend to disproportionately flag posts from African Americans."[96] Furthermore, in a survey released by the Center for Democracy and Technology, "78% of teachers reported that digital monitoring tools were used to discipline students [while] Black and Hispanic students reported being far more likely than white students to get into trouble because of online monitoring."[97]

Where schools use facial recognition technology, its well-documented shortcomings[98] when it comes to accurately identifying faces of color can also lead to Black and Brown students and their family members being misidentified as having engaged in wrongdoing or being on a list of persons excluded from school grounds. The resulting harms could range from humiliation to criminal arrest.

Ultimately, the EdTech Surveillance industry's tools are likely to make an already harmful and inequitable school disciplinary environment for students of color even worse. And all this comes at the cost of other interventions that may have proven helpful to students of color and students at large. As summarized by the Brennan Center, "While none of these [student surveillance] methods have been proven to be effective in deterring violence, similar systems have resulted in diverting resources away from enrichment opportunities, policing school communities to a point where students feel afraid to express themselves, and placing especially dangerous targets on students of color who are already disproportionately mislabeled and punished."[99] Put simply, for many students of color, and especially Black and Brown students, surveillance creates danger, it does not alleviate it.

Students with Disabilities

As with students of color, students with disabilities[100] already face a school climate that subjects them to higher levels of discipline. In fact, U.S. Department of Education's data from all U.S. states, districts, and territories found that students with disabilities were overrepresented in in-school suspensions, out-of-school suspensions, and expulsions, with Black and Indigenous students with disabilities facing even greater rates of school discipline.[101] And as with students of color, "automated surveillance is likely to have severe impacts for students with disabilities, who already face disproportionately high rates of school discipline and surveillance" especially because many of them "may need access to specific assistive and adaptive technology for their education."[102]

Indeed, the Department of Education (DOE) recently cautioned in guidance that schools' federal nondiscrimination obligations under Section 504 of the Rehabilitation Act extend to companies that provide security or surveillance technologies.[103] Specifically, the DOE noted that a "school's responsibility not to discriminate against students with disabilities applies to the conduct of everyone with whom the school has a contractual or other arrangement, such as [...] private security companies or other contractors" and that "schools cannot divest themselves of their nondiscrimination duty by relying on ... personnel [that] operate under a contract or other arrangement."[104]

It is also important to note that students with disabilities and their families tend to feel more privacy protective than those without disabilities. As a November 2022 briefing by the Center for Democracy and Technology observed, "Across several dimensions, students with disabilities, their parents, and their teachers demonstrate higher regard than their peers for protecting student data and preserving privacy. Sixty-eight percent of parents whose children use Individualized Education Programs (IEPs), or 504 plans report being concerned about the privacy and security of their child's school data, compared to 58% of parents of students who don't use these programs. The difference in teacher groups is even more striking: Fifty-one percent of teachers of students with disabilities but only 34% of general education teachers report being worried about privacy and security issues.'[105]

An opinion piece written by neurodivergent authors Evan Enzer and Sarah Roth, expressed a palpable frustration with student surveillance technologies:

> Rather than being some magic crystal ball, the [student surveillance technology] algorithms used by schools represent little more than bias in a box. These algorithms crudely decide who is and is not 'normal,' punishing students simply because their brains act differently. ... Today, schools across the country increasingly turn to techno-solutionist tools that harm students with invisible disabilities. Crude risk assessment tools mistake neurodivergence as a harm to ourselves and others. ... For nearly every one of us, neurodivergence is nothing to be concerned about, but school surveillance technology treats our differences as a threat. Much like the shame we felt when teachers singled us out, it hurts students when surveillance tech targets neurodivergence.[106]

Given that many student surveillance technologies, ranging from surveillance cameras to aggression detectors, are designed to flag behaviors that are "anomalous" or "out of the ordinary" or appear, without context, to signal a threat, it is not surprising that "disabled students are more likely to be flagged as potentially suspicious ... simply because of the ways disabled people already exist."[107]

Remote monitoring and automated proctoring surveillance technologies have been singled out as particularly threatening because they frequently "flag students for cheating when they look away from their screens or make other 'suspicious' movements. This harbors real danger for people with disabilities. The vocal and facial expressions of a student with a disability may differ from the [nondisabled person's] baseline that a software program compares the student to — mislabeling their affect and singling them out for discipline. In many cases, remote proctoring programs do not even try to accommodate disabilities — denying test-takers bathroom breaks, time away from their computer screen, scratch paper, and dictation software. This exacerbates disabilities, causes stress, and forces test takers to rush through the most important tests of their lives."[108]

Another problematic technology for disabled students is social media monitoring, which "evaluate[s] posts about mental health and penalize[s] students who need psychological evaluations as part of their individualized learning assessment."[109] The end result is this "monitoring drives neurodivergent students into the shadows, deterring them from sharing their feelings, degrading their mental health, and reducing their willingness to seek help."[110]

Overall, the very existence of student surveillance technologies by schools can make getting an education even more challenging for certain disabled students, as "the mere presence of the technology can cause or exacerbate anxiety, which is itself a disability."[111]

Privacy experts have long understood that, for students with disabilities, "the introduction of new kinds of surveillance may be especially harmful."[112] Accordingly, it is hard to justify any school district decision to increase the disproportionate educational challenges and discipline already faced by students with disabilities — especially when the justification for doing so is the deployment of surveillance technologies whose efficacy is questionable at best.

LGBTQ+ and Nonbinary Students

LGBTQ+ (lesbian, gay, bisexual, transgender, and queer) and nonbinary students are a particularly vulnerable when it comes to student surveillance technology. The youth find online spaces more affirming than offline spaces and are more likely to seek out help and information online than their non-LGBTQ+ peers.[113] LGBTQ+ and nonbinary students rely more on internet-based tools for community, communication, and information, and as such, they are more likely to be targeted by student surveillance technologies. As a groundbreaking 2022 report by the Center for Democracy and Technology (CDT), entitled “Hidden Harms: Targeting LGBTQ+ Students,” explained,

> LGBTQ+ students are increasingly being targeted by novel policies and practices that threaten their privacy in schools, and monitoring student activity online is no exception. In fact, algorithms that scan students’ messages, documents, and websites visited may include search terms like ‘gay’ and ‘lesbian.’ Although the stated purpose for targeting LGBTQ+ students with online monitoring efforts is to keep them safe, recent research from CDT suggests that they are being harmed instead.[114]

ACLU’s own polling found that among a national representative sample of students, more than 1 in 10 (13%) expressed concern that school surveillance could be used to “out” LGBTQ+ youth This fear is borne out in CDT’s survey, with nearly 1 in 3 LGBTQ+ students reporting that they or someone they knew had been “outed” as a result of their school’s digital activity monitoring through companies such as GoGuardian, Gaggle, Securly and Bark.[115]

This very much runs counter to the EdTech Surveillance industry’s marketing narrative that its products protect youth. In a clumsy and transparent attempt to buttress itself against criticisms from the LGBTQ+ community, one EdTech Surveillance company, Gaggle, tried to buy the support of an LGBTQ+ organization to support its marketing narrative with a $25,000 donation to The Trevor Project, a prominent LGBTQ+ youth mental health nonprofit. The attempt backfired catastrophically, with a public outcry and an almost immediate return of the donation accompanied by a state of concern about negative effects of companies like Gaggle on LGBTQ+ youth.[116]

Potential damage of school surveillance technologies to LGBTQ+ youth extends to discriminatory discipline and greater involvement in the school-to-prison pipeline, something which LGBTQ+ youth are already subject to at higher rates,[117] particularly LGBTQ+ youth with disabilities and Black and Brown LGBTQ+ youth.[118] Data from CDT’s survey indicates surveillance technology is more likely to result in experiences that funnel LGBTQ+ youth into the school-to-prison pipeline, such as being disciplined at school and being contacted by law enforcement for criminal investigation — with 31% of LGBTQ+ students reporting they or someone they knew had been contacted about possibly committing a crime, compared to 19% of non-LGBTQ+ students.[119]

Undocumented Students and Students with Undocumented Family Members

There are over half a million undocumented children attending K-12 schools and over 3 million students with an undocumented parent.[120] The potential risks of surveillance to these students is dire because, for them, surveillance technologies may result in literal removal from the home or separation from their families.[121] Broader student bodies are aware of these potential risks, with almost 1 in 5 (18%) students in our national survey expressing concern that school surveillance could be used against immigrant students, particularly those who are undocumented.

For undocumented students, the constant surveillance of what they communicate to their peers, post online, research on their computers, and even their actions at home and at school might reveal a misstep that begins with discipline and ends with deportation. This threat exists because these “students are drawn into the dragnet of immigration authorities and face the threat of deportation as a result of zero tolerance discipline and policing practices in schools.”[122]

For students who are lawfully in the United States, but who have an undocumented parent or other relative at home, the surveillance associated with remote learning may present an intolerable level of risk. Any teacher or school official who may not have supportive views towards undocumented persons, upon spotting an unfamiliar or “suspicious” relative on camera, could report that person to immigration authorities, producing devastating consequences for the student and their family. For such students, surveillance technology provides the complete opposite of safety — it is an ongoing and serious threat to the well-being of the people they love.

But the harm student surveillance can cause to undocumented students and students with undocumented family members is not limited to deportation. The mere existence and use of student surveillance technologies, “can cause severe anxiety in immigrant students, which often results in decline in academic performance. This fear can ripple throughout the school community and can create a climate of fear that is not suitable for learning for any student."[123]

Low-Income Students

There is little disagreement that low-income students are a vulnerable group that must confront numerous, easily quantifiable disadvantages in school. For example, DoSomething.org reports[124] that: (1) Children living in poverty have a higher rate of absenteeism or leave school all together because they are more likely to have to work or care for family members;[125] (2) 40% of children living in poverty are not prepared for primary schooling;[126] (3) children that live below the poverty line are 1.3 times more likely to have developmental delays or learning disabilities than those who do not live in poverty;[127] (4) by the end of fourth grade, low-income students are already two years behind grade level. By the time they reach the 12th grade, they are four years behind;[128] and (5) less than 30% of students in the bottom quarter of incomes enroll in a four-year college. Among that group – less than 50% graduate.[129] To that list, one can add that low-income students are more likely to be subjected to student surveillance technologies.

The reason low-income students are subjected to greater surveillance is explained by what is commonly referred to as the "digital divide," which is the technological gap between those who can afford access to better quality, more privacy-protective technologies and those that cannot. In the case of student surveillance, this digital divide occurs because:

> Low-income students are likely to need school-issued computers for homework more than higher-income students; they are thus more likely to bear the brunt of surveillance policies that facilitate a school's ability to reach into a student's home. While one might suggest that a possible remedy is for the student to use her own device rather than the device issued by the school, such a response ignores the reality that many low-income students cannot afford the technology on which schools increasingly rely.[130]

The EdTech Surveillance industry is focused, first and foremost, on making money, not on student safety — a fact school districts would be well advised to remember.

other words, schools often load student surveillance technologies, from content monitoring software to remote video/audio access tools, onto computers they lend to students via "one-to-one" technology sharing programs.[131] Low-income students who cannot afford to buy their own computers are then forced to choose between protecting their privacy and getting an education; clearly, that is not a real choice. Where school districts make surveillance a practical prerequisite for low-income students to have the tools they need to learn, those students are essentially forced to accept it, along with the greater rates of fear and discipline that come with belonging to a highly surveilled group.

Opportunity Costs: What Students — and Schools — Lose by Investing in the Wrong Tools

To get school districts on board, EdTech Surveillance companies often point to the availability of federal and state funds to reduce or zero out the cost of their products. However, they consistently fail to note the multitude of ways these funds could be used on other safety and educational interventions that have proven benefits.[132] This, of course, is predictable and understandable given that the EdTech Surveillance industry is focused, first and foremost, on making money, not on student safety — a fact school districts would be well advised to remember.

For example, when the Lockport, New York, school district "paid for its five-year, $1.4 million Aegis [facial recognition] license using public funds allocated through the [New York State] Smart Schools Bond Act," it chose to dedicate those funds, which were generally "available for educational technology,"[133] to a faulty, privacy-undermining surveillance technology whose safety benefits for schools are speculative at best. As local Lockport parent Jim Schultz wrote, "While high-technology security is among the allowed expenditures under the Smart Schools Bond Act, it's doubtful that facial-recognition technology is what voters had in mind. Neighboring districts invested their money in iPads and faster internet, while we bought spy cameras."[134]

As Johns Hopkins University pointed out in its report, the EdTech Surveillance industry's marketing has influenced school districts to make unwise decisions that often sacrifice proven interventions for its more highly marketed ones: "A perception of particular interest to this study is the apparent belief that technology is needed to address school safety. And yet, the presence of adult supervision in hallways, rather than high-visibility technology, was identified as effective in reducing peer victimization by 26% according to one study."[135]

Another example of the opportunity cost of school districts reflexively choosing student surveillance technology interventions over better available options comes from University of North Carolina law professor Barbara Fedders, who points out that "while detection and prevention of potential student self-harm are critical functions, Gaggle may not be the best way to achieve them. Much of the administration of Gaggle and similar tools is left to school Information Technology Specialists, who have neither the training nor institutional capacity to know how to evaluate and respond to students who present with mental health problems."[136]

According to ACLU student focus groups, the safety and support interventions most preferred by students seem to be losing out to the ones they favor the least. Specifically, when asked what would help make them feel safer at school, students pushed for policies and practices that would foster belonging and emotional safety. Students suggested, "I think if we can introduce emotional intelligence as a full-time class ... about how to handle certain things as it relates to people better, how to feel good about ourselves," and "[they could] curb on racial discrimination, discrimination of any kind, I believe that we should all be taught love and tolerance."

Many students pushed back against the methods they felt criminalized students and instead recommended efforts that promote trust, respect, and belonging. As one student in our focus groups noted, "if we put [students] in an environment where we trust them, and you know, [if] we provide them with a safe and welcoming environment, then they're more likely ... to result in better grades and result in even like better attitudes."

Less often, but no less emphatically, students in our focus groups also spoke about measures for physical safety, such as well-organized safety drills and building security that could reassure students. Surveillance tools were rarely cited as contributing to safety.

To date, the massive marketing efforts of the EdTech Surveillance industry have largely turned the opportunity costs of acquiring and using student surveillance technologies into an afterthought.[137] It is no wonder that alternative options with the fraction of the Ed Tech Surveillance industry's marketing budget — like hallway monitors, mental health counselors, or manufacturers of hardened, interior-locking classroom doors — have not stood a chance.

Of course, with better informed decision-making, that can change.

Efforts to Push Back Against Student Surveillance

“There can be a tendency to grab the latest technology and make it appear that you are doing something really protective and very innovative. We really have to take a step back and look at it and say: What benefit are we getting out of this? And what’s the cost?” - Brian Casey, the technology director at the Stevens Point Area Public School District in Wisconsin”[138]

Concerns about EdTech Surveillance have been raised by a diverse cross section of stakeholders. From local students and parents to educators, IT staff, United States senators, and even the White House, their collective voice is cautionary and concerned.

In an October 2021 letter to four leading EdTech Surveillance companies — Gaggle, Bark, GoGuardian, and Securly — United States senators Elizabeth Warren, Edward Markey, and Richard Blumenthal expressed concerns about relying on student surveillance technologies to protect students, writing, “It is crucial that the tools school districts select will keep students safe while also protecting their privacy, and that they do not exacerbate racial inequities and other unintended harms.”[139]

Writing in its Blueprint for an AI Bill of Rights in October 2022, the White House Office of Science and Technology Policy steadfastly warned that “Continuous surveillance and monitoring should not be used in education ... where the use of such surveillance technologies is likely to limit rights, opportunities, or access.”[140]

On the state level, an increasing number of efforts to push back against the runaway adoption of student surveillance technologies and the degradation of student privacy provides some cause for optimism. In 2022, after seven years of tireless advocacy by ACLU-MN and key partners, including Education Minnesota, Youthprise, and the Student Data Privacy Project, Minnesota passed the “Student Data Privacy Act.” This law prohibits schools and tech providers from using school laptops or tablets to monitor students or families.[141] Communities across the country are also working to ensure student privacy and combat the increasing criminalization of schools (See spotlights on New Jersey, New York, Rhode Island, and Southern California).

SPOTLIGHT ON NEW JERSEY

Investigating and Combatting a Growing Student Surveillance Ecosystem

Last year, reporters discovered that a facial recognition camera company had enlisted the help of a local school superintendent to win lucrative contracts across New Jersey's 336 school districts.[142] The superintendent essentially became an ambassador for the surveillance vendor, working with the company to generate sales leads and guiding school districts through the process of getting state funding to pay for the expensive surveillance tools.

This incident revealed how little is understood about the ecosystem that promotes school surveillance tools in New Jersey. The ACLU of New Jersey partnered with Encode Justice — a youth-led coalition of activists leading the fight against unjust facial recognition tech use — to investigate just how much school surveillance technologies have impacted the lives of students in New Jersey.

The investigation revealed a major red flag: New Jersey schools are spending millions of taxpayer dollars on unproven surveillance technologies that can harm the well-being of our students, particularly students of color and LGBTQ+ students.[143]

Tracking the security practices of schools is difficult in a state like New Jersey, where control of school districts is largely devolved to 697 local education agencies. ACLU of New Jersey and Encode Justice's investigation is still ongoing, but already we have uncovered concerning patterns and practices. In one school district, it was discovered that alerts from the district's communications surveillance software would, in some cases, go directly to the local police department, raising significant concerns about the role of law enforcement in schools.

Some communities in New Jersey are beginning to ask essential questions about the spying tools being used in their kids' schools. Students and parents in Montclair, New Jersey, stopped using the online monitoring platform GoGuardian after swift backlash from parents who were rightly concerned about how the tracking impacted their children's privacy.[144] The same concerns stopped the roll out of a similar monitoring program in the South Orange-Maplewood School District.

Community discussions — and the questions that come out of them — must be a key part of the districts' vetting process for any surveillance tool *before* they are acquired. New Jersey students' privacy should not be an afterthought.

SPOTLIGHT ON NEW YORK

Fighting Facial Recognition Technology in Schools Through Litigation, Advocacy, and Legislation

For the past five years, the ACLU of New York (NYCLU) has fought to prevent New York schools from using facial recognition technology. NYCLU has pushed back on the use of this harmful and discriminatory technology in the courts, in community town hall meetings, in school board and agency meetings, and in the legislature.

In 2014, New York state voters approved the Smart Schools Bond Act, authorizing $2 billion for school districts to upgrade their infrastructure and technology to “improve learning and opportunity for students throughout” New York.[145] Most districts used these funds to improve internet connectivity or buy computers, tablets, and 3D printers for their classrooms. But where educators saw opportunity, the EdTech Surveillance industry saw dollar signs. These companies viewed the public funds as a lucrative business opportunity, telling shareholders how they planned to convince districts to buy facial recognition and other invasive technologies.

In spring 2018, NYCLU was notified by concerned community members that the Lockport City School District, a suburban district outside Buffalo, had wasted almost all the $4 million it was awarded by the state on surveillance cameras, facial and object recognition software, and related hardware.[146] Lockport officials — who were advised by a “school safety consultant” with links to the EdTech Surveillance company that sold the facial recognition technology — kept the purchase secret from their constituents.

Lockport is neither a wealthy school district, nor a dangerous one. In recent budget years, the district considered drastic cost-saving measures including canceling full-day kindergarten programs. Yet school board members became laser focused on being the first district in the state to implement this biased and faulty technology, going so far as to tout how helpful it would be in the trivial task of keeping suspended students out of school.

NYCLU repeatedly contacted the New York State Educations Department (NYSED) with concerns over issues of accuracy, bias, privacy, transparency, and data security with Lockport’s facial recognition system. After months of urging, the department looked into the district and required it to undertake a privacy assessment. They also reviewed Lockport’s draft privacy policies, and even banned Lockport from testing its face recognition system multiple times.[147] During the course of the public battle, Lockport community members were extremely vocal in their opposition to the high-tech surveillance system. As one parent told Vice News: “The risk of an accident, the risk of something horrible happening because the system is structured the way it is, to me, is one million times higher than [the chance] that the cameras are going to prevent a real situation.”[148]

Despite the pushback, in November 2019, NYSED granted Lockport permission to deploy its biometric surveillance system in schools, despite a multitude of unanswered questions about the system’s functionality and the very serious risks for the more than 4,000 students in the district. In June 2020, NYCLU, on behalf of four parents, sued NYSED over its approval of Lockport’s surveillance system.[149]

Shortly after, the New York state Legislature passed the first statewide law in the country prohibiting the use of biometric identifying technology in in all elementary and secondary schools until the Office of Information Technology Services (OITS), in partnership with NYSED, issued a report on the risks and benefits of this technology in schools. The moratorium will remain in effect until and if the commissioner of education authorizes the use of biometric identifying technology following the report.[150] The law mandates that OITS consider the privacy implications of collecting, storing and/or sharing the biometric information of everyone who enters school grounds, including children; the impact of this technology on civil liberties, civil rights, and privacy; and the risks of false identifications and whether they differ among demographic groups. The study must also examine the risk of hacking, the cost of the systems, and any connections between the technology and law enforcement. This law was a direct response to Lockport's purchase and concerns over the racial disparities in identification of people of color, risks of data breaches, and access to the highly sensitive data produced by the system.

OITS issued its report on August 7, 2023, declaring that the risks of using facial recognition technology in an educational setting may outweigh its benefits, and Lockport City School District pledged not to use their facial recognition system. Now, NYCLU is focused on getting NYSED to institute a ban on the use of facial recognition in all New York schools. The children of New York deserve better than to be treated as guinea pigs for inaccurate, biased, invasive, and expensive facial recognition technology.

Breaking News: On September 27, 2023, the Commissioner of the New York State Education Department issued an order banning the purchase or use of facial recognition technology in New York's schools. This landmark prohibition recognizes that the harms of this invasive, inaccurate, and biased technology outweigh its benefits. We hope that New York's ban on facial recognition in schools is the first of many across the country.

SPOTLIGHT ON RHODE ISLAND

Bringing Attention and Solutions to a State's Lack of Student Privacy Protections

When school districts in Rhode Island commenced an effort to rapidly disburse school-loaned technologies to students, the ACLU of Rhode Island began to investigate and express concerns about the lack of privacy protections students had available to them as they used these devices. Specifically, it reviewed school district policies to see if and how they covered a few critical privacy-related subjects: Specifically, did the school policy indicate that students had any expectation of privacy in their use of the computers; did the school grant itself the unlimited ability to remotely or otherwise access the contents of the school-loaned devices; and did schools have the ability to access the school-loaned devices' cameras, microphones, or location services at any time for any reason.

In 2017, the ACLU of Rhode Island performed an initial and comprehensive review of these policies by sending open records requests to every school district in the state and found that all 22 of the districts who provided school-loaned devices to students offered no expectation of privacy, and a majority of them maintained the right to remotely access or inspect the devices for any reason.[151]

The onset of the COVID-19 pandemic and the ubiquitous turn to remote schooling prompted another investigation of these privacy issues. In April 2020, the ACLU of Rhode Island sent a letter to all superintendents in the state urging them to adopt comprehensive protections to assure students and their families that, during the tumultuous and sensitive circumstances of the pandemic, they would not have to fear their privacy being compromised by students' reliance on school-loaned devices and schools' increased remote access to student schoolwork and computers. This letter was followed by our release of another report investigating the state of student privacy in the midst of the pandemic.[152] Similar to their 2017 investigation, in 2019, the ACLU of Rhode Island found a majority of the state's 36 school districts were providing no meaningful privacy protections to students.

The ACLU of Rhode Island concluded that school districts' inconsistent patchwork of student privacy policies prompted a need for statewide legislation. To that end, it drafted and has been advocating, as a starting point, for legislation that would protect students from unjustified access to the microphones, cameras, and location services on their school-loaned devices. The ACLU of Rhode Island has garnered support for the bill from the Rhode Island School Superintendents Association. The legislation passed the Rhode Island House in both 2022 and 2023 but regretfully died in the Senate.

SPOTLIGHT ON SOUTHERN CALIFORNIA

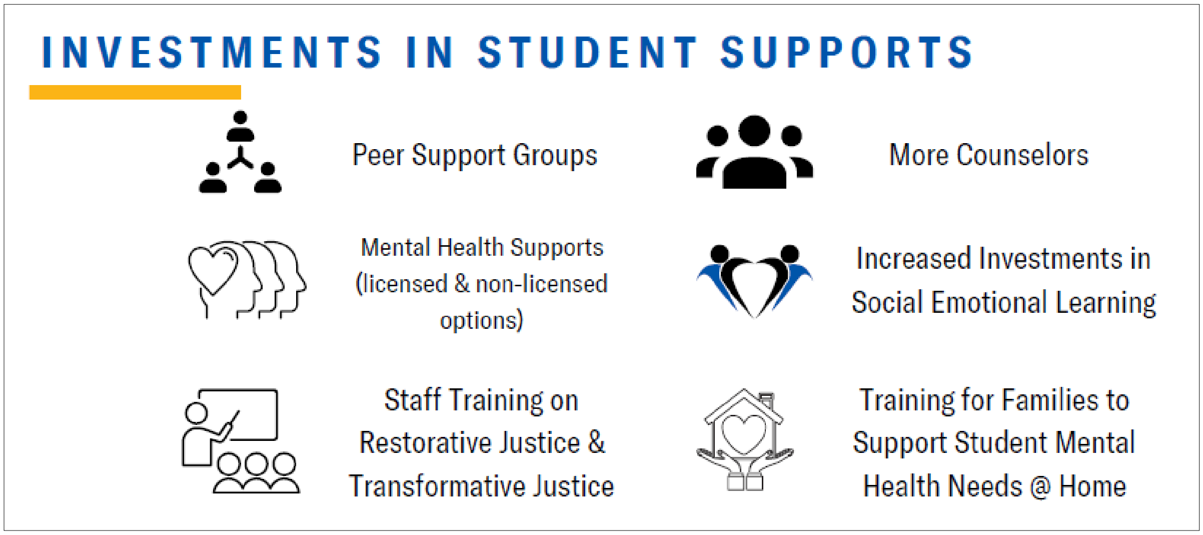
Advocating for Equity, Combatting Surveillance Technologies

ACLU of Southern California's (ACLU SoCal) Education Equity Project is committed to engaging in impactful advocacy, including for increased supports for students and to vastly increase funding to traditionally underserved school communities; to dismantle law enforcement and surveillance structures that shunt students of color and students with disabilities into the school-to-prison-pipeline; and to invest in alternative discipline structures in schools that lead to transformative justice rather than pushing students out.

In today's world where we are constantly connected to electronic devices, we find ourselves confronting a disturbing convergence: a *digitized* version of the school-to-prison pipeline. Across California, school districts have used, and sometimes misallocated, limited education funding, diverting it towards the creation of a surveillance infrastructure that invades student privacy, unnecessarily blocks student access to resources, and harmfully exposes students to contact with law enforcement.

For several years through our integrated advocacy approach, ACLU SoCal has worked in collaboration with community partners and other ACLU affiliates to combat the proliferation of surveillance technology in schools. We have advocated for policy changes at the local level, advocated for legislative protections that safeguard student' civil rights and civil liberties, discouraged school districts from deploying harmful surveillance technology, propounded several public records act requests to school districts to learn more about their surveillance technology, and educated students, families, and educators on the harms of surveillance technology and students' rights to digital privacy.

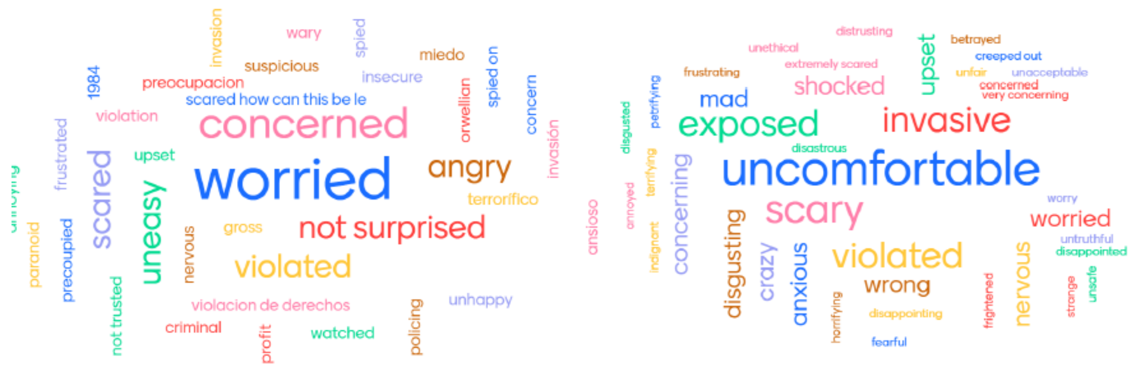
A central focus of our advocacy to combat the digitization of the school-to-prison pipeline is centered on online monitoring and filtering programs. These programs surveil students'



INVESTMENTS IN STUDENT SUPPORTS

- Peer Support Groups
- More Counselors
- Mental Health Supports (licensed & non-licensed options)
- Increased Investments in Social Emotional Learning
- Staff Training on Restorative Justice & Transformative Justice
- Training for Families to Support Student Mental Health Needs @ Home

STUDENTS' & PARENTS' REACTIONS TO SCHOOL SURVEILLANCE



online activity, including their school-based emails and instant messages, while a student is logged into their school-issued account or school-issued device. Upon detecting certain keywords or phrases, the program sends an alert to school administrators and, alarmingly in some cases, law enforcement or other agencies. This is a dangerous infrastructure, and one that is alarming to students and families. When we've surveyed students and parents during our "Know Your Rights" workshops, they share their deep concern and discomfort with these programs, highlighted in the following word clouds:

While students demand more mental health resources in schools, companies shamelessly market their online monitoring programs to school districts as tools for safeguarding student well-being and mental health. However, local advocates in various school districts wanted their leadership to stop investing in these programs and, instead, use education funding for mental health resources that foster trust between school staff and students, urging increased investments in trauma-informed and culturally competent counselors, school psychologists, social workers, and nurses, alongside peer-to-peer counseling programs. In one school district, for example, we worked with a family that sounded the alarm when its school district purchased an expensive contract with one such company called Gaggle. We and the ACLU of Northern California then reached out to community-based organizations in the school district, shared what we learned through our investigation that included information obtained through a Public Records Act request, and worked together with families and advocates to craft a community-based vision of what student well-being means. The following is an example of our public education tool that lists the community demands for alternatives to surveillance:

In another concerning example, students innocently conducting research for homework or playing video games on their school-issued computers were flagged by online monitoring software. Rather than addressing these flags by a simple inquiry by an educator to the student, the school staff escalated matters, subjecting students to interrogation by law enforcement, both on- and off-campus. In many of these situations, teachers or administrators did not directly communicate with the student but resorted to having police interrogate the student, despite the absence of an emergency or life-threatening situation. This egregious pattern is expanding the school-to-prison pipeline, facilitated by technology. Instead of supporting students through trained school staff, district staff resorted to criminalizing student behavior by involving police, criminalizing adolescent behavior, and causing great harm. Students reported feeling traumatized, criminalized, or distrustful of the adults meant to support their learning and development.

As students, parents, and advocates continue to rise against the digital arm of the school-to-prison pipeline, we will continue to stand with them. ACLU SoCal's Education Equity Project will continue to champion evidence-based measures that are rooted in building trusting relationships between students and school staff and improving school climate through our integrated advocacy approach.

Recommendations and Conclusions

How To Protect Students and Promote Better Student Surveillance Technology Decision-Making

Educate Others and Advocate for Reform

For those who care about protecting our students' privacy and promoting better student surveillance technology decision-making, our first recommendation, which may be the most important, is to help educate others about the suspect benefits and clear harms of student surveillance. Stressing the availability of such information will hopefully end decision-makers' and other community members' near exclusive reliance on self-serving information being provided to them by the EdTech Surveillance industry.

Such work can start by sharing this report[153] with as many school decision-makers and community members as you can (bonus points for including elected officials on the local, state, and federal level).

Key points to highlight:

- When considering the acquisition and use of student surveillance technologies, school policymakers, influencers, and other community members should not let fear drive their decision-making. While that may be understandably difficult, better decisions are made through the dispassionate examination of established facts.
- When learning about the alleged benefits of using student surveillance technologies, school policymakers, influencers, and other community members should not rely on unsubstantiated efficacy claims offered to them by EdTech Surveillance companies who have a financial interest in the sale of the technologies (including those that provided free technology but make money off its maintenance, data storage, or by selling related products or enhanced versions of their free product). Instead, insist on proof of efficacy from unbiased, fully independent sources that provide evidence, gathered in the education context, that has been peer-reviewed to ensure accuracy and reliability.
- School policymakers, influencers, and other community members should make it a top priority to learn about the harmful impacts of surveillance technologies on students and other school community members, including their heightened adverse impact on already vulnerable groups. They should talk to students and other school community members about how surveillance makes them feel, and they should also be mindful that "feeling safer" is very different from actually being safer (the former is more reflective the effectiveness of the EdTech Surveillance industry's marketing and press coverage than established facts).
- In weighing the actual, proven benefits of student surveillance technologies (they should not be surprised if they find none) against their harms, school policymakers, influencers, and other community members should never forget to think about opportunity costs. In other words, what other options to keep kids safe will we be forgoing to use student surveillance technologies? Do those alternatives have proven benefits? Are their proven benefits greater than those for student surveillance technologies? Do they have less unintended harms associated with them? Overall, do any alternative safety measures have a better cost-benefit ratio than the student surveillance technologies under consideration?

In the end, if the school policymakers, influencers, and other community members you engage adopt these suggestions, they will be much better informed and make wiser decisions when it comes to student surveillance technologies.

Adopt Best Practices for Decision-Making at Your School District Level

Hopefully, having reviewed the information provided in this report, school district officials and other school community members — including teachers, staff, families, and students — as well as their elected representatives will want to know what actions they can take to promote better decision-making when it comes to student surveillance technologies at the school district level.

Adopting a consistent approach to follow every time a school district considers the use of a student surveillance technology, which emphasizes well-informed decision-making that is based upon reliable, unbiased, verifiable information, will produce better outcomes for schools and their communities.

We advise adopting a school district policy that requires adherence to the following steps:

Step One: *Define the Precise Problem Your School District Is Seeking To Solve*

Too often, an ambiguous definition of the problem to be solved — such as "keep students safe" — can lead to the adoption of an intervention that is not well-tailored to provide the benefit being sought. To that end, the problem to be solved should be defined as specifically as possible. So, for example, choose "to safely and respectfully identify students in need of mental health interventions and to provide those interventions in a timely and supportive manner while respecting student privacy" over "keep students safe from themselves and others."

Step Two: *Evaluate a Student Surveillance Technology's Actual Benefits and Costs/Harms in Light of the Specific Problem To Be Solved*

This second step requires school districts to look beyond the EdTech Surveillance industry's biased marketing materials to answer the following questions:

- What are the proven, evidence-based benefits of the surveillance technology, if any, when it comes to addressing the specific problem to be solved? Beware of industry-produced or funded[154] studies that are designed to look independent but are not;
- What are the surveillance technology's financial costs? This includes their acquisition, operational, and maintenance costs, as well as related costs like data storage;
- What are the opportunity costs of investing in the surveillance technology? This means evaluating what alternative safety, health, and/or educational options must be forgone if resources are spent on a surveillance option; and
- What unintended harms might the use of the surveillance technology cause to students and other school community members that other interventions would not? This analysis should be conducted for your general student population

If the costs/harms of the student surveillance technology — including its opportunity costs — exceed its benefits, or where an alternative intervention has a better benefits-to-costs/harms ratio, the student surveillance intervention should be rejected.

as well as for any specific groups of vulnerable students who attend your school.

Step Three: *Seek Input from Your Entire School Community*

When you have completed the above two steps, share the information you learn, and your analysis of that information, with your school's community members and then solicit their input at a well-noticed public meeting in which everyone's opinions and ideas can be freely shared. The more perspectives your school district gains and the more communitywide problem solving it engages in, the better — and more inclusive — its decision-making is likely to be.

Step Four: *Conduct a Final Benefits Versus Costs/ Harms Analysis*

If after hearing from your school's community members, you are still considering using a student surveillance technology, it is time to undertake a benefits versus costs/harms analysis. Relying solely on the unbiased, evidence-based benefits, costs, and harms that have been established for the proposed student surveillance technology, your school district should determine if the technology's *proven* benefits outweigh its costs and harms in light of the specific problem your school district is seeking to address. If the costs/harms of the student surveillance technology — including its opportunity costs — exceed its benefits, or where an alternative intervention has a better benefits-to-costs/harms ratio, the student surveillance intervention should be rejected.

Pass State Legislation Requiring All Schools/ School District To Follow Best Practices for Student Surveillance Technology Decision-Making

For those who want to produce an even broader impact, rather than seeking to adopt best practices at just your school/school district, you can advocate for every school in your state to adopt these best practices. This should be a particularly appealing approach for state-level elected officials, and for persons and organizations with influence over state-level legislation and policy.

To facilitate the adoption of highly effective and consistent legislative standards, the ACLU drafted the "Student Surveillance Technology Acquisition Standards Act" model bill (see Appendix 2 for full text of the model bill).

It is important to note that the provided model legislation does *not* interfere with local school decision-making — it only seeks to ensure such decisions are well-informed, based on reliable information, and benefit from school community member input.

It should also be noted that, in our hyperpartisan times, keeping our children safe, wanting them to grow up free from the prying eyes of government surveillance, respecting personal privacy, and wanting our tax dollars to be spent wisely are all nonpartisan concepts. To continue the avoidance of partisanship, the efficacy standards contained in the model bill are borrowed from a recently adopted bipartisan federal law.

Passing the provided model legislation will not predetermine any results at the local school level, but it will ensure their decisions about the potential acquisition and use of student surveillance technologies are thoughtful, deliberative, and based on reliable, unbiased information.

Advocate Against the Use of Student Surveillance Technologies

The final point of recommended advocacy in this report is based upon a conclusion we are confident most if not all readers will eventually arrive at: that the benefits of student surveillance technologies, which are limited to nonexistent, are significantly outweighed by their near-certain significant harms — especially to already vulnerable groups of students — as well as by the opportunity costs of investing in such technologies.

Accordingly, our final point of recommended advocacy is to oppose your school district's use of invasive and harmful student surveillance technologies. At best, such technologies present a tangible, quick-to-implement intervention that creates the perception of improving student safety without actually moving us closer to that goal. In truth, the use of student surveillance technologies moves schools further away from that goal by harming students and supplanting measures that are more likely to have a positive impact on students' safety and well-being.

School Surveillance Doesn't Keep Students Safe

When it comes to student safety, better decisions come from better information and better decision-making processes. For too long, the marketing reach and power of the EdTech Surveillance industry — and school districts' lack of time and resources to question its marketing claims — have allowed pro-surveillance narratives to dominate the school safety discussion. While the ACLU believes students' and other school community members' civil rights and civil liberties are best protected by rejecting student surveillance technologies in favor of more supportive measures whose efficacy has been demonstrated by independent, reliable research, we also feel an exposure to honest, accurate information regarding the unproven benefits and certain harms of student surveillance make that case as well as we ever could.

To that end, if school districts commit to fully educating themselves and their communities before making decisions involving student safety and surveillance, and if they rely on proven facts from reliable sources that are not driven by those who have a financial interest in the outcome of their decisions, we trust America's schools and students will ultimately find themselves in a much better and safer place.

Methods

We use a multimethod approach in the development of this report, drawing on deep reviews of existing research and scholarship, investigation of EdTech industry products and practices, an audit of school shooting incidents, and original research through student polling and focus groups.

Research Review

We reviewed the published empirical research on educational technology used for school surveillance, including quantitative, qualitative, mixed-methods, and systematic reviews. Following an initial scoping review, we narrowed our focus to research in two main areas: the effects of school surveillance technologies, intended or unintended; 2) impact on and perspective of students, including those subgroups of students who might be at particular risk: students of color, students with disabilities, LGBTQ+ students, immigrant students, and students with immigrant families.

Research sources were identified through iterative searches of peer reviewed and legal articles, government publications, and organizational reports. In addition to targeted searches, we used citation tracing to identify potentially relevant sources. Additional news, legal, and commentary sources were also consulted, and these and other research sources are included in the report for context and informational purposes; the methods referenced here apply to these key areas of focus for the research review. However, the specific review of the research was limited to sources that met the research criteria.

Criteria for research review:

- Empirical research, quantitative, qualitative, and/or mixed method; including meta-analysis or systematic reviews.
- Addressed school surveillance technologies specifically (one or more). It may be that these technologies were included along with analog surveillance or school safety measures, e.g., school resource officers. In other cases, these surveillance technologies may be included in a study that also included educational technologies used for nonsurveillance purposes. As long as school surveillance technology was a substantives component of the research, it was also included in the review sample if surveillance technology was a substantive component of the research.
- K–12 school or school-age focus.
- We focused on U.S. context but did include studies from outside the U.S. when highly relevant or filling a gap in the U.S. literature.

Based on this criterion, 58 original research sources were included for this review.

Investigation of EdTech Industry Products and Practices

We conducted a comprehensive review of the products and practices of the EdTech Surveillance industry. Specifically, we collected and analyzed materials from: reputable journalistic sources; EdTech Surveillance company websites and available promotional materials; opinion pieces; advocacy organizations' websites, resources, and materials; and legal and scholarly research and papers.

Audit of Surveillance Tech in School Shooting Incidents

Our reviews of both the published research and the efficacy claims from the Ed Tech Surveillance industry, yielded little data on specific role of these technologies in curbing school violence. In order to supplement these reviews, we undertook an audit of select school shooting incidents, specifically to uncover if any of these schools had surveillance technologies in place prior to these incidents.

1. Database development: Records of school shooting incidents are maintained by a number of outlets, specifically: CNN, The Washington Post, Center for Homeland Defense and Security, Wikipedia, and School Shooting Database.[155] While having many similarities, each of these datasets was unique, and they varied from each other in number and type of incidents, criteria for inclusion, variables of interest, and ways in which variables were defined and operationalized. Datasets from each of these outlets incorporated both overlapping and distinct variables of interest. Thus, in order to create one comprehensive database on school shootings in the U.S., we merged these multiple databases into one master databases. The datasets were cleaned and merged in fall 2020. From that point on, we regularly maintained the database by adding new incidents as needed, up through August 2023. The final database includes 2,188 incidents from 1764-2023.

2. Case selection: Using this database, we selected our cases for review. Specifically, selecting cases based on the following criteria:

   - Time period: April 1999 (including and following the shootings at Columbine High School, Colorado) through April 2023, as of the drafting of this report.

   - Incidents: "Mass shootings" were defined as incidents with four or more student/faculty deaths since 1999 through drafting of this report (May 2023).

   - Setting: K-12 schools, i.e., elementary, middle, and/or high schools. Incidents at institutions of higher education institutions, i.e., colleges or universities, were excluded given this report focused on K-12 education systems.

   A total of 1,602 incidents met the time period criteria. Applying the remainder of the criteria resulted in 10 incidents occurring at: Columbine High School in Colorado (1999), the 2005 Red Lake High School in Minnesota (2005), West Nickel Mines School in Pennsylvania (2006), Sandy Hook Elementary School in Connecticut (2012), the 2014 shooting at Marysville Pilchuck High School in Washington (2014), the 2018 shooting at Marjory Stoneman Douglas High School in Florida (2018), Santa Fe High School in Texas (2018), Oxford High School in Mississippi (2021), Robb Elementary School in Texas (2022), and The Coventry School in Tennessee (2023).

3. Audit of Ed Tech Surveillance: In order to ascertain whether there were EdTech Surveillance products in use prior to or during these 10 incidents, we used several sources and approaches:

   - Review of incident information from our database: In some cases, our database already included information about types of security measures in place, i.e., metal detectors and security cameras;

   - Data from National Center for Educational Statistics Database;

   - Searches of publicly available information,[156] including media reports and documentation of public records requests from journalists;[157]

   - Existing list of EdTech Surveillance key providers and a nonexhaustive inventory of school districts that used the products, provided by NYCLU; and

   - All 10 schools were contacted by ACLU twice by phone and once by email July-August 2023. None of the schools responded.

National Survey

In order to better understand the perceptions and attitudes of the general population of high school students, the ACLU commissioned YouGov to conduct a national survey of adolescents as part of its US Youth Omnibus Survey. The survey was conducted using an online interview administered to members of the YouGov plc panel of individuals who have agreed to take part in surveys. For respondents who were 18 years old, emails emails were sent to panelists selected at random to be representative. The email invites them to take part in a survey and provides a generic survey link. Once a panel member clicks on the link they are sent to the survey that they are most required for, according to the sample definition and quotas.To reach students 14–17, panelists who have self-identified as parents were sent emails selected at random to be representative. Panelists who had children who would qualify to take the survey were then asked to have their child take the survey. Invitations to surveys don't expire, and respondents can be sent to any available survey. The responding sample is weighted to the profile of the sample definition to provide a representative reporting sample. The profile is normally derived from census data or, if not available from the census, from industry accepted data.

Total sample size was 502 youths from ages 14-18 years. The online survey was fielded between 20-26 October 2022. Data was weighted to be demographically representative of all U.S. youth (aged 14-18 years). Descriptive analyses and bivariate analyses assessing demographic group differences were conducted.

Focus Groups

We conducted 11 one-hour virtual focus groups with a total of 47 students in grades 9-12 from August 2021-August 2022. Participant consent and parental/guardian consent for minors was obtained. Students were eligible to participate in the focus groups if they were in grades 9-12 and not attending school in an exclusively remote/virtual learning environment.

Participants were recruited through 1) invitations to participants of the ALCU National Advocacy Institute in 2021 and 2022 — "aware students" and 2) outreach to potentially eligible participants by affiliates and youth-serving organizations — "general students." We conducted four focus groups with a total of 15 "aware" students, and seven focus groups with a total of 32 "general" students, resulting in a total of 11 focus groups and 47 student participants.

The focus group protocol was developed by the ACLU research team in consultation with the school surveillance tech project team, and informed by existing research, discussions with key scholars, and feedback from ACLU affiliate subject matter experts from ACLU, NYCLU, ACLU-PA, ACLU-RI, and ACLU-SoCal, The protocol examined three main domains: perceptions of school safety; knowledge and experiences with school surveillance, particularly EdTech Surveillance; and feelings about EdTech surveillance in schools.

All focus groups were moderated by two members of the research team, with one staff member serving as the moderator and the other serving as the notetaker. Focus groups took place via Zoom and were recorded. All data was securely stored, accessible only to study researchers and in accordance with ACLU's data privacy policies. All participants received a $25 gift card to food delivery service (i.e., UberEats).

Transcripts were cleaned and formatted for coding. We developed a codebook for qualitative coding based on the focus group protocol and study objectives. Transcripts were coded using qualitative analysis software, Inductive codes were based on focus group protocol and study objectives, inductive codes that emerged were also included in analyses. Coded excerpts were reviewed and summarized into key themes. Coding and analysis of "aware" groups and "general" groups were initially conducted separately. However, as the same themes arose with relatively the same frequency, the groups were combined for final analyses.

Appendix 1:
Ed Tech Surveillance: 10 Leading Products[158]

Surveillance Cameras

Providers Include	Aegis protective solutions, Avigilon (Motorola), Axis, Fusus, NetTalon, and Verkada
Capabilities	Provides schools with the ability to watch students via live video feeds and to capture video recordings, sometimes with accompanying audio. Some surveillance cameras allow police real-time access to school surveillance cameras, including the ability to control their operation and view their video feeds at any time.
Related Harms	(1) Students who know or believe they are being watched all the time may feel the need to avoid any behaviors or associations that may be unpopular, embarrassing, subject to misinterpretation, or which they do not want recorded. Lawful behaviors or associations likely to be deterred include those that are beneficial to students' education, social/emotional growth and well-being, and the exercise of their constitutional rights; (2) surveillance cameras erode school environments, implicitly labeling students as untrustworthy and potential criminals right as they are developing their identities; (3) surveillance cameras can create a security vulnerability, such as when an outside hacker gained access to the security cameras at several United Kingdom schools and live-streamed their video feeds online;[159] (4) the stated motive for acquiring surveillance cameras does not match up with how they are actually used. In truth, "rather than being used to stop school shootings, [surveillance] cameras are being used to identify students committing minor infractions of school rules."[160] While cameras with police integration provide police with real time access to school cameras, which may be of value during an ultrarare, active shooter situation, allowing the police to monitor schools full-time in the absence of an emergency does not benefit students, threatens to push at-risk students out of school, and worsens the existing school-to-prison pipeline for students of color, students with disabilities, and low-income students. We already have a name for a place where one's presence is compulsory and law enforcement watches over you 24/7: It is a jail, not a school.

Facial Recognition Surveillance

(commonly used in conjunction with surveillance cameras/footage)

Providers Include	Aegis, FaceFirst, Oosto (formerly AnyVision), SAFR (RealNetworks), SN Technologies, TriCorps/FacePRO (Panasonic), Visitor Aware, and Verkada.
Capabilities	Images captured by cameras are run against photo databases using AI to identify persons in the images. Captured images can be analyzed either in real time or after-the-fact by applying the technology to pictures and video recordings. The technology can be used to document and analyze the movements and interactions of every student, teacher, staff member, and school visitor.
Related Harms	(1) High potential for error and bias: Facial recognition technology is fallible and exhibits higher error rates when it comes to identifying people of color, women, and young persons,[161] meaning the chances of false identifications and discriminatory applications within a youthful K-12 school population is even greater than with the general public; (2) when students know or believe a technology is in use that can identify and track them wherever they go at school, and which can determine and create a record of every person they associate with, they may refrain from engaging in positive conduct. For example, the use of face surveillance in schools could deter students from vulnerable populations (such as LGBTQ+ and politically active students) from participating in related clubs and affinity groups. In some communities, the presence of this surveillance technology may even deter some students from associating with students from vulnerable groups, as doing so may be deemed too risky; (3) where schools capture the faceprints of students and other school community members but fail to vigorously protect the data, that sensitive information can end up in the hands of malevolent hackers.

Access Control

(via facial recognition technology)

Providers Include	Dormakaba and Visitor Aware
Capabilities	Frequently combines the use of still or video cameras with facial recognition technology to screen visitors to schools.
Related Harms	(1) Due to the shortcomings of facial recognition technology, this technology may exclude legitimate visitors (such as a parent coming for a teacher conference), a mistake that is more likely to be made when the visitor is a person of color. (2) Also, standards for exclusion, such as a database hit showing a parent was previously incarcerated or is undocumented may reveal private, irrelevant information and use it to discriminate or take other action against the visitor and embarrass, isolate, or otherwise harm the student.

Behavior Detection: Actuate, Artificial Intelligence (AI)-Driven

Providers Include	Avigilon, Axis, BriefCam (Cannon), and Verkada.
Capabilities	This technology[162] watches and analyzes video-subjects for behaviors it is either taught are problematic, or which it concludes, via self-learning, may be "anomalous." Upon the observation of such behavior, the technology will issue a notification to school officials.
Related Harms	(1) This unreliable technology can misinterpret or misunderstand certain student behaviors based on cultural, community, ability, or age differences, which could lead to interventions — from being pulled out of class for questioning to suspensions — for behaviors that are neither dangerous nor unlawful. This has been observed to be a particularly heightened risk for students of color and students with disabilities. By way of example, a student might lightly punch a friend in the arm as a greeting in the hallway, only to have AI interpret and flag that action as the commencement of an assault. The impact of such false notifications can be particularly problematic for overpoliced and overdisciplined student populations, such as students of color and disabled students. (2) Additionally, for certain student populations who may exhibit different traits and behaviors than a nondisabled student, like autistic students who already face challenges in school, such systems may flag disability-related behaviors as threatening even though they are not.

Social Media Monitoring Software

Providers Include	DigitalStakeout and Social Sentinel (Navigate360).
Capabilities	Scans students' public social media accounts for words and phrases that are designated by the school and/or the product provider to be problematic, even when they are off campus.[163] When the technology scans a concerning post, it notifies the provider and/or school.
Related Harms	(1) If students know or suspect their school is monitoring their social media posts, they may stop using such platforms to communicate with their peers, including online support/affinity groups for LGBTQ+ students or students with mental health challenges. Students may even stop trusting "private" groups and chats for communicating with their peers about sensitive subjects, such as how to access reproductive health resources.[164] (2) Such monitoring could exacerbate a student's mental health struggles if they find out their private communication was intercepted and shared with an unintended audience. (3) Words that have previously been used to trigger alerts when monitoring student communications have reflected the discriminatory biases of the technology provider or school, such as flagging words like "gay," "lesbian," and "queer,"[165] which could lead to a student being outed or targeted by persons with animus towards LGBTQ+ persons. (4) Social media surveillance companies use proprietary algorithms to digest and filter content, and these nontransparent algorithms can be biased. In one study, researchers at University of Massachusetts Amherst found a natural language processing algorithm coded African American vernacular English as Dutch with 99% confidence.[166] (5) Social media monitoring can lead a school to regulate and punish students for speech that has nothing to do with school safety but everything to do with free expression; for example, schools have run afoul of the First Amendment by policing students who express innocuous opinions about their community on their own time outside of the school environment, as the 2021 United States Supreme Court ruling in *Tinker v. Des Moines Independent Community School District* made clear.[167]

Student Communications Monitoring

Providers Include	Bark, Gaggle, Securly, and Social Sentinel (as part of Navigate360).
Capabilities	Scans private student electronic communications, such as emails and documents written on school accounts and software applications for words and phrases deemed by the technology provider and/or school to be problematic and shares concerning communications with the provider and/or school. While normally it is not constitutional to intercept private communications, that can change when students use school-provided equipment to communicate.
Related Harms	Monitoring students' communications, including emails and what they write in private documents using school provided resources, may chill the contemplation and discussion of unpopular or private subjects. Software vulnerabilities in certain student communications surveillance technologies have exposed student communications, webcams, and computers to hackers.[168]

Online Monitoring and Web Filtering

Providers Include	GoGuardian and Bark.
Capabilities	Monitors what students search for online and what websites they visit and flags concerning activities for the technology provider and/or school. Can block access to website content deemed by school to be inappropriate.
Related Harms	(1) Monitoring students' online activities may chill the use of the internet and internet-based tools for the research and contemplation of potentially unpopular or private subjects (e.g., sexual orientation, gender identity, locally unpopular political candidates and viewpoints, reproductive care resources, and mental health resources), even when such research and writing is part of an academic project. (2) Some schools have unlawfully weaponized web filtering tools to engage in viewpoint discrimination, such as a Missouri school which used the technology to block LGBTQ+ content.[169] (3) When students use school mandated education apps on their home computers, even in some cases after they are logged off the app, the monitoring continues and can scan and report the online activities of nonstudents in the same household.

Weapon Detection

Providers Include	Actuate, AnyVision, Evolv, Xtract One, SN Technologies, SoundThinking (formerly ShotSpotter), Virtual eForce, and ZeroEyes.
Capabilities	Claims to be able to analyze video from surveillance cameras to detect and warn schools about the presence of a weapon.[170]
Related Harms	False hits, such as mistaking a broomstick,[171] three-ring binder, or a Google Chromebook laptop[172] for a gun or other type of weapon, could result in an armed police response to a school. Sending police into a school with weapons drawn, thinking they are facing an armed student or potential active shooter, could have devastating and even life-threatening impacts on innocent students and school staff.

Gunshot Detection and Analytics

Providers Include	CLS Technology, Databuoy, and SoundThinking (formerly ShotSpotter)
Capabilities	Audio-based system which is used to detect and report gun shots (sometimes integrated with video).
Related Harms	The false detection of a gunshot — which could be triggered by something as innocuous as the sound of a dropped textbook or slammed door — could result in a traumatizing school lock down or even an armed police response to a school.[173] Again, sending police into a school thinking there is an active shooter could have life-threatening impacts. Even in the absence of an armed police response, these devices — which not surprisingly have been used more frequently in schools with greater numbers of Black and Brown students — bring an even greater police presence into schools in already overpoliced communities.[174] There is also a risk that the microphones may be repurposed into general listening and audio recording surveillance devices.

Remote Video Monitoring/Proctoring

(e.g., via laptop computer cameras) (including with "attention monitoring" capabilities)

Providers Include	ExamSoft, Gauge, GoGuardian, and Nestor Analytics.
Capabilities	Using the integrated video camera on students' computers, schools can monitor a student's attendance, focus, and compliance with anti-cheating rules.
Related Harms	Peering into students' homes is a particularly invasive and problematic form of surveillance that extends well beyond the school building. (1) Attendance taking efforts can produce false results if the facial recognition fails. (2) Students from very low-income homes, homes with domestic challenges or with undocumented occupants, students who live in homeless shelters, or unsheltered students who may be joining class from a McDonald's or Starbucks may all be ashamed or afraid to allow others to access their video cameras. (3) Neurodivergent students, such as those with attention-deficit/hyperactivity disorder (ADHD), may appear to not be focusing on their screen during class or repeatedly looking off camera during a test when such behavior is simply reflective of a disability or behavior that has nothing to do with academic integrity. Students with certain physical disabilities, such as those who require more time for bathroom breaks, might also be flagged for suspicious conduct. A federal court in Ohio recently found that such monitoring violates the Fourth Amendment's prohibitions against unreasonable searches,[175] but due to its limited geographic applicability, very few students are directly impacted by that ruling. In what is certainly a worst-case scenario, a teacher in Philadelphia suburb used this remote access technology to secretly activate a student's webcam and watch him while he was sleeping and partially undressed.[176]

Appendix 2
Model Legislation: Student Surveillance Technology Acquisition Standards Act

WHEREAS, the *[Name of Legislative Body]* finds that, over the past several years and especially since the onset of the COVID-19 pandemic, the acquisition and use of student surveillance technologies has grown exponentially;

WHEREAS, the *[Name of Legislative Body]* finds that, in response to numerous high-profile school shootings and other risks to students' health and well-being, parents, teachers, and administrators have prioritized efforts to improve student safety;

WHEREAS, the *[Name of Legislative Body]* finds that a growing number of well-financed companies are using massive promotional budgets to capitalize on these parents', teachers', and administrators' fears to promote the purchase of their student surveillance products;

WHEREAS, the *[Name of Legislative Body]* finds that these companies regularly make claims that their products deter violence and promote student safety without providing any reliable, independent, transparent data or studies that verify the accuracy of their claims;

WHEREAS, the *[Name of Legislative Body]* finds that the acquisition, use, and maintenance of student surveillance technologies and the data therefrom has significant opportunity costs; namely, it diverts financial and organizational resources away from other student safety interventions whose efficacy is better established;

WHEREAS, the *[Name of Legislative Body]* finds that all school community members — including parents, legal guardians, students, faculty, staff, and administrators — should have an opportunity to learn about student surveillance products, examine their efficacy or lack thereof, and consider the unintended, adverse consequences and opportunity costs of their use before limited school funds are expended to acquire and operate them;

WHEREAS, the *[Name of Legislative Body]* finds that some of the unintended adverse consequences of the use of student surveillance technologies include negatively impacting students' civil rights and liberties, privacy, academic freedom, and even safety, such technologies should not be used in the absence of clear evidence that their claimed benefits are real and that they substantially outweigh the harms such technologies can cause;

WHEREAS, the *[Name of Legislative Body]* finds that a uniform standard of evidence-based analysis should be established to help school districts and school community members arrive at well-informed opinions about whether a student surveillance technology should be acquired and used.

THEREFORE BE IT RESOLVED, that the *[Name of Legislative Body]* adopts the following:

SECTION 1. Definitions.

A. "Surveillance Technology" shall mean any digital device, system, hardware, or software that is capable of analyzing, capturing, collecting, intercepting, monitoring, processing, or recording audio, visual, digital, location, thermal, biometric, behavioral, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group.

   1. "Surveillance technology" shall not include any digital device, system, hardware, or software that only collects data that is directly related to the teaching and/or academic testing of students.

      a. For purpose of this subsection, a digital device, system, hardware, or software does not "only collect data that is directly related to the teaching and/or academic testing of students" if it:

         i. Uses biometrics to identify or track a student;

         ii. Monitors a student's movements, such as eye movements or keystroke tracking;

iii. Captures or monitors a student's location or surroundings;

iv. Captures words or terms entered by a student into an internet search engine;

v. Identifies websites visited by a student; or

vi. Intercepts or monitors any student communication that is not directed towards the student's school or an employee thereof, unless required by law.

vii. The above examples are an illustrative, non-exclusive list.

B. "Surveillance Data" shall mean any electronic data that is analyzed, captured, collected, intercepted, processed, recorded, retained, or shared by surveillance technology.

SECTION 2. Standards

A. Model Legislation: Student Surveillance Technology Acquisition Standards Act Consistent with the "School Safety Evidence-based Practices" standard contained in the federal Bipartisan Safer Communities Act, Public Law 117–159 (June 25, 2022), Subtitle C, Sec. 2220D(b)(2)(B), no school or school district shall be permitted to acquire, borrow, install, or use a surveillance technology or surveillance data unless the technology "has been shown to have a significant effect on improving the health, safety, and welfare of persons in school settings."

1. Consistent with the federal Bipartisan Safer Communities Act, Sec. 2220D(b)(2)(B)(i), proof of such efficacy must be established through independent, peer-reviewed, published, "relevant research that is evidence-based, as defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801), supporting the evidence-based practice or recommendation."

B. In determining if the acquisition and use of a school surveillance technology is in the best interest of a school's students and other relevant community members, a school or school district should investigate and consider any unintended harms or other consequences that might accompany the use of such a technology, as well as the opportunity costs of electing to acquire and use such a technology.

SECTION 3. School Community Member Engagement

A. Prior to acquiring, borrowing, installing, or utilizing a student surveillance technology or surveillance data, or renewing a contract for the same whose prior approval did not comply with the provisions of this Act, the school or school district shall present its rationale for wanting to acquire, borrow, install, or utilize a student surveillance technology or surveillance data, and the evidence-based research establishing it meets the efficacy standards set forth in Section 2, along with any available evidence-based research to the contrary of which the school or school district is aware, to the school's or school district's community of parents, legal guardians, students, faculty, staff, administrators, and other relevant community members.

B. The presentation of the information required in Section 3(A) of this Act shall be provided:

1. At least 14 days in advance of a well-noticed public hearing in which all school community members are given a reasonable opportunity to ask questions and present their views, both orally and in writing, before the school or school district officials who are authorized to make the final determination regarding the acquisition, borrowing, installation, or use of the student surveillance technology or surveillance data under consideration; and

2. At least 28 days before any vote or other final determination is made by the school or school district with respect to the acquisition, borrowing, installation, or use of the student surveillance technology or surveillance data under consideration.

SECTION 4. Applicability

This law shall apply to all public schools in the State of (STATE NAME) as well as any other schools that receive funding from the State of (STATE NAME).

SECTION 5. Enforcement

Any violation of this Act constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or a writ of mandate in any court of competent jurisdiction to enforce this Act.

SECTION 6. Severability

The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person or circumstance, is held invalid, the remainder of this Act, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

SECTION 7. Effective Date

This Act shall take effect immediately upon adoption.

Endnotes

1 Natasha Singer, "Schools Are Spending Billions on High-Tech Defense for Mass Shootings," *New York Time*s (June 26, 2022),

2 Ibid.

3 Captured from https://www.bark.us/blog/bark-for-schools-free/) on September 27, 2023.

4 Captured from https://www.gaggle.net/safety-management on July 20, 2023.

5 Captured from https://www.nettalon.com/ on July 20, 2023.

6 A Comprehensive Report on School Safety Technology, Johns Hopkins University Applied Physics Laboratory (with The Johns Hopkins University School of Education, Division of Public Safety Leadership), October 2016. https://www.ojp.gov/pdffiles1/nij/grants/250274.pdf; Schwartz, Heather L., Rajeev Ramchand, Dionne Barnes-Proby, Sean Grant, Brian A. Jackson, Kristin J. Leuschner, Mauri Matsuda, and Jessica Saunders, The Role of Technology in Improving K–12 School Safety. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1488.html.

7 National Threat Assessment Center. (2021) *Averting Targeted School Violence: A. U.S. Secret Service Analysis of Plots Against Schools. U.S. Secret Service, Department of Homeland Security.* https://www.secretservice.gov/sites/default/files/reports/2021-03/USSS%20Averting%20Targeted%20School%20Violence.2021.03.pdf

8 U. S. Department of Education, Institute of Education, National Center for Education Statistics (NCES), *Digest of Education Statistics, 2021 Tables and Figures*, Table 214.30 (April, 2022), https://nces.ed.gov/programs/digest/d21/tables/dt21_214.30.asp?current=yes.

9 While this report frequently references "school districts," which is a term that encompasses K-12 regular public school districts and independent charter school districts, these issues are equally present and important for all K-12 schools, including private and parochial schools.

10 For example, compare https://www.goguardian.com/beacon ("A student safety solution built for K-12: Notify designated staff about online activity that indicates a risk of suicide, self-harm, or possible harm to others.") with https://www.goguardian.com/distance-learning ("Distance Learning Resource Center: During COVID-19 school closures, many districts are leaning into distance and remote learning to avoid interruption of their students' education. We've put together this page of resources to support your school's e-learning practice.").

11 Chad Marlow, "Those 'Free' Remote Learning Apps Have a High Cost: Your Student's Privacy," American Civil Liberties Union (ACLU) (2020), https://www.aclu.org/news/privacy-technology/those-free-remote-learning-apps-have-a-high-cost-your-students-privacy.

12 See discussion, *infra*.

13 Natasha Singer, "Schools Are Spending Billions on High-Tech Defense for Mass Shootings," *New York Times* (June 26, 2022), https://www.nytimes.com/2022/06/26/business/school-safety-technology.html.

14 Ke Wang, Jana Kemp, and Riley Burr, *Crime, Violence, Discipline, and Safety in U.S. Public Schools in 2019-20*, NCES, no. 2022-029 (July 2022), https://nces.ed.gov/pubs2022/2022029.pdf.

15 Amir Whitaker et al., "Cops and No Counselors: How the Lack of School Mental Health Staff Is Harming Students," ACLU (2019), https://www.aclu.org/wp-content/uploads/legal-documents/030419-acluschooldisciplinereport.pdf.

16 As with all advanced technologies, new surveillance technologies are constantly being developed, and those producing them join and leave the market regularly. Thus, this is not intended to be an exhaustive list of all types of student surveillance technologies in 2023, and it most certainly is not inclusive of all the companies currently providing or marketing these technologies.

17 This is particularly problematic given that the U.S. Supreme Court has held that schools are supposed to be limited in what they can do in response to off-campus student speech. See (20-255 Mahanoy Area School Dist. v. B. L. (06/23/2021) (supremecourt.gov)).

18 The claims appear to be dubious - See generally https://www.aclu.org/news/privacy-technology/are-gun-detectors-the-answer-to-mass-shootings

19 YouGov. School Surveillance, Fielded October 22-26, 2022. Commissioned by ACLU.

20 Johns Hopkins University Applied Physics Laboratory (with the Johns Hopkins University School of Education, Division of Public Safety Leadership), "A Comprehensive Report on School Safety Technology" (October 2016), https://www.ojp.gov/pdffiles1/nij/grants/250274.pdf.

21 Todd Feathers, "Schools Spy on Kids to Prevent Shootings, But There's No Evidence It Works," Vice (December 4, 2019), https://www.vice.com/en/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works; Barbara Fedders, "The Constant and Expanding Classroom: Surveillance in K-12 Public Schools," *North Carolina Law Revue* 97, no. 6 (2019), 1673; https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=6749&context=nclr; and Mark Keierleber, "Inside the $3 Billion School Security Industry: Companies Market Sophisticated Technology to 'Harden' Campuses, but Will It Make Us Safe?" The 74 (August 9, 2018), https://www.the74million.org/article/inside-the-3-billion-school-security-industry-companies-market-sophisticated-technology-to-harden-campuses-but-will-it-make-us-safe/.

22 Keierleber, "Inside the $3 Billion School Security Industry"; and Heather L. Schwartz et al., *The Role of Technology in Improving K–12 School Safety* (Santa Monica, California: RAND Corporation, 2016), https://www.rand.org/pubs/research_reports/RR1488.html.

23 See Axis Communications, "Helping Schools Create Safer Learning Environments"; Avigilon, "Education Security Technology," https://www.avigilon.com/industry/education; and NetTalon, "Delivering the Safest Schools in America," https://www.nettalon.com/.

24 Frances Adams-O'Brien, "Is There Empirical Evidence that Surveillance Cameras Reduce Crime?," University of Tennessee,

Municipal Technical Advisory Service (MTAS), Institute for Public Service, MTAS Research and Information Center (September 26, 2016), https://www.mtas.tennessee.edu/knowledgebase/there-empirical-evidence-surveillance-cameras-reduce-crime; and David Greenberg and Jeffery Roush, "The Effectiveness of an Electronic Security Management System in a Privately Owned Apartment Complex, *Evaluation Review* 33, no. 1, February 2009, https://popcenter.asu.edu/sites/default/files/215_greenberg_roush_cctveffectiveness.pdf.

25 E. E. Tanner-Smith et al., "Adding Security, but Subtracting Safety? Exploring Schools' Use of Multiple Visible Security Measures," *American Journal of Criminal Justice* 43, no.1 (August 2, 2018),102–119, https://doi.org/1https://link.springer.com/article/10.1007/s12103-017-9409-30.1007/s12103-017-9409-3.

26 Benjamin W. Fisher, Ethan M. Higgins, and Emily M. Homer, "School Crime and Punishment and the Implementation of Security Cameras: Findings from a National Longitudinal Study," *Justice Quarterly* 38, no. 1 (2021), 22–46, https://www.tandfonline.com/doi/full/10.1080/07418825.2018.1518476.

27 "Mass shootings" were defined as shooting incidents on school grounds with four or more student or educator casualties (see Methods section of this report for further details about our school shooting incident audit).

28 Surveillance cameras were present at Columbine High School (Colorado, 1999), Red Lake High School (Minnesota, 2005), Sandy Hook School (Connecticut, 2012), Marjory Stoneman Douglas High School (Florida, 2018), Santa Fe High School (Texas, 2018), Oxford High School (Michigan, 2021), Robb Elementary School (Texas, 2022), and The Coventry School (Tennessee, 2023). They were not present at West Nickel Mines School (Pennsylvania, 2006) and Marysville Pilchuck High School (Washington, 2014).

29 Lina Alathari, "Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools," U.S. Department of Homeland Security, U.S. Secret Service, National Threat Assessment Center (2021), https://www.secretservice.gov/sites/default/files/reports/2021-03/USSS%20Averting%20Targeted%20School%20Violence.2021.03.pdf.

30 Robb Elementary, Uvalde Consolidated Independent School District in Texas, experienced a deadly shooting in 2022. During this time, the district also had a variety of up-to-date security measures including Raptor's Alert system and Social Sentinel monitoring. Jenni Lee, "How Central Texas School Districts Are Addressing Safety and Security Concerns," KVUE (August 15, 2022), https://www.kvue.com/article/news/investigations/defenders/uvalde-shooting-school-safety-policies-before-after/269-b697160e-3079-452a-81b8-410b4894771c; and Rachel Levinson-Waldman, "School Social Media Monitoring Won't Stop the Next Mass Shooting," Brennan Center for Justice (June 22, 2022), https://www.brennancenter.org/our-work/analysis-opinion/school-social-media-monitoring-wont-stop-next-mass-shooting.

31 Singer, "Schools Are Spending Billions."

32 Keierleber, "Inside the $3 Billion School Security Industry."

33 Ibid.

34 Gaggle, "Gaggle Safety Management," https://www.gaggle.net/safety-management (accessed July 20, 2023).

35 Ibid.

36 NetTalon, "Why Are Schools Either Vulnerable or Defenseless" (accessed July 20, 2023), https://www.nettalon.com/threat.

37 Keierleber, "Inside the $3 Billion School Security Industry."

38 Associated Press, "How Hard Is It to Win the Lottery? Odds to Keep in Mind as Powerball and Mega Millions Jackpots Soar" (July 19, 2023), https://apnews.com/article/powerball-mega-millions-winning-odds-numbers-a3e5a8e8e7ed15d7500c1d6acdab6785.

39 Keierleber, "Inside the $3 Billion School Security Industry."

40 Ibid.

41 Gaggle, "Gaggle Safety Management."

42 GoGuardian, "Youth Suicide Isn't Just an Issue—It's a National Crisis" (accessed July 20, 2023), https://www.goguardian.com/suicide-self-harm-resources.

43 Securly, "Identify At-risk Students and Intervene Early" (accessed July 20, 2023), https://www.securly.com/solutions/student-wellness?utm_term=&utm_source=adwords&utm_medium=ppc&utm_campaign=Securly_Rhtim_Search_26/04/2023.

44 Feathers, "Schools Spy on Kids."

45 Ibid.

46 Ibid.

47 Gaggle, "95% of Gaggle Educators Believe Gaggle Makes School Safer, According to New EdWeek Research Center Survey (October 26, 2022), https://www.gaggle.net/press/k-12-educators-believe-gaggle-makes-schools-safer#:˜:text=During%20the%202021%2D2022%20academic,planning%20or%20actively%20attempting%20suicide.

48 Feathers, "Schools Spy on Kids."

49 Charlie Warzel, "Welcome to the K-12 Surveillance State," *New York Times* (July 2, 2019), https://www.nytimes.com/2019/07/02/opinion/surveillance-state-schools.html.

50 Lois Becket, "Under Digital Surveillance: How American Schools Spy on Millions of Kids, *The Guardian* (October 22, 2019), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle#:˜:text=The%20amount%20American%20public%20school,contracts%20between%20just%20two%20major.

51 Wikipedia, "Syms Corporation," https://en.wikipedia.org/wiki/Syms_Corporation.

52 Gaggle, "Gaggle Safety Management."

53 Aggression detectors, one of the newer products being offered by the EdTech Surveillance industry, have been found to be completely unreliable. See Jack Gillum and Jeff Kao, "Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students," ProPublica (June 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/. They also raise significant civil liberties concerns and their use may, under certain states' laws, be illegal. See Jay Stanley,

"Firestorm over Green Bay City Hall Surveillance Microphones Is a Reminder of Country We Don't Want to Live In," ACLU (February 22, 2023), https://www.aclu.org/news/privacy-technology/firestorm-over-green-bay-city-hall-surveillance-microphones-is-a-reminder-of-country-we-dont-want-to-live-in.

54 NetTalon, "Delivering the Safest Schools in America" (accessed July 20, 2023), https://www.nettalon.com/.

55 Navigate360, "Detect District-owned Sources Scanning, Social Media Scanning and Web Filtering" (accessed July 21, 2023), https://navigate360.com/safety-solutions/detect/.

56 Corin Faife, "After Uvalde, Social Media Monitoring Apps Struggle to Justify Surveillance" (May 31, 2022), https://www.theverge.com/2022/5/31/23148541/digital-surveillance-school-shootings-social-sentinel-uvalde.

57 GoGuardian, Beacon, "A Student Safety Solution Built for K-12" (accessed July 21, 2023), https://www.goguardian.com/beacon.

58 Gaggle, "What Educators Think About Gaggle" (accessed July 21, 2023), https://news.gaggle.net/what-educators-think?hsCtaTracking=cd1c9dd8-91cc-444c-8e2b-ec3eec3354cf%7C70203cdf-e2a0-4c3a-81ee-33c77cf16e82.

59 Aaron Gordon, "When School Superintendents Market Surveillance Cameras," Vice (October 4, 2022), https://www.vice.com/en/article/93anj7/when-school-superintendents-market-surveillance-cameras.

60 Ibid.

61 The Educator's School Safety Network is a self-described "501(c)(3) not-for-profit organization dedicated to empowering educators with education-based school safety training and resources." See Educator's School Safety Network, "Dedicated Experts with Experience Across Disciplines," https://eschoolsafety.org/about.

62 Michele Caffre, "Spending on School Security Tops $3 Billion, With Focus on New Surveillance and Tech," EdWeek Market Brief (July 26, 2022), https://marketbrief.edweek.org/marketplace-k-12/spending-school-security-tops-3-billion-focus-new-surveillance-tech/#:˜:text=July%2026%2C%202022-,Spending%20on%20School%20Security%20Tops%20%243%20Billion%2C%20With,on%20New%20Surveillance%20and%20Tech.

63 Vice, "'They're Watching Us', Inside the Company Surveilling Millions of Students," YouTube, https://www.youtube.com/watch?v=o3YLpTWcclo.

64 Ibid.

65 Singer, "Schools Are Spending Billions."

66 See, e.g., Christine Dzou, "New Jersey Will Soon Award $500 Million in School Safety and Improvement Grants," https://www.verkada.com/blog/new-jersey-school-security-grants/.

67 As discussed further below, while the direct financial costs of student surveillance technology acquisition, when paid for by grants, may be low (assuming ongoing operational and maintenance cost are also paid for, which they often are not), the opportunity cost associated with such purchases, and the cost to students' civil right/liberties and academic freedom, are significant.

68 Gordon, "When School Superintendents Market Surveillance Cameras."

69 Charlotte Morabito, "The School Security Industry Is Valued at $3.1 Billion. Here's Why That May Not Be Enough," CNBC (July 6, 2022), https://www.cnbc.com/2022/07/06/the-school-security-industry-was-valued-at-3point1-billion-in-2021.html.

70 Elizabeth Laird et al., "Hidden Harms: The Misleading Promise of Monitoring Students Online," Center for Democracy and Technology (August 3, 2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/.

71 Michael Adorjan and Rosemary Ricciardelli, "Youth Responses to the Surveillance School: The Bifurcation of Antagonism and Confidence in Surveillance Among Teenage Students," *YOUNG* 27, no. 5 (February 21, 2019), 451–467, https://doi.org/10.1177/1103308818821206; Frida Alim et al., "Spying on Students: School-issued Devices and Student Privacy," Electronic Frontier Foundation (April 13, 2017), https://www.eff.org/files/2017/04/13/student-privacy-report.pdf; Michael Birnhack, Lotem Perry-Hazan, and Shiran German Ben-Hayun, "CCTV Surveillance in Primary Schools: Normalisation, Resistance, and Children's Privacy Consciousness," *Oxford Review of Education* 44, no. 2 (December 13, 2017), 204–220, https://doi.org/10.1080/03054985.2017.1386546; and Ahmed Eleyan and Anton Persson, *Student Perspectives on School Surveillance: An Explorative Study Using a Mobile Application Prototype* (master's thesis, Umeå University, 2019), http://www.diva-portal.org/smash/get/diva2:1329863/FULLTEXT01.pdf.

72 This dynamic was revealed in our focus group research as well as in Eleyan, *Student Perspectives on School Surveillance*.

73 Birnhack, "CCTV Surveillance."

74 Fedders, "The Constant and Expanding Classroom."

75 Ibid.

76 Chris Gilliard, "School Surveillance Will Never Protect Kids from Shootings," *Wired* (June 30, 2022), https://www.wired.com/story/school-surveillance-never-protect-kids-shootings/.

77 Feathers, "Schools Spy on Kids."

78 Fedders, "The Constant and Expanding Classroom."

79 Alim, "Spying on Students."

80 See. e.g., Jacob Dirnhuber, "HACK ATTACK: Hackers Attack UK School CCTV and Stream Live Footage of Students Online," *The Sun* (February 25, 2018), https://www.thesun.co.uk/news/5670211/hackers-attack-uk-school-cctv-stream-footage-pupils/ (hacker accesses school surveillance cameras in UK and places feeds online); Mark Keierleber, "Popular Student Monitoring Software Could Have Exposed Thousands to Attacks," *Fast Company* (October 18, 2021), https://www.fastcompany.com/90686770/netop-student-monitoring-software-hack (student surveillance tech used by hackers to install malware, ransomware, and gain access to student webcams); and Wikipedia, "*Robbins v. Lower Merion School District*," https://en.wikipedia.org/wiki/Robbins_v._Lower_Merion_School_District (teacher uses remote webcam technology to watch student undressing).

[81] Jay Stanley, “Does Surveillance Affect Us Even When We Can’t Confirm We’re Being Watched? Lessons From Behind the Iron Curtain,” ACLU (October 15, 2012), https://www.aclu.org/news/national-security/does-surveillance-affect-us-even-when-we-cant.

[82] Michael Birnhack and Lotem Perry-Hazan, “School Surveillance in Context: High School Students’ Perspectives on CCTV, Privacy, and Security,” *Youth and Society* 52, no.7 (May 27, 2020), 1312–1330, https://journals.sagepub.com/doi/full/10.1177/0044118X20916617; and Valerie Steeves, “Teaching in a Fishbowl: How Surveillance Is Reshaping the Networked Classroom. *Journal of Information Communication and Ethics in Society* 12, no. 4 (January 2016), 298-313, https://www.researchgate.net/publication/366977241_Teaching_in_a_Fishbowl_How_Surveillance_is_Reshaping_the_Networked_Classroom.

[83] Feathers, “Schools Spy on Kids.” See also, Office of U.S. Sen. Elizabeth Warren, “Warren, Markey, Blumenthal Raise Concerns About Discriminatory Bias in EdTech Student Surveillance Platforms and Harmful Effects on Students’ Mental Health,” Sen. Warren press release, October 4, 2021, https://www.warren.senate.gov/oversight/letters/warren-markey-blumenthal-raise-concerns-about-discriminatory-bias-in-edtech-student-surveillance-platforms-and-harmful-effects-on-students-mental-health.

[84] ACLU of Pennsylvania, “Fast Facts on School Safety: The Research,” End Zero Tolerance, https://www.endzerotolerance.org/fast-facts-on-school-safety.

[85] Fedders, “The Constant and Expanding Classroom.”

[86] YouGov. School Surveillance. On Behalf of ACLU. Field dates Oct 20-26, 2022.

[87] Lily Hay Newman, “The Surveillance State Is Primed for Criminalized Abortion,” WIRED (May 20, 2022), https://www.wired.com/story/surveillance-police-roe-v-wade-abortion/.

[88] Movement Advancement Project, “Equality Maps: Bans on Best Practice Medical Care for Transgender Youth,” https://www.mapresearch.org/equality-maps/healthcare/youth_medical_care_bans (accessed September 8, 2023).

[89] James Alan Fox, “As Students Head Back to School, Should Parents Worry About Shootings? The Math Says No,” *USA Today* (August 8, 2023), https://www.usatoday.com/story/opinion/2023/08/08/school-shootings-rare-parents-students-shouldnt-worry/70520793007/.

[90] Sarah Lindstrom Johnson et al., “Surveillance or Safekeeping? How School Security Officer and Camera Presence Influence Students’ Perceptions of Safety, Equity, and Support,” *Journal of Adolescent Health, 63,* no. 6 (September 6, 2018), 732–738, https://doi.org/10.1016/j.jadohealth.2018.06.008.

[91] Amir Whitaker et al., “Cops and No Counselors,” ACLU (2019), https://www.aclu.org/report/cops-and-no-counselors.

[92] U.S. Education Department, Office for Civil Rights, Civil Rights Data Collection (CRDC), *2017-18 State and National Estimations* (June 2021), https://ocrdata.ed.gov/estimations/2017-2018.

[93] Melinda Anderson, “When Schools Feel Like Prisons,” *The Atlantic* (September 12, 2016), https://www.theatlantic.com/education/archive/2016/09/when-school-feels-like-prison/499556/.

[94] Jason Nance, “Student Surveillance, Racial Inequalities, and Implicit Racial Bias,” *Emory Law Journal 66,* no. 4 (2017), 765–837, https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1093&context=elj.

[95] Priyam Madhukar, “The Hidden Costs of High-Tech Surveillance in Schools,” Brennan Center for Justice (October 17, 2019), https://www.brennancenter.org/our-work/analysis-opinion/hidden-costs-high-tech-surveillance-schools.

[96] Feathers, “Schools Spy on Kids.”

[97] Mark Keierleber, “Gaggle Drops LGBTQ Keywords from Student Surveillance Tool Following Bias Concerns,” The 74 (January 27, 2023), https://www.the74million.org/article/gaggle-drops-lgbtq-keywords-from-student-surveillance-tool-following-bias-concerns/.

[98] Alex Najibi, “Racial Discrimination in Face Recognition Technology,” Harvard University Graduate School of Arts and Sciences (October 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[99] Madhukar, “The Hidden Costs of High-Tech Surveillance in Schools.”

[100] As used in this report, the term “students with disabilities” includes neurodivergent students as well as students with other disabilities.

[101] CRDC, *2017-18 State and National Estimations*.

[102] Lydia Brown et al., “Ableism and Disability Discrimination in New Surveillance Technologies,” Center for Democracy and Technology (May 2022), https://cdt.org/wp-content/uploads/2022/05/2022-05-23-CDT-Ableism-and-Disability-Discrimination-in-New-Surveillance-Technologies-report-final-redu.pdf.

[103] U.S. Education Department, Office for Civil Rights, “Supporting Students with Disabilities and Avoiding the Discriminatory Use of Student Discipline under Section 504 of the Rehabilitation Act of 1973” (letter from Assistant Secretary Catherine Lhamon, July 2022), https://www2.ed.gov/about/offices/list/ocr/docs/504-discipline-guidance.pdf.

[104] Ibid.

[105] Brown, “Ableism and Disability Discrimination.”

[106] Evan Enzer and Sarah Roth, “How Tech Treats Students With Disabilities Like Criminals,” The Daily Beast (August 3, 2022), https://www.thedailybeast.com/how-school-tech-treats-students-with-disabilities-like-criminals.

[107] Brown, “Ableism and Disability Discrimination.”

[108] Enzer, “How Tech Treats Students With Disabilities.”

[109] Ibid.

[110] Ibid.

[111] Brown, “Ableism and Disability Discrimination.”

[112] Lois Beckett, “Under Digital Surveillance: How American Schools Spy on Millions of Kids,” *The Guardian* (October 22,

2019), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

113 The Trevor Project "2023 U.S. National Survey on the Mental Health of LGBTQ Young People" (2023), www.thetrevorproject.org/survey-2023/assets/static/05_TREVOR05_2023survey.pdf; Kimberly J. Mitchell et al., "Accessing Sexual Health Information Online: Use, Motivations and Consequences for Youth with Different Sexual Orientations," *Health Education Research* 29, no. 1 (July 2014), 147-157, https://www.researchgate.net/publication/249967307_Accessing_sexual_health_information_online_Use_motivations_and_consequences_for_youth_with_different_sexual_orientations.; and Michele L. Ybarra et al., "Online Social Support as a Buffer Against Online and Offline Peer and Sexual Victimization Among US LGBT and Non-LGBT Youth." *Child Abuse and Neglect* 39 (September 2015), 123-136, https://www.researchgate.net/publication/265395448_Online_social_support_as_a_buffer_against_online_and_offline_peer_and_sexual_victimization_among_US_LGBT_and_non-LGBT_youth.

114 Laird, "Hidden Harms."

115 Ibid.

116 Mark Keierleber, "Trevor Project to Refund Donation From Student Surveillance Company Accused of LGBTQ Bias Following 74 Investigation," The 74 (September 30, 2022), https://www.the74million.org/article/trevor-project-teams-upith-student-surveillance-company-accused-of-lgbtq-bias//.

117 Neal A. Palmer and Emily A. Greytak, "LGBTQ Student Victimization and Its Relationship to School Discipline and Justice System Involvement," *Criminal Justice Review* 42, no. 2 (May 17, 2017), 63 – 187, https://journals.sagepub.com/doi/10.1177/0734016817704698; and Shannon D. Snapp and Stephen T. Russell, "Discipline Disparities for LGBTQ Youth: Challenges That Perpetuate Disparities and Strategies to Overcome Them." *Inequality in School Discipline: Research and Practice to Reduce Disparities* (New York: Palgrave Macmillan, 2016), 207-223, https://www.researchgate.net/publication/306357063_Discipline_Disparities_for_LGBTQ_Youth_Challenges_that_Perpetuate_Disparities_and_Strategies_to_Overcome_Them.

118 Shannon D. Snapp, Jack K. Day, and Stephen T. Russell. "School Pushout: The Role of Supportive Strategies Versus Punitive Practices for LGBT Youth of Color." *Journal of Research on Adolescence* 32, no. 4 (December 2022), 1470-1483, https://www.s-r-a.org/index.php?option=com_dailyplanetblog&view=entry&category=researchsummaries&id=130:school-pushout-the-role-of-supportive-strategies-versus-punitive-practices-for-lgbt-youth-of-color; Gay, Lesbian, and Straight Education Network (GLSEN), "Educational Exclusion: Drop Out, Push Out, and School-to-prison Pipeline Among LGBTQ Youth," GLSEN (2016); and Jennifer Chmielewski et al., "Intersectional Inquiries with LGBTQ and Gender Nonconforming Youth of Color: Participatory Research on Discipline Disparities at the Race/Sexuality/Gender Nexus," *Inequality in School Discipline: Research and Practice to Reduce Disparities* (New York: Palgrave Macmillan, 2016), 171-188.

119 Elizabeth Laird et al., "Hidden Harms: The Misleading Promise of Monitoring Students Online. Center for Democracy & Technology," Center for Democracy and Technology (August, 2022), https://cdt.org/wp-content/uploads/2022/08/Hidden-Harms-The-Misleading-Promise-of-Monitoring-Students-Online-Research-Report-Final-Accessible.pdf.

120 Philip Connor, "At Least 600,000 K-12 Undocumented Students Need a Pathway to Citizenship," fwd.us (Aug 19, 2021), https://www.fwd.us/news/k-12-undocumented-students/.

121 Asad L. Asad, "The Everyday Surveillance of Undocumented Immigrants," American Sociological Association, footnotes, 51, no. 3, https://www.asanet.org/footnotes-article/the-everyday-surveillance-of-undocumented-immigrants/.

122 Emma Tynan et al., "Caught in an Educational Dragnet: How the School-to-Deportation Pipeline Harms Immigrant Youth and Youth of Color," National Immigration Law Center (May 19, 2022), https://www.nilc.org/2022/05/19/caught-in-an-educational-dragnet-how-the-school-to-deportation-pipeline-harms-immigrant-youth-and-youth-of-color-the-torch/.

123 Ibid.

124 DoSomething.org, "11 Facts About Education and Poverty in America," https://www.dosomething.org/us/facts/11-facts-about-education-and-poverty-america - fn7.

125 Karen Broadhurst, Helen Paton, and Corinne May-Chahal, "Children Missing from School Systems: Exploring Divergent Patterns of Disengagement in the Narrative Accounts of Parents, Carers, Children and Young People," *British Journal of Sociology of Education* 26, no. 1 (February 2005), 105-119, https://www.jstor.org/stable/30036047.

126 Save Our Schools March, "Poverty; The Effect on the Whole Child" (accessed March 1, 2014), https://saveourschoolsmarch.org/issues/poverty-and-the-effect-on-education/poverty-the-effect-on-the-whole-child/.

127 Janet Currie, "Poverty Among Inner City Children," in Robert Inman (ed.), *Making Cities Work: Prospects and Policies for Urban America* (Princeton: Princeton University Press, 2009), https://drive.google.com/file/d/1ee68T2XU_NCN07GefhB_tsw2AHn5RrEW/view.

128 U.S. Department of Education, National Center for Education Statistics (NAEP), "NAEP 1999 Trends in Academic Progress: Three Decades of Academic Progress" (August 2000), 107, https://nces.ed.gov/nationsreportcard/pdf/main1999/2000469.pdf.

129 Jason DeParle, "For Poor, Leap to College Often Ends in a Hard Fall," *New York Times* (December 22, 2012), https://www.nytimes.com/2012/12/23/education/poor-students-struggle-as-class-plays-a-greater-role-in-success.html?pagewanted=all.

130 Fedders, "The Constant and Expanding Classroom."

131 Stephanie Coyle and Simon McCormack, "This Software Could Be Spying on NYC Students," ACLU of New York" (November 19, 2021), https://www.nyclu.org/en/news/software-could-be-spying-nyc-students.

132 Corrine David-Ferdon et al., "Youth Violence Prevention Resource for Action: A Compilation of the Best Available Evidence," Centers for Disease Control and Prevention, National Center for Injury Prevention and Control (2016), www.cdc.gov/violenceprevention/pdf/YV-Prevention-Resource_508.pdf; Sanna King and Nicole Bracy, "School Security in the Post-Columbine Era: Trends, Consequences, and Future Directions," *Journal of Contemporary Criminal Justice*, 35, no. 3 (2019), 274 – 295, https://doi.org/10.1177/1043986219840188";

and Jonathan Cohen et al., "Rethinking Effective Bully and Violence Prevention Efforts: Promoting Healthy School Climates, Positive Youth Development, and Preventing Bully-Victim-Bystander Behavior" (September 2015), https://www.researchgate.net/publication/281593701_Rethinking_Effective_Bully_and_Violence_Prevention_Efforts_Promoting_Healthy_School_Climates_Positive_Youth_Development_and_Preventing_Bully-Victim-Bystander_Behavior.

[133] Kyle S. Mackie. "Facial recognition in Lockport schools: 'Best technology in the world' or 'not proven to work?'", *WBFO-FM 88.7 NPR* (June 24, 2020), https://www.wbfo.org/education/2020-06-24/facial-recognition-in-lockport-schools-best-technology-in-the-world-or-not-proven-to-work

[134] Jim Shultz, "Spying on Children Won't Keep Them Safe," *The New York Times* (June 07, 2019), https://www.nytimes.com/2019/06/07/opinion/lockport-facial-recognition-schools.html

[135] A Comprehensive Report on School Safety Technology, Johns Hopkins University Applied Physics Laboratory (with The Johns Hopkins University School of Education, Division of Public Safety Leadership), October 2016. https://www.ojp.gov/pdffiles1/nij/grants/250274.pdf

[136] Fedders, "The Constant and Expanding Classroom."

[137] This is deeply regretful because harmful student surveillance technologies will not make schools safer. To do that we need to invest in teachers, mental health professionals, and support staff who can build deep relationships with students, pay attention to when things are going wrong, and create a culture of trust and accountability, and these meaningful interventions frequently represent the opportunity costs of committing to surveillance interventions.

[138] Singer, "Schools Are Spending Billions."

[139] Warren, "Warren, Markey, Blumenthal Raise Concerns."

[140] White House, "Blueprint for an AI Bill of Rights," White House Office of Science and Technology Policy (October 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[141] ACLU of Minnesota, "Bill Championed by ACLU-Minnesota to Protect Student Privacy Becomes Law" (May 23, 2022), https://www.aclu-mn.org/en/news/bill-championed-aclu-mn-protect-student-privacy-becomes-law.

[142] Aaron Gordon, "When School Superintendents Market Surveillance Cameras," Vice (October 4, 2022), https://www.vice.com/en/article/93anj7/when-school-superintendents-market-surveillance-cameras.

[143] Mark Keierleber, "The Risks of Student Surveillance Amid Abortion Bans and LGBTQ Restrictions," *The Guardian* (September 8, 2022), https://www.theguardian.com/education/2022/sep/08/abortion-bans-school-surveillance-lgbtq-restrictions.

[144] Louis Hochman, "Montclair Schools Halt Use of GoGuardian Monitoring (for Now), *Montclair Local* (March 8, 2021), https://montclairlocal.news/2021/03/montclair-schools-halt-use-of-goguardian-monitoring-for-now/

[145] New York State Education Department (NYSED), Ed Management Services, "Smart Schools" (2014), https://www.p12.nysed.gov/mgtserv/smart_schools/home.html; and NYSED, Ed Management Services, "Smart Schools Bond Act Implementation Guidance," https://www.p12.nysed.gov/mgtserv/documents/SSBAGuidancerev_6_1_18_Final.pdf.

[146] NYSED, Ed Management Services, Lockport City School District, "Smart Schools Investment Plan (2016-2017)" (last modified October 23, 2017) (emphasis added), https://p1232.nysed.gov/mgtserv/documents/LOCKPORTCITYSD.pdf.

[147] See *Shultz v. New York State Education Department,* 2021 N.Y. Slip Op. 33434 (N.Y. Sup. Ct. 2021), https://casetext.com/case/shultz-v-ny-state-educ-dept; and Davey Alba, "The First Public Schools in the US Will Start Using Facial Recognition Next Week," Buzzfeed News (May 30, 2019), https://www.buzzfeednews.com/article/daveyalba/lockport-schools-facial-recognition-pilot-aegis.

[148] Todd Feathers, "Company Lied to School District About Its Racist Tech," Vice (December 1, 2020), https://www.vice.com/en/article/qjpkmx/fac-recognition-company-lied-to-school-district-about-its-racist-tech; *Times Union* editorial board, "A Study in Surveillance," *Times Union* (June 9, 2019), https://www.timesunion.com/opinion/article/Editorial-A-study-in-surveillance-13964155.php; Alfred Ng, "Facial Recognition in Schools: Even Its Supporters Say It Won't Stop Shootings," CNET (January 24, 2020), https://www.cnet.com/news/politics/features/facial-recognition-in-schools-even-supporters-say-it-wont-stop-shootings/; and Connor Hoffman, "Funding Off Limits for Facial Recognition Projects," *Lockport Union-Sun Journal* (April 20, 2020), https://www.lockportjournal.com/news/local_news/funding-off-limits-for-school-facial-recognition-projects/article_408f2c42-3683-5331-ba38-a8269767e76f.html.

[149] Shultz 2021 N.Y. Slip Op. 33434 (N.Y. Sup. Ct. 2021), https://www.nyclu.org/en/cases/shultz-et-al-v-new-york-state-education-department. This case was dismissed as moot in August 2021 because the court found that due to the passage of the moratorium on biometric identifying technology in schools, State Technology Law § 106-b, petitioners had received all the relief that they had requested. The court, however, noted that any data produced from Lockport's system while it was activated is protected by Education Law § 2-d. *Shultz v. NYSED*, Index No. 904134-20, August 27, 2021 Judgment, New York Supreme Court, Albany County 2020.

[150] N.Y. Tech Law §§106-b(2)(a), (3)(a), https://www.nysenate.gov/legislation/laws/STT/106-B.

[151] ACLU of Rhode Island, "High School Non-confidential: How School-Loaned Computers May Be Peering Into Your Home" (June 1, 2017), https://www.riaclu.org/en/publications/report-high-school-non-confidential-how-schools-may-be-peering-your-home-june-2017.

[152] ACLU of Rhode Island, "Zooming in on Students: How Virtual Education Gets an "F" in Protecting Student Privacy (September 21, 2020), https://www.riaclu.org/en/publications/report-zooming-students-sept-2020.

[153] This report can be shared by providing a link to its home on the ACLU website: https://www.aclu.org/report/digital-dystopia

[154] This fact may be intentionally hidden or disguised.

[155] CNN, "cnn-school-shooting-data, https://github.com/cnnlabs/cnn-school-shooting-data/; Washington Post, "data-school-shootings" https://github.com/washingtonpost/data-school-shootings; Center for Homeland Defense and Security, "CHDS School Shooting Safety

Compendium” https://www.chds.us/sssc/data-map; Wikipedia, “List of School Shootings in the United States by Death Toll,” https://en.wikipedia.org/wiki/List_of_school_shootings_in_the_United_States_by_death_toll.; School Shooting Database,” https://schoolshootingdatabase.com/databases

156 Reporting from the Brennan Center of Justice was particularly helpful in identifying school districts that used particular social media monitoring tools. See Jun Lei Lee and Sophia DenUyl, “School Surveillance Zone,” Brennan Center for Justice (April 30, 2019), https://www.brennancenter.org/our-work/research-reports/school-surveillance-zone; and Brennan Center for Justice, “Social Media Monitoring in K-12 Schools: Civil and Human Rights Concern” (October 17, 2019), https://www.brennancenter.org/our-work/research-reports/social-media-monitoring-k-12-schools-civil-and-human-rights-concerns.

157 Multiple journalists attempted to submit public records requests and contacted schools, including one journalist who contacted schools about Social Sentinel. See Lizzie O’Leary, “Why Expensive Social Media Monitoring Has Failed to Protect School,” Slate (June 4, 2022), https://slate.com/technology/2022/06/social-media-monitoring-software-schools-safety.html.

158 As with all advanced technologies, new surveillance technologies are constantly being developed, and those producing them join and leave the market regularly. Thus, this is not intended to be an exhaustive list of all types of student surveillance technologies in 2023, and it most certainly is not inclusive of all the companies currently providing or marketing these technologies.

159 Dirnhuber, “HACK ATTACK”; and Stanley, “Does Surveillance Affect Us.”

160 Jay Morrison, “Cameras Are Being Used To Punish Students, Not Stop School Shooters,” *Forbes* (April 11, 2021), https://www.forbes.com/sites/nickmorrison/2021/04/11/cameras-are-being-used-to-punish-students-not-stop-school-shooters/?sh=6d9842f83669.

161 Patrick Grother, Mei Ngan, and Kayee Hanaoka, “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,” U.S. Department of Commerce, National Institute of Standards and Technology (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

162 Jay Stanley, “Video Analytics: A Brain Behind the Eye,” ACLU (August 20, 2012), https://www.aclu.org/news/national-security/video-analytics-brain-behind-eye.

163 This is particularly problematic given that the U.S. Supreme Court has held that schools are supposed to be limited in what they can do in response to off-campus student speech. See *Mahanoy Area School Dist. v. B. L.*, 141 S. Ct. 2038, 2021, https://www.supremecourt.gov/opinions/20pdf/20-255_g3bi.pdf.

164 Vice, “‘They’re Watching Us.’”

165 Ibid.

166 University of Massachusetts Amherst, Manning College of Information and Computer Sciences, “Disparities in Natural Language Processing,” https://groups.cs.umass.edu/equate/research/natural-language-processing.

167 For an explanation of the importance of the ACLU’s ”fuck cheer” Supreme Court case, see David Cole, “The Supreme Court Teaches Students an Important Lesson on Free Speech,” *Washington Post* (June 23, 2021), https://www.washingtonpost.com/opinions/2021/06/23/cheer-case-supreme-court-speech/.

168 Keierleber, “Popular Student Monitoring Software.”

169 ACLU, “Court Orders Missouri School District to Stop Censoring LGBT Websites” (February 15, 2012), https://www.aclu.org/press-releases/court-orders-missouri-school-district-stop-censoring-lgbt-websites#:~:text=LGBTQ%20Rights-,PFLAG,Camdenton%20R%2DIII%20School%20District&text=JEFFERSON%20CITY%2C%20Mo.,communities%20through%20discriminatory%20filtering%20software.

170 The claims appear to be dubious. See Jay Stanley, “Are Gun Detectors the Answer to Mass Shootings?” ACLU (November 2, 2022), https://www.aclu.org/news/privacy-technology/are-gun-detectors-the-answer-to-mass-shootings.

171 Todd Feathers, Facial Recognition Company Lied to School District About its Racist Tech,” Vice (December 1, 2020), https://www.vice.com/en/article/qjpkmx/fac-recognition-company-lied-to-school-district-about-its-racist-tech.

172 “Opinion: Body Scanner Problems at Charlotte-Mecklenburg Schools,” *Charlotte Observer* (editorial) (August 25, 2022), https://www.govtech.com/education/k-12/opinion-body-scanner-problems-at-charlotte-mecklenburg-schools.

173 KFSM-TV, “Greenwood Police Assure High School Is Safe After False Alarm Leads to Lockdown” (February 23, 2023), https://www.5newsonline.com/article/news/local/false-alarm-greenwood-high-school-gunshot-detector/527-be4f0e9b-b096-4aee-bdea-25339135f998.

174 Patrick Wall, “Newark is Installing Gunshot Detectors on Mostly Black Schools As City Shootings Rise,” Chalkbeat Newark (July 26, 2021), https://newark.chalkbeat.org/2021/7/26/22594328/shotspotter-newark-schools.

175 See *Ogletree v. Cleveland State University*, 1:21-cv-00500 (N.D. Ohio Dec. 20, 2022), https://www.govinfo.gov/content/pkg/USCOURTS-ohnd-1_21-cv-00500/pdf/USCOURTS-ohnd-1_21-cv-00500-0.pdf.

176 Wikipedia, “*Robbins v. Lower Merion School District*.”

ACLU