The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies: Recommendations for Schools

BY SARA COLLINS • JASMINE PARK • ANISHA REDDY • YASAMIN SHARIFI • AMELIA VANCE

FUTURE OF PRIVACY FORUM

SEPTEMBER 2021

As educators and school leaders return to campus after two years of significant upheaval and loss, many are prioritizing efforts focused on students' well-being, including ensuring that students receive adequate mental health support. Throughout the COVID-19 pandemic, some experts suggest that the stressors associated with the pandemic and learning from home may have impacted students' mental health, potentially increasing students' risks of self-harm and suicide.[1] Given this increased concern about student mental health, many school districts have recently and rapidly adopted self-harm monitoring systems.

Self-harm monitoring systems are computerized programs that can monitor students' online activity on school-issued devices, school networks, and school accounts to identify whether students are at risk of dangerous mental health crises. These monitoring systems identify individual students by processing and collecting personal information from their online activities and sending alerts about individual students and their flagged content to school officials. In some cases, these systems or school policies facilitate sharing this information with parents or third parties, such as law enforcement agencies.

Despite their increased use, self-harm monitoring systems are an unproven technique for effectively identifying and assisting students who may be considering self-harm simply based on their online activities.

Despite their increased use, self-harm monitoring systems are an unproven technique for effectively identifying and assisting students who may be considering self-harm simply based on their online activities. School districts may overestimate the ability of self-harm monitoring systems to identify students and underestimate the importance of developing comprehensive policies and processes for using the systems. Due to the inherent limitations in a computer system's ability to interpret context, these systems often inaccurately or mistakenly flag student content and over-collect confidential data.[2]

The increased and rapid adoption of these systems raises important questions about the effectiveness and consequences of self-harm monitoring systems for students' mental health, privacy, and equity. Monitoring systems can scan and monitor students' searches, emails, documents, and online activities including social media and online communications on school-issued devices. Education leaders must carefully weigh the risks and harms associated with adopting monitoring technologies, implement safeguards and processes to protect students who may be identified, establish a strong communications strategy that includes school staff, students, parents,[3] and caregivers, and ensure that their schools' and districts' monitoring programs and service-delivery systems do not exacerbate inequities. Further, schools must have the necessary mental health resources and professionals (school-based psychologists, counselors, and social workers) in place to support students identified by the program, which most schools across the country do not have.[4]

Merely adopting monitoring systems cannot serve as a substitute for robust mental health supports provided in school or a comprehensive self-harm prevention strategy rooted in evaluated strategies that have evidence of effectiveness. Identifying

students alone does not equate to supporting their mental health. Absent other support, simply identifying students who may be at risk of self-harm—if the system does so correctly—will, at best, lead to no results. At worst, it can violate a student's privacy or lead to a misinformed or otherwise inappropriate response. Schools must have robust mental health response plans in place to effectively support any students who may be identified *before* adopting monitoring systems.

Without proper planning and recognition of monitoring systems' limitations, using monitoring software as a self-harm detection tool can trigger unintended consequences. In particular, using self-harm monitoring systems without strong guardrails and privacy-protective policies is likely to disproportionately harm already vulnerable student groups. Potential harmful outcomes include:

- Students being mistakenly flagged,
- Students being unfairly treated once flagged as a result of improper sharing of this status and bias or stigma around mental illness,
- Students being subject to excess scrutiny by the school in ways that can be stigmatizing and alienating,
- Students having mental health details or their flagged status inappropriately disclosed,
- Students being needlessly put in contact with law enforcement and social services, or facing school disciplinary consequences as a result of being flagged,
- Students having sensitive personal information, such as gender identity, sexual orientation, citizenship status, religious beliefs, political affiliations, or family situation revealed or shared, and
- Students experiencing a chilling effect, making them hesitant to search for needed resources on school devices out of fear of being watched by school officials or flagged by the monitoring system.

All of these outcomes could ultimately undermine the primary goal of improving students' mental well-being.[5] To mitigate this, schools must:

> **Schools must have robust mental health response plans in place to effectively support any students who may be identified before adopting monitoring systems**

- Ensure they have sufficient school-based mental health resources and appropriate processes in place to support any students with mental health needs if they are accurately identified through self-harm monitoring technology,
- Develop a robust mental health response plan beyond simply identifying students through a monitoring system, and
- Have well-developed policies governing how schools will use monitoring systems, respond to alerts, and protect student information before they acquire the technology.

To help education leaders understand and weigh these risks, this report describes self-harm monitoring technology and how schools use it, details the privacy and equity concerns introduced by these monitoring systems, points out challenges that undermine the accuracy and limit the usefulness of these systems for addressing student mental health crises, outlines legal considerations related to monitoring students for self-harm, provides crucial questions that school and district leaders should consider regarding monitoring technologies, and offers recommendations and resources to help schools and districts protect students' privacy in the context of monitoring for self-harm.

AUTHORS

Sara Collins

Jasmine Park

Anisha Reddy

Yasamin Sharifi

Amelia Vance

ACKNOWLEDGMENTS

FPF thanks the following individuals and organizations for contributing their time, insight, and work in providing feedback on the information in this report:

Nic Albert

Elijah Armstrong

Isabelle Barbour, MPH, *Truthteller Consulting*

Caitlyn Clibbon, *Disability Rights Florida*

Tony DePalma, *Disability Rights Florida*

Juliana Cotto

Ahuva Goldstand

Ashleigh Imus

Dr. Sara Jordan

Dr. Carrie Klein

Lindsay Kubatzky, *National Center for Learning Disabilities*

Clarence Okoh, *NAACP Legal Defense and Educational Fund, Inc.*

Jennifer Mathis, *Bazelon Center for Mental Health Law*

David Sallay

Zoe M. Savitsky

Todd A. Savage, Ph.D., NCSP, *School Safety and Crisis Response Committee of the National Association of School Psychologists*

Sam Boyd, *Senior Staff Attorney, Southern Poverty Law Center*

The Children's Rights Practice of the Southern Poverty Law Center

Gretchen M. Shipley, *Fagen Friedman & Fulfrost LLP*

Jim Siegl

Alexis Shore

John Verdi

Scott A. Woitaszewski, Ph.D., *NCSP, School Safety and Crisis Response Committee of the National Association of School Psychologists*

DISCLAIMER

This report provides general information, not legal advice, and following the recommendations or tips within does not guarantee compliance with any particular law.

ABOUT THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a nonprofit organization focused on how emerging technologies affect consumer privacy. FPF is based in Washington, DC, and includes an advisory board comprised of leading figures from industry, academia, law, and advocacy groups.

FPF's Youth & Education Privacy program works to protect child and student privacy while allowing for data and technology use that can help young people learn, grow, develop, and succeed. FPF works with stakeholders from practitioners to policymakers, providing technical assistance, resources, trend analysis, and training. FPF's Youth and Education Privacy team runs Student Privacy Compass, the one-stop-shop resource site on all things related to student privacy.

TABLE OF CONTENTS

Background: What Is Self-Harm Monitoring Technology and How Do Schools Use It?

Schools often adopt self-harm monitoring technology with the best intentions: to help keep students safe and improve their well-being. However, if implemented without due consideration to the significant privacy and equity risks posed to students, these programs may harm the very students that need the most support or protection, while ineffectively fulfilling their intended purpose of preventing self-harm. Before adopting self-harm monitoring technology, schools and districts should understand the risks self-harm monitoring technology can pose to students' privacy and safety, take thoughtful steps to mitigate those risks, and carefully weigh the risks against any benefits.[6] After weighing the equities, some schools choose not to adopt this technology. When schools choose to adopt, strong privacy and equity practices must be identified and implemented.

Why do schools use monitoring technology?

Schools generally use monitoring software with two goals: legal compliance and with the intention to keep students safe.

Legal Compliance

Most schools adopted monitoring software long before self-harm monitoring software was available in order to comply with the Children's Internet Protection Act (CIPA). When CIPA was enacted more than 20 years ago, the role of software was to block access to obscene or harmful online content, and monitoring typically took place in a computer lab, where teachers and school staff could view, in person, the content students were accessing on their school computers. Today, schools across the country provide students with various options to learn through technology, including requiring students to bring their own devices to school[7] or providing them with school-issued laptops, tablets,[8] or mobile hotspots,[9] dramatically increasing the breadth and invasiveness of monitoring that can occur. The type and extent of monitoring required by the law has been interpreted unevenly by different districts, ranging from fairly minimal approaches to much more extensive interpretations.[10] The Federal Communications Commission (FCC) has yet to publish guidance on CIPA and monitoring. In addition to the lack of guidance on CIPA's practical

application, there is also no guidance on how CIPA interacts with the Family Educational Rights and Privacy Act (FERPA), a federal education privacy law that grants parents and students specific rights to student education records. For more on FERPA's application to student monitoring, see page ___.

Remote learning during the COVID-19 pandemic (see Box 3 discussing the effect of the pandemic) has only increased student usage and reliance on school-mediated technology, especially take-home internet hotspot devices issued by schools to help close the digital divide. In response to the pandemic, in August 2021, the FCC announced more than $5 billion in school and library-issued requests to fund 9.1 million connected devices, with 5.4 million broadband connections through the Commission's Emergency Connectivity Fund.[11] Without clarity on CIPA's requirements, schools may unintentionally over-surveil and over-collect sensitive, personal information about students or their families in an attempt to comply with the law. For example, monitoring on school-issued hotspot devices brought home by students may not be limited solely to school hours, and may capture internet activities of not just the student but also other members of the household.

In addition to CIPA, schools may be subject to state-level filtering and cyberbullying laws that may require them to implement filtering and monitoring technology to ensure that students safely access the internet for school purposes.

Keeping Students Safe

In addition to legal obligations, schools want to ensure the wellbeing of their students. The internet has enabled access to inappropriate content, bullying in cyberspace in addition to school hallways, and non-consensual sharing of intimate images. The rapid adoption by schools of communication and collaboration tools from Google and Microsoft, driven in part recently by remote learning needs,[12] has also generated large volumes of student communications and digital content. Because of these factors, monitoring technologies are often appealing to many schools, families, and other education stakeholders who seek to know what students are doing online,[13] including identifying when students are facing mental health concerns and particularly when students are looking up information about self-harm or suicide.

Many policymakers and educators hope that these monitoring systems can help schools identify students at risk of self-harm or suicide so that schools can direct them to help and resources they might not otherwise receive. For example, in early 2021, a Florida legislator sought funding for

> **Before adopting self-harm monitoring technology, schools and districts should understand the risks self-harm monitoring technology can pose to students' privacy and safety, take thoughtful steps to mitigate those risks, and carefully weigh the risks against any benefits.**

schools across the state to adopt the monitoring provider Gaggle to "protect Florida youth from suicide and self-harm."[14] Similarly, the North Carolina Coronavirus Relief Act 3.0 made $1 million "available to public school units to purchase one or more Gaggle safety management products to enhance student safety while providing remote instruction."[15] Local education leaders also see a need to adopt self-harm monitoring systems. In 2019, for example, a school system in Wilson County, Tennessee expanded its monitoring system, designed initially to detect violent threats to school safety, to also scan student-created content on school devices, such as emails and online posts, for signs of self-harm. A counselor in the school district described the monitoring system as generating red flags in response to keywords, including "self-harm," "suicide," and "overdosing," or phrases such as "I just want to cut myself."[16] Importantly, the district noted that the

BACKGROUND

program was incorporated in a larger process—when such online activity is identified as a potential source of harm, counselors can then perform a risk assessment, involve parents, and offer mental health resources. In the first two months of 2019, Wilson County schools told *News4 Nashville* that they had identified 11 cases requiring intervention using their expanded monitoring system, although these cases were not limited to suicide-related comments and also included language related to drug use and sharing inappropriate photos.

Self-harm monitoring companies and the media have shared similar accounts and experiences from other school districts as well. In Caddo Parish Public Schools in Louisiana, the district's instructional technologist reported that the self-harm monitoring system Lightspeed Alert helped identify a student contemplating suicide during the pandemic.[17] In Las Vegas, a 12-year-old student was flagged by his school after he used his school-issued iPad to search for "how to make a noose."[18] Neosho School District in Missouri told *NPR* that the district has identified a struggling student at least once per semester, which enables them to conduct an early intervention.[19] These anecdotes illustrate just a few of the compelling reasons why schools and districts may want to adopt self-harm monitoring technologies.

Charged with the care of children, schools have clear incentives to look for straightforward indicators of self-harm risks; they would certainly want to catch students messaging classmates with a plain intention to harm themselves, or students querying a search engine for ways to die by suicide. But those circumstances—in which there is a clear, imminent danger of a student about to harm themselves—are fortunately rare, and scanning for self-harm using monitoring systems often seeks to identify situations that are much more ambiguous.

What do schools monitor?

Monitoring technologies generally work by scanning and flagging (marking for action by the system based on certain criteria) students' online activities and content on school-issued devices, school networks, and certain school services (e.g. Google Workspace or Microsoft Office 365) for indications that a student may be at risk of harming themselves.

BACKGROUND

As discussed above, CIPA specifically requires schools that receive federal E-Rate funding to filter and monitor[20] students' online activity to prevent them from accessing inappropriate content, such as graphic, violent, or sexually explicit material.[21] When schools adopt self-harm monitoring software, it often is an addition to this more general monitoring occurring in the district.

Each type of monitoring software is different, and may offer different features. Generally, monitoring software is either scanning all web traffic—the information received and sent in a web browser (such as Chrome, Firefox Safari, or Edge)—or monitoring the content of specific applications owned by the school, such as their email (such as Outlook or Gmail), file storage (such as Microsoft OneDrive or Google Drive), and school-managed chat applications (such as Google Chat or Microsoft Teams). Several monitoring software companies also provide an option for classroom management software, which allows a teacher to monitor the screens and web browsing of their students during a class session, and focus the class's attention by preventing web browsing, pushing a web page to all students, or focusing student's attention on a specific web page. Unlike general internet filtering software (which may filter or monitor student's personal devices that connect to a school network or a school-provided wireless hotspot), self-harm monitoring software is typically installed only on school-provided devices. However, when there is monitoring of certain school-managed services (e.g. Google Workspace or Microsoft Office 365), monitoring can occur on both school-provided and personal devices since the monitoring software is scanning all content created in those accounts.

How does monitoring occur?

When monitoring software is scanning web traffic or specific applications, it could either 1) scan the content and only keep content when it is "flagged" as inappropriate or otherwise problematic,[22] or 2) keep all of the content that is scanned so schools officials can retrospectively see the websites that specific students were visiting and some of their activities online.

This process of reviewing, flagging, and alerting will be familiar to anyone that has ever received an alert from their credit card company of a suspicious transaction. While some schools deploy technology that simply emails an administrator when a student accesses an inappropriate website, email or search term,[23] other schools use more intensive monitoring that creates a log of each student's search and web browsing activity.[24]

BACKGROUND

> **While some schools deploy technology that simply emails an administrator when a student accesses an inappropriate website, email or search term, other schools use more intensive monitoring that creates a log of each student's search and web browsing activity.**

Monitoring services overwhelmingly employ algorithms that rely on scanning and detecting key words or phrases across different platforms. [25] These algorithms can be based on simple natural language processing of keywords or may attempt to use other types of artificial intelligence[26] to examine the context of the content to improve the reliability of the "flagging" process.[27] Some monitoring services go beyond algorithms and employ a second step in their flagging process, in which the content is reviewed by the monitoring companies' internal personnel to check for false positives or to review additional context to better understand the flagged content.[28]

The alerting process varies between services and in different situations. For many monitoring services, different content can trigger different alerts or responses. For example, terms or activity that monitoring services have grouped into lower-level or less serious inappropriate content may simply be blocked.[29] If more serious inappropriate content is flagged or detected, students may receive warnings by email for violations, and school administrators may be copied in instances of multiple warnings.[30] When content indicating a possible threat to a student's personal safety or the safety of other students is detected, it could result in direct personal notification to the school or, in extreme cases, to law enforcement or emergency services.[31] These more extensive monitoring services can allow school officials to see what each student has been doing online (and, with some software, can automatically send that information to parents).[32]

How common is student monitoring in schools?

Monitoring technology has become prevalent in schools throughout the country. E-rate funding is provided to approximately 95 percent of schools,[33] so most schools have some web filtering and monitoring system that blocks access to content that is obscene or harmful to minors in order to comply with CIPA. In recent nationwide research with teachers whose schools use monitoring systems, 52 percent reported their school's monitoring included flagging keyword searches, such as "accessing information on self-harm." [34] For example, more than 15,000 schools use the monitoring service Securly, and 10,000 schools use the service GoGuardian.[35] However, all of these services only advertise their number of subscribers for their general CIPA monitoring or classroom management services, and not for their specific self-harm monitoring service. As a result, it is unclear what percentage of their subscribing schools have chosen to use self-harm monitoring detection in addition to their existing monitoring services. In contrast, Gaggle, which is used in over 1,500 school districts,[36] does not provide CIPA content filtering directly and focuses exclusively on self-harm, violence, and objectionable content monitoring.

How is self-harm monitoring different from monitoring generally?

Self-harm monitoring systems present a new, significant turn from the way schools have used monitoring systems for content filtering and CIPA compliance over the past 20 years. By seeking to draw conclusions about students' mental health status based on their online activities and initiating actions involving school officials and other third

BACKGROUND

parties based on these inferences, self-harm monitoring systems introduce greater privacy risks and unintended consequences for students.

Several online monitoring companies that market to schools have expanded their services to offer monitoring technology that specifically seeks to identify students at risk of self-harm or suicide. These services employ the same general flagging and alerting process described above, but with a specific focus on content that might implicate suicide or other forms of self-harm. A range of content may be flagged, and the appropriate response or alert may depend on the severity of the content, such as whether intentions of self-harm appear with evidence of an imminent plan.[37] For example, the monitoring company Lightspeed has a product called "Alert", which employs "safety specialists"[38] who escalate immediately "to district safety personnel and/or law enforcement, enabling early intervention"[39] if a student's plan to harm themselves is deemed imminent. The monitoring company GoGuardian offers the alert service "Beacon," which scans browser traffic to and from "search engines, social media, emails, chats, apps, and more" for "concerning activity surrounding self-harm and suicide."[40] Managed Methods, a student online monitoring service, offers a "Student Self-Harm Detection" tool that is described as detecting "self-harm content in school Google Workspace and Microsoft 365 apps."[41] Securly Auditor and Gaggle similarly monitor content in school Google Workspace and Microsoft 365 apps. While not the primary focus of this report, a relatively small number of schools have also used dedicated tools that scan students' social media posts for indicators of self harm or other threats.[42]

By seeking to draw conclusions about students' mental health status based on their online activities and initiating actions involving school officials and other third parties based on these inferences, self-harm monitoring systems introduce greater privacy risks and unintended consequences for students.

BACKGROUND

Concerns and Challenges Associated with Monitoring Technologies: Important Considerations for School Districts

Schools often adopt self-harm monitoring technology with the best intentions: to help keep students safe. However, if implemented without due consideration of the significant privacy and equity risks posed to students, these programs may harm the very students that need the most support or protection, while ineffectively fulfilling their intended purpose of preventing self-harm.

While monitoring companies claim to have flagged thousands of instances of self-harm content, there is no information available about how many of the students that were identified in these examples were found to be truly at-risk of self-harm as diagnosed by a mental health professional, how many students in these districts were at-risk but not picked up by the system, and what the context and size of the student population are in these publicized cases. No independent research or evidence[43] has established that these monitoring systems can accurately identify students experiencing suicidal ideation, considering self-harm, or experiencing mental health crises.[44] Self-harm monitoring technologies remain unproven as a prevention strategy and have not been substantiated by mental health professionals and clinicians as an effective tool for addressing mental health crises.

It is difficult to conclude the effectiveness and benefit of self-harm monitoring systems based solely on a few anecdotal examples shared by school districts and monitoring companies, especially when there are countervailing anecdotes of false flags and invasions of privacy. For example, *The 74* reported in 2021 that the monitoring software Gaggle, used in Minneapolis Public Schools, "flagged the keywords 'feel depressed' in a document titled 'SEL Journal,' a reference to social-emotional learning" taught as part of the school curriculum. In another instance, it "flagged the term 'suicidal' in a student's document titled 'mental health problems workbook.'"[45] Gaggle's CEO shared that a student "wrote in a digital journal that she suffered with self esteem issues and guilt after getting raped," which allowed school officials to "'get this girl help for things that she couldn't have dealt with on her own.'" *The Guardian* reported in 2019 that school officials had received "red flags when students tell each other sarcastically to 'kill yourself', talk about the band Suicide Boys, or have to write a school assignment on the classic American novel To Kill a Mockingbird."[46] *Education Week* reported that in Evergreen Public Schools in Washington State, at least a dozen students were flagged by monitoring software when they "stored or sent files containing the word 'gay.'"[47] These incidents demonstrate how monitoring systems can both flag innocuous, extraneous content and create significant privacy incursions of sensitive student information. These privacy incursions and the related legal concerns for the districts running monitoring software (described on page __) can be exacerbated when the majority of content flagged occurs when students are at home outside of normal school hours.[48]

Simultaneously, deploying self-harm monitoring technology raises important privacy and equity considerations that education leaders must consider. Schools and districts that consider or use self-harm technology must therefore weigh the harmful implications of using this technology against the uncertainty of its benefits or effectiveness. The section below outlines these specific privacy and equity considerations.

"*The 74* reported in 2021 that the monitoring software Gaggle, used in Minneapolis Public Schools, "flagged the keywords 'feel depressed' in a document titled 'SEL Journal,' a reference to social-emotional learning" taught as part of the school curriculum. In another instance, it "flagged the term 'suicidal' in a student's document titled 'mental health problems workbook."

Privacy and Equity Concerns Raised by Self-Harm Monitoring Technology

Before adopting self-harm monitoring technology, schools and districts should understand the risks self-harm monitoring technology can pose to students' privacy and safety and carefully weigh those risks against any benefits.

Schools have widely and rapidly adopted self-harm monitoring technologies, despite the fact that they are relatively new and unstudied.[49] Over the past two years, adoption increased as concerns grew about students struggling with mental health during the COVID-19 pandemic.[50] These facts raise important questions about the privacy risks and implications of monitoring that schools must carefully consider prior to implementation and revisit regularly. Such privacy risks may lead to disproportionate harms to students who are identified by self-harm monitoring, with especially inequitable consequences for systemically neglected groups of students. Suicide and self-harm disproportionally affect these vulnerable student populations, such as certain students who are minoritized in terms of race/ethnicity, sexual orientation, gender identity, disability status, or experiencing homelessness.[51] Moreover, students who are identified as "at-risk" may feel they have a target on their backs, with their personal struggles given limited privacy in school.

When schools use monitoring software, students deserve clear policies around what data is collected, who has access to it, how it will be used, and after what period it will be destroyed. Students deserve the assurance that all collected data will not be misused and that data collection and storage will be privacy-protective. Students deserve to have their schools held accountable, with clear consequences for those who put student privacy at risk by violating data sharing protocols. And students, educators, and families all deserve transparency.

The following privacy, equity, and implementation considerations guide the analysis in the following section. School leaders should ask themselves these key questions as they consider implementing a self-harm monitoring system:

- How will the school district create a school-wide mental health support program that is equitable and inclusive, and how does the technology fit into that program?
- Does the school district employ staff (e.g. school psychologists, school counselors and school social workers) with expertise to address mental health concerns that may be detected?
- What kinds of information do monitoring systems identify and flag, is the system collecting more information than the purpose requires, and how long will the data be retained?
- What harms, such as stigma or discrimination, may stem from collecting and/or sharing students' information or flagged status?
- Who has access to the information identified or flagged, and do they have a legitimate health or educational purpose for accessing it?
- How is student information shared with third parties, if at all, and are such disclosures permitted by law?
- How does the school district plan to provide transparent communication with families and students about monitoring policies, and how have they ensured that monitoring plans meet community needs?

How will the school district create a school-wide mental health support program that is equitable and inclusive, and how does the technology fit into that program?

Merely adopting monitoring systems cannot serve as a substitute for robust mental health supports provided in school or a comprehensive self-harm prevention strategy rooted in well-developed medical evidence. Schools must have robust mental health response plans in place to effectively support any students who may be identified *before* adopting monitoring systems. Schools and districts should carefully consider and discuss the extent to which self-harm monitoring is necessary and beneficial to the goals of their mental health support program, and, if so, craft evidence-based policies to manage the privacy and equity risks. These goals need to be clearly stated and specific in their scope. Goals such as "improving student mental health," or "saving lives" are too general because the connection between the tool and the steps required to achieve the goal are not evident. Specific goals define the problems to be solved and provide benchmarks to measure how successfully the chosen tool addresses the problem. Schools should have a clear explanation for why self harm monitoring is necessary, as opposed to, for example, establishing deeper systems of school-based mental healthcare and providing more robust preventative care resources to students. If the benefit of adopting self-harm monitoring technology will not outweigh the privacy and equity risks, and if there are other ways to fulfill the goals of the mental health support program, schools and districts should reconsider monitoring altogether.

Schools and districts should carefully consider and discuss the extent to which self-harm monitoring is necessary and beneficial to the goals of their mental health support program, and, if so, craft evidence-based policies to manage the privacy and equity risks.

If monitoring technology is adopted, it must be implemented as just one component of the broader mental health response plan. Identifying students alone does not support students or give them access to help. Monitoring companies agree that effective self-harm monitoring cannot solely rely on software and must be part of a comprehensive mental health approach by schools.[52] Absent other support, simply identifying students who may be at risk of self-harm—if the system does so correctly—will, at best, lead to no results. At worst, it can violate a student's privacy or lead to a misinformed or otherwise inappropriate response.

Does the school district employ staff with mental health expertise to address concerns that may be detected through self-harm monitoring systems?

It is imperative that schools employ professionals with the expertise (e.g. school psychologists, school counselors and school social workers) necessary to identify and address mental health concerns such as depression and anxiety. Unlike these professionals, teachers and school administrators are typically not licensed to identify and address mental health concerns and crises. In the absence of staff with this specialized knowledge and training, mental health misconceptions can drive and negatively influence even the best-intentioned efforts to help students. The American Civil Liberties Union found in 2019 that millions of students nationwide attend schools with no counselors, no school nurses, no school psychologists, and no school social workers.[53] Lack of in-school personnel and support means that flagging students via monitoring does not necessarily lead to help and resources for the students when there are none available in the school for them to receive. Likewise, simply informing a student's parents that their child has been flagged by a school monitoring system as at-risk for self-harm will not necessarily result in the student receiving appropriate mental health supports—many parents may be left unsure what to do with this information, especially in the absence of in-school or community-based resources and services that they can access.

What kinds of information do monitoring systems identify and flag, is the system collecting more information than the purpose requires, and how long will the data be retained?

Identifying content indicating a student's intent to self-harm is more challenging than it may seem. The data and activities that each monitoring system flags vary. A system may flag a student's activity when their content matches specific words or phrases, based on an algorithm or a machine learning model.[54] As a result, monitoring systems often fail to capture context or correctly interpret colloquial language that many students use. Peer-reviewed empirical research has repeatedly shown that context is extraordinarily difficult for most computer programs to accurately interpret,[55] such that monitoring systems end up simply searching for certain words and flagging them without the capacity to determine what they mean and how they are being used. A computer program is therefore prone to interpret many innocuous phrases as dangerous language and raise alerts, thereby flagging content unrelated to any mental health condition or any intent to self-harm.[56]

For example, the search history of a student conducting research on the poet Sylvia Plath or grunge-rock legend Kurt Cobain—both of whom died by suicide—might look remarkably similar to a monitoring system as the searches of a student suffering from depression. Similarly, students who share innocuous posts using slang about a "photobomb" or how their parents are "killing them" may be mistakenly flagged for using terms associated with violence.[57] This is an inherent shortcoming of using monitoring technology as a self-harm reduction strategy; it can penalize students for conducting research or expressing and exploring their feelings in developmentally normal ways. Published research studies[58] on the subject suggest that monitoring and flagging student content in this way can have a chilling effect[59] on students' healthy and natural exploration while making students hesitant to seek help when they need it.[60]

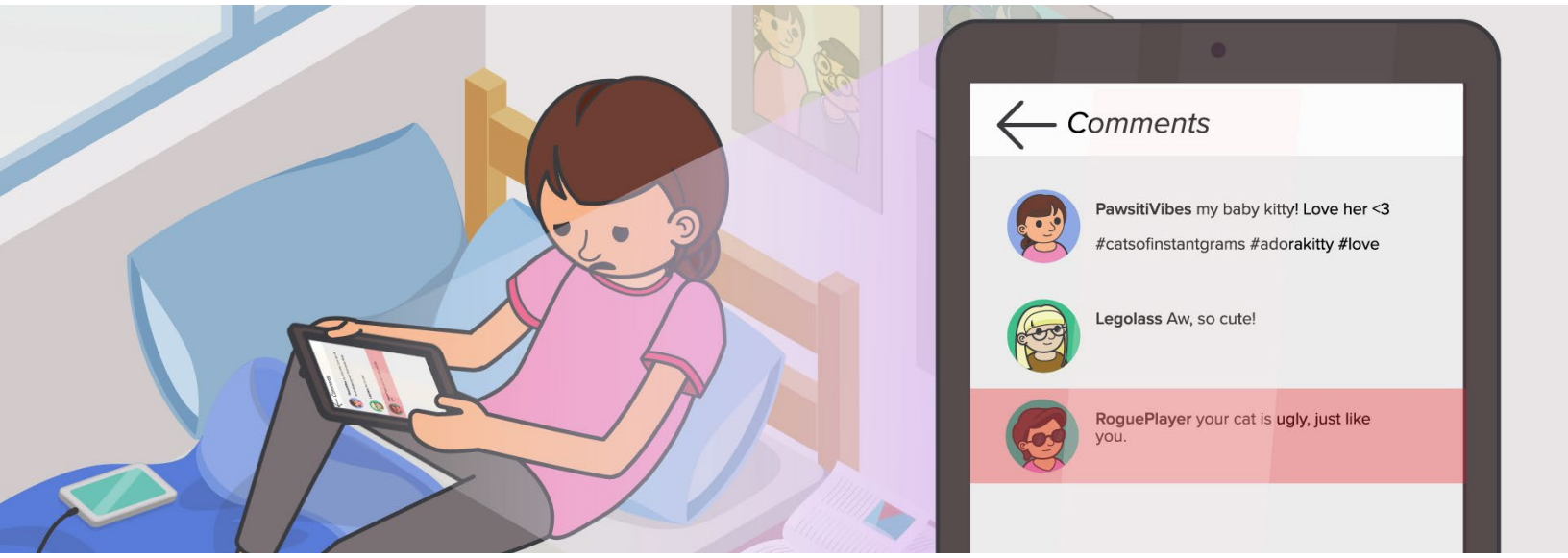
While some monitoring systems may include a broad range of default categories and indicators out of a well-intentioned belief that it is best to

capture any and all alarming student content possible, flagging overbroad keywords can reduce a monitoring program's potential effectiveness. In systems with a more narrow self-harm focus, school officials may be able to expand alert settings to monitor categories such as profanity. Including such overbroad indicators increases the administrative burden on school officials and provides little benefit, inundating them with vast amounts of normal student content that require extensive staff time and effort to review. This makes it harder for school staff to notice and identify flagged content actually related to risk of self-harm, and detracts time and resources from providing useful follow-up for any true risks and student needs.

Moreover, some monitoring systems flag data and activities by default that are unrelated to self-harm but that the school district or monitoring company may consider otherwise inappropriate or concerning. For example, *Buzzfeed* reported in 2019 that one monitoring company included "LGBTQ-related words like 'gay,' 'lesbian,' and 'queer'" as keywords that sent alerts to school officials (under the category of keywords that were monitored "in the context of possible bullying and harassment").[61] Other monitoring companies have filtered and blocked access to websites related to health resources for LGBTQ teens, news outlets that cover LGBTQ issues, anti-discrimination advocacy pages, and professional associations for LGBTQ individuals as part of their general monitoring regimen.[62] These flags and blocks risk inadvertently disclosing a student's gender identity or sexual orientation. This disproportionate flagging of LGBTQ students by monitoring systems can expose them to the privacy harms associated with monitoring and can even directly endanger their safety by exposing their sexual orientation or gender identity to school officials, families, or third parties. For more on the unique harms LGBTQ students may face as a result of monitoring technology in schools, and the legal implications of disparate flagging, see page ___ and Boxes 1 and 2.

Finally, a key factor in limiting unnecessary over-collection of student information revolves around schools' and monitoring providers' data retention and deletion practices. Data collection and retention will vary by monitoring system, and in some cases by type of data collected (e.g. students' web browsing history, email messages, drive files, etc.). One system, for example, monitors student emails by sending a copy of each email to the monitoring system and analyzing it for indicators of self-harm or other content that the system flags. If content is flagged, the student's email is saved and the monitoring system sends an alert to school administrators. If content is flagged, the student's email is saved and the monitoring system sends an alert to school administrators. If nothing is flagged, the copy of the email message is discarded.[63]

School leaders and monitoring companies should specify the period of time for which student information is retained by schools and by the company. School district leaders should consult with their state archives or records officer to determine the retention schedule for any data collected on



> While some schools deploy technology that simply emails an administrator when a student accesses an inappropriate website, email or search term, other schools use more intensive monitoring that creates a log of each student's search and web browsing activity.

students. Before publishing a retention schedule, school districts should determine whether any information collected through monitoring would be considered sensitive. Sensitive information, meaning any information that could adversely impact a student's educational or employment prospects, or could jeopardize a student's privacy or well-being by being shared, should be deleted as soon as legally allowable.

School districts should publish a retention schedule as part of their transparent communication about policies around the use of monitoring technology and should include information on how information will be destroyed once it is no longer needed. For example, in 2019, Montgomery Public Schools, Maryland, became the first district in the country to publicize a policy to annually delete student information from certain systems, such as internet search histories from the district's internet content filtering and classroom management provider.[64] This plan provides a strong example of appropriately limiting data retention and can serve as a model of effective student data retention policies for other school districts.

Increased data collection and sharing without clear justification frequently overwhelms administrators with information, undermines effective learning environments, casts suspicion on already marginalized students, tends to punish or criminalize students' medical struggles or disabilities, increases inequities, and can fail to promptly identify individuals who may be at true risk of self-harm. To mitigate these drawbacks, schools should develop clear guidelines about the kinds of material that systems should flag, tailor systems narrowly to respond to actual risks, and think critically about how they address identified concerns.

What harms, such as stigma or discrimination, may stem from sharing of students' information or flagged status?

Using self-harm monitoring systems raises potential risks of stigma or discrimination. Biases embedded in public perception and media lead to exaggerated fears that students experiencing mental health challenges are prone to violent acts,[65] even though most people with mental health needs have no propensity for violence.[66] As a result of such biases, school staff may treat flagged students differently from their peers or subject them to additional scrutiny. The common but false assumption that flagged students may be violent can increase harmful stigmas toward the students who need support and can lead them, especially systematically neglected students, to experience disproportionate rates of discipline.[67]

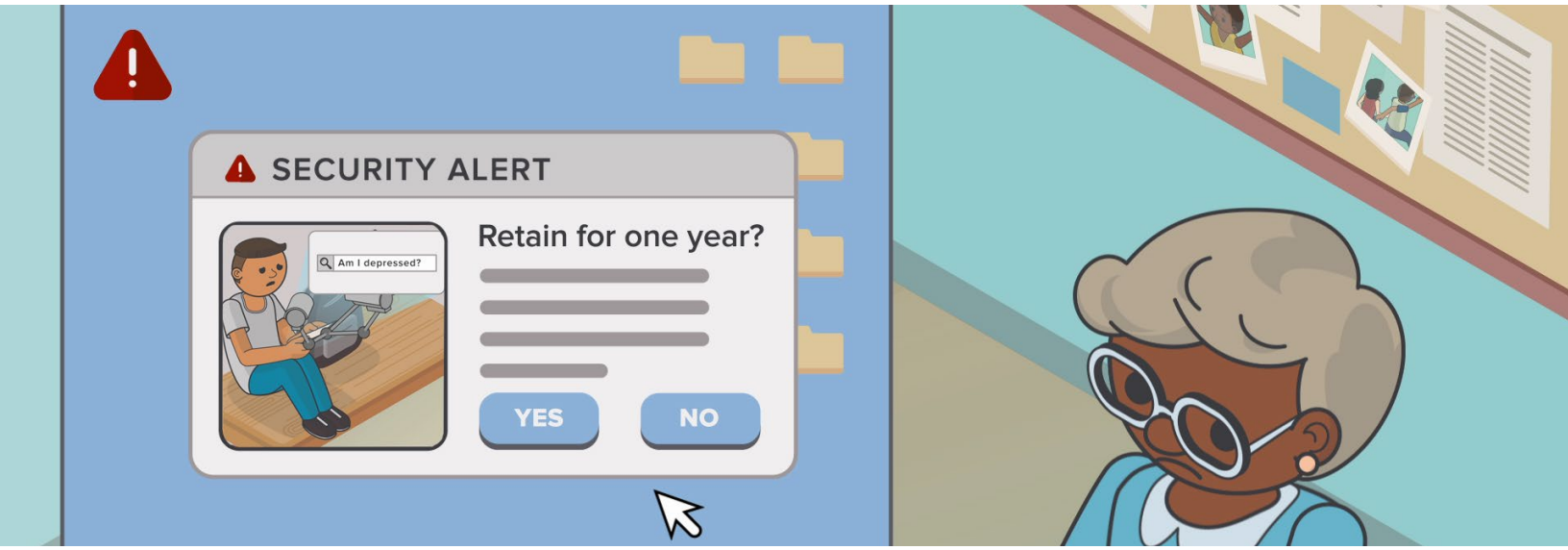
For example, in 2018, Florida passed a law[68] requiring schools to collect information from students at registration about past mental health referrals, while the state's school safety commission proposed that "students with IEPs [Individualized Education Programs] that involve severe behavioral issues" should be referred to threat assessment teams,[69] which are committees created in the wake of the tragic Parkland school shooting to evaluate whether individual students pose threats

of violence to the school community. Policies such as these immediately put students who struggle with mental health on a separate tier of scrutiny and potential disciplinary action due to deeply ingrained societal stigma, without leading to improved support or mental healthcare resources for the students. These policies could also have a chilling effect on disclosure. Parents are likely to worry that if their "children's mental health history becomes part of their school records, it could be held against them."[70] These concerns could result in a loss of trust and an unwillingness to provide schools and districts with sensitive information. In some cases, parents and students may even be disincentivized from seeking mental health treatment for fear that disclosure will harm their future opportunities.

In some cases, even when students seek help on their own, they may experience negative consequences. In one extreme example, the Bazelon Center for Mental Health Law represented a college student who voluntarily admitted himself to a campus hospital after a close friend died by suicide.[71] When he checked in, the campus hospital shared his health information with university administrators. The next day, while still in the hospital, the student received a letter from the university charging him with a violation of the disciplinary code, allegedly for endangering himself. The student was suspended from school, barred from entering the campus (including to see his psychiatrist), and threatened with arrest if he returned to his dormitory. While his father and friends removed his belongings from his dorm room, he was forced to sit in a car with a university official.

Situations like these demonstrate the potential harms of invasive or disciplinary school responses to information about a student struggling with mental health. Stigma is unfortunately real and should not be underestimated. Punitive responses contradict the goals of self-harm protection programs because they discourage students from seeking the help they need and engaging openly with mental health counselors or other healthcare providers. While monitoring companies claim their products help schools save lives, students may ultimately experience harm by not searching for resources that could help them out of a fear of being identified by school officials. Students who may be considering self-harm or who are struggling with their mental health can be disincentivized from seeking help if they fear that all help sought is monitored. Moreover, students who are identified as "at-risk" may feel like they have a target on their backs, with their personal struggles facing scrutiny in school. Students' opportunities should not be limited, either by mental health challenges or by violations of their privacy.

The risk of students being unfairly treated or experiencing discrimination as a result of a self-harm flag can be particularly high in schools and districts without enough school-employed mental health professionals—for example, school-based counselors, school psychologists, social workers, and nurses—a shortage that unfortunately afflicts most schools.[72] For detailed information on the potential discriminatory harms and stigma-related effects that can arise once a student is identified, see Boxes 1 and 2.



Box 1. Monitoring Inflicts Particular Harms on Systemically Marginalized Groups of Students

Beyond understanding the risk of criminalization and potential for referral to law enforcement, school districts should carefully consider the uniquely harmful impacts of monitoring on various systemically marginalized groups of students. Below are some examples of groups of students that may experience unique harms as a result of self-harm monitoring.

Students from Low-Income Backgrounds. Students from low-income backgrounds may not have a personal computer or internet access outside of the school campus or school-issued devices, leaving students without the ability to engage online free from their school's monitoring system. Educators report that while 71 percent of schools who use monitoring do so on school-issued devices, only 16 percent monitor students' personal devices,[73] leaving students without personal devices more prone to monitoring and any associated harms. Students without personal devices may be especially uncomfortable using school devices to seek support, if they know that these devices are subject to monitoring. These disparate impacts may be especially pronounced during the COVID-19 pandemic: while learning remotely, students have limited opportunities to seek more information or professional assistance beyond the internet and school-issued devices because they may have limited access to in-person resources. A survey in 2020 found that 8 percent or 4.4 million households do not have a computer always available. In households where a computer was always available, 60 percent received devices from the child's school or school district.[74] Similarly, students experiencing homelessness are unlikely to have access to personal devices and may heavily rely on school-issued devices, while especially needing to use them to search for non-academic resources or supports. These contextual factors suggest that self-harm monitoring programs require clear and transparent boundaries, protocols, and appropriate privacy protections. Otherwise, such programs risk harming the students they intend to protect.

Students Experiencing Language Barriers. Almost 5 million students in schools across the country are English Language Learners, comprising 9 percent of all public school students.[75] Students who are English Language Learners or multilingual, as well as students with disabilities, may be at especially high risk of false, inequitable flagging and of experiencing harm[76] from being flagged by a monitoring system. Students who are English Language Learners may often use or interact with content in languages that school officials or a monitoring company do not understand or may interpret negatively.[77] Deeply ingrained biases against students who are English Language Learners can especially influence suspicious and negative interpretations of their writing and activities.[78] Similarly, students who are English Language Learners may sometimes lack the proficiency or cultural nuance to express themselves as non-English Learners would and may mistakenly use words or phrases that a monitoring program may flag or school officials may misinterpret as a threat to self. As a result, there is a high risk that intent and meaning may get lost in translation, and these students will end up flagged or penalized for innocuous language that school staff fail to accurately decipher. Language barriers or miscommunications and misunderstandings based on differential language use can also surface when monitoring technology scans the content of some students with disabilities.

In addition, monitoring systems may utilize automatic, computerized translations when scanning student content in non-English languages. These computerized translations are frequently inaccurate

Box 1. Monitoring Inflicts Particular Harms on Systemically Marginalized Groups of Students

and fail to account for idiomatic language use or cultural nuance.[79] For example, direct translation of a phrase meaning, "You're annoying me," from Korean to English resulted in widespread use of the phrase, "Do you wanna die?" in Korean-American communities.[80] These inherent shortcomings of monitoring systems risk disproportionately targeting students who are English Language Learners. For more information on legal protections for students who are English Language Learners, see Legal Implications on page ___.

Students with Disabilities. In addition to disproportionate risks of stigmatization and criminalization, students with disabilities may be especially harmed by the ways self-harm monitoring systems analyze student content and writing. Some students with disabilities may interact with online content or use speech differently than their non-disabled peers and may consequently face risks of disproportionate flagging because of the limitations of these systems in interpreting context. Speech that is a manifestation of a disability may be misinterpreted as a threat to self-harm by the monitoring software or by untrained school staff who are unfamiliar with the intersection of disability and mental health. This misinterpretation often occurs with students who have developmental or learning disabilities.[81] School district leaders should be aware that disparate treatment of students with disabilities, including disproportionately and needlessly flagging them due to typical manifestations of their disabilities, can constitute discrimination and invite potential legal challenges under the Americans with Disabilities Act (ADA). For more information on legal anti-discrimination protections for students with disabilities, please see Legal Implications on page 24.

Students of Color and Racial Minorities. In addition to harms stemming from sharing student information with law enforcement and referring mental health-related issues to law enforcement, students of color may disproportionately experience other harms from self-harm monitoring.

For example, natural language processing algorithms, which are used by monitoring systems, have been shown to analyze and interpret Black dialects of English used online less accurately than writing by white individuals online.[82] Likewise, research at MIT shows many common automated tools that scan online content using natural language processing disproportionately flag writing from Black users.[83] These examples demonstrate the technological shortcomings, and inequities, inherent in accurately monitoring online content. Such technological inaccuracies lead to racial disparities in students mistakenly flagged by monitoring systems and can cause students of color to disproportionately experience the harms related to mismanaged and privacy-violative monitoring.

Additionally, low-income youth of color and other vulnerable young people may have a very different relationship with school-based and medical-based systems of formal mental healthcare. These student populations may often look to community-based resources and peer social networks as their preferred sources of care and wellness.[84] While many monitoring technologies proceed from the assumption that school-based systems of care are best positioned to support young people, that may not be the case for many youth. For many students, state-based systems of mental health screenings and services can trigger harmful episodes where they, or their caregivers, have had to deal with the child welfare system, criminal legal system, juvenile justice system, etc.[85]

Box 1. Monitoring Inflicts Particular Harms on Systemically Marginalized Groups of Students

School districts should keep the different needs and preferences of various student groups in mind and recognize that a one-size-fits-all approach to responding to student self harm will not equally benefit all students.

Another important consideration is the effect of high-surveillance schools[86] on the academic outcomes and well-being[87] of Black students and other structurally disadvantaged racial groups. These students may experience monitoring more as a form of surveillance and control of student behavior than as a mental health support tool, due to the greater prevalence of schools with harsh security and zero-tolerance policies in communities of color.[88] In these cases, implementing a monitoring system can add to an atmosphere of surveillance and criminalization, thereby compromising students' sense of comfort and support in their school environment. Research from John Hopkins University and Washington University shows that high surveillance schools can lead to lower test scores and graduation rates for Black students, as well as greater disciplinary disparities.[89]

LGBTQ Students. Besides facing the risks of discipline and criminalization described in Box 2, LGBTQ students face unique additional harms from having their digital activities monitored. These unique harms can be exacerbated depending on students' school and home environments.

Research shows that LGBTQ students who experience victimization or bullying in school face detrimental psychological outcomes, such as higher instances of depression, low self-esteem, increased isolation, and increased suicidal ideation, compared to non-LGBTQ peers.[90] The American Psychological Association has reported[91] that 64 percent of LGBTQ students feel unsafe in schools because of prejudice and harassment. Sixty percent of these students did not report these incidents to school officials due to fear the situation would be made worse or that the school would take no action to help them. Self-harm monitoring technologies that flag incidents of harassment and prejudice may result in these very fears for LGBTQ students, particularly in unsupportive school environments or without thoughtful protocols for handling flags.

LGBTQ students have a unique interest in controlling who has information about their sexual orientation and gender identity to prevent incidents of harassment, particularly in situations of unsafe home or school environments. Nonprofit suicide-prevention organization The Trevor Project reports that about 50 percent of LGBTQ youth selectively and carefully decide which family members and teachers and in which contexts they disclose their sexual orientation or gender identity.[92] In a national survey conducted by The Trevor Project, less than half of LGBTQ youth had disclosed their identity to an adult at school.[93] Research has also found LGBTQ youth are more likely than their peers to seek identity-related resources and help online.[94] Monitoring systems may discourage youth from seeking LGBTQ-affirming resources online if they fear surveillance, repercussions, or reporting or being outed to school staff, other students, or even their parents through the monitoring program.

This ability to decide when and how to come out is a critical right that supports mental well-being, particularly when students are in situations where they may feel unsafe or unsupported. This includes school environments where students do not feel confident that their school leaders would support their identities if they were to report bullying or harassment. Consequently, exposing LGBTQ students as a result of monitoring, even with the good intention to help them, can in fact undermine their mental health and safety by damaging this important protective strategy.

School leaders concerned about the mental health of LGBTQ youth should work to create actively affirming and supportive school climates that respect students' boundaries and privacy, and to provide resources and information in school related to sexual orientation and gender identity, rather than engage in monitoring that would invasively and forcefully expose these students.

Even if schools do not explicitly regard students experiencing mental health challenges as threats or target them for discipline, monitoring can impact students' natural exploration, academic freedom, or ability to find online communities and resources that are important for their well-being and mental health.

The National Association of School Psychologists reports that school surveillance can corrode learning environments by instilling an implicit sense that children are untrustworthy.[95] Many organizations have noted that surveillance technologies such as social media monitoring and facial recognition can harm students by stifling their creativity, individual growth, and speech. The sense that "Big Brother" is always watching can destroy the feelings of safety and support that students need to take intellectual and creative risks—to do the hard work of learning and growing. For example, in one study of Texas high school students whose district monitored their social media accounts, students reported that even if they had nothing to hide, they nonetheless found it chilling to be watched.[96] A recent national survey found that 80 percent of students who were aware of their schools using monitoring software reported being more careful about what they search online because of knowing that they are being monitored.[97]

Who has access to the information identified or flagged, and do they have a legitimate health or educational purpose for accessing it?

Because of the harms that can stem from sharing student information, a key privacy issue involves who can access information about which students have been flagged and the content collected by a self-harm monitoring system. Schools should carefully consider which school staff receive information collected through monitoring technologies and what training and communication is being provided to this staff and limit this access to only those who need it to provide specific mental health-related follow-up and support to the students. Schools must also determine if the information may be lawfully disclosed to these individuals.

Coordination among teachers, parents, administrators, and school-employed mental health professionals regarding identified students could help adults spot warning signs and establish comprehensive support plans for the students. Providing increased attention to students' mental health from qualified individuals may result in better resources and increased care. However, simply having information about students' mental health status, without the skills or capacity to provide specific follow-up or support, could damage teachers' perceptions of the students or negatively affect how the wider school community treats such students. This may be especially true when teachers or school staff receiving this information do not have the training, qualifications, or responsibility for providing mental health-related

... simply having information about students' mental health status, without the skills or capacity to provide specific follow-up or support, can damage teachers' perceptions of the students or negatively affect how the wider school community treats such students.

support to students. Peer-reviewed research demonstrates that teachers do frequently inaccurately identify students as experiencing symptoms of depression and anxiety.[98] As a result, students may experience the sharing of this information as an invasion of their privacy, resulting in feelings of stigmatization and mistrust.

In addition to considering whether school staff are appropriately equipped to provide mental health-related support to students, schools and districts should ensure that any staff with access to the information identified or flagged are trained on the district's internal protocol for appropriately handling student information collected through monitoring. Staff must be trained to understand the sensitivity of the information being collected on students, understand appropriate disclosure and use limitations, and be familiar with how and when to appropriately escalate any concerns. They should also be trained on the myriad privacy and equity concerns that arise when students' online activities are monitored surreptitiously. Finally, staff who may have access to student information collected through monitoring or who may be responsible for following-up with identified students must be

trained on the district's broader mental health policies, including the school's self-harm prevention and suicide intervention protocols.[99]

Schools should also consider the potential risks and harms that can result from sharing information collected from monitoring with students' parents. For example, some monitoring software flags terms related to sexual orientation or gender identity (such as "gay" and "lesbian") as terms that signify potential bullying.[100] If a student is searching for identity-affirming materials and their searches are flagged, what consequences might the student experience if the school shared that information with their parents, to whom the child may not have disclosed these identities? Children in these situations may face serious dangers to their safety and well-being if their home environments are not supportive. More information about this type of harm is presented above in Box 1.

Schools and districts should incorporate processes to appropriately ensure that these types of considerations are factored into how, if at all, parents are notified of flags containing sensitive information and what information collected from monitoring is shared with them. These considerations should fall within a broader approach of similar caution that schools must exercise when sharing flagged information with anyone because of the potential negative effects it may have on the identified student. Significant risks arise any time sensitive student information collected through monitoring is shared with any individual who does not directly need access to the information in order to provide mental health-related support.

How is student information shared with third parties, if at all, and are such disclosures permitted by law?

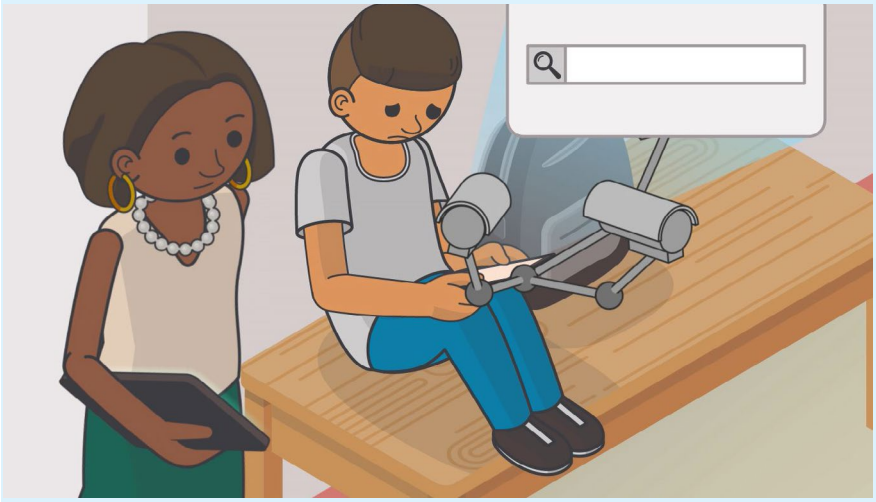
Another key privacy consideration is whether and how schools share student information collected from monitoring programs, including individual students' flagged status, with third parties, such as law enforcement entities, hospitals, or social services providers.

School districts may be inclined to share a student's flagged status or mental health information with law enforcement because of biases and misperceptions that conflate mental health problems with violence, or even because of a lack of school-based mental health resources or expertise.[101] This conflation of mental health disorders with violence may even be directly promoted by monitoring companies themselves; for example, Gaggle's homepage prominently states that "70% of students who plotted school attacks showed signs of mental health issues."[102]

Sharing student information collected through self-harm monitoring with law enforcement is a particular risk when schools monitor students' online activity outside of school hours and school administrators are unavailable to respond to afterhours flags. Although sharing the information collected through monitoring software in this manner may stem from good intentions, underlying social inequities cause certain student groups to likely suffer particular harm when schools share their information with third parties or unduly refer them to law enforcement. Monitoring technology itself may not cause the systemic biases that lead particular student groups to experience harm when they are referred to law enforcement. However, school districts must recognize that having a monitoring provider generate law enforcement referrals for self-harm flags can criminalize normal adolescent behavior and subject students to these systemic biases.[103] School officials and education leaders must exercise utmost caution to not exacerbate existing systemic injustices for their students through their choice of monitoring provider—undermining the original goal of improving student well-being rather than endanger it.

While harms may also occur from sharing student information with other third parties such as contracted mental health personnel or local psychiatric facilities,[104] law enforcement is often the most common third party presence on school campuses, and existing societal inequities make sharing of student information with law enforcement particularly risky for many student groups (see Box 2 discussing vulnerable students and law enforcement).

Box 2. Intersections with Mental Health: Vulnerable students are likely to face disproportionate criminalization and harm from referral to law enforcement



In many cases, law enforcement officers, including school resource officers (SROs), are more common resources than counselors or school psychologists on school campuses. In 2019, the American Civil Liberties Union found that almost two million students attend schools with police officers but no counselors, three million attend schools with police officers but no school nurses, six million are in schools with police officers but no school psychologists, and ten million are in schools with police officers but no school social workers.[105] In such contexts, schools may be more likely to frame and treat mental health needs as threats or disciplinary issues for law enforcement to handle, simply because they may lack access to school employed mental health professionals.

For example, in some states, police officers, including SROs, are statutorily authorized to submit students to involuntary psychiatric examinations.[106] A study by civil rights groups in Florida found that schools routinely refer "school children who make jokes, act out, exhibit normal manifestations of a known disability, or express ordinary sadness" for police-initiated psychiatric confinement, rather than connecting them to long-term, community-based care.[107] This practice takes children away from their families without their consent, confines them in a psychiatric facility alone, and may lead to "devastating results, including trauma and abuse, for these children, as young as 6."[108] Florida is unfortunately not unique in over-involving law enforcement in issues related to student mental health to the detriment of students.[109]

In addition to creating stigma, this approach of framing potential mental health needs as a disciplinary problem to be handled by law enforcement often prevents students from receiving necessary medical treatment and unnecessarily entangles them in the criminal justice system. Needlessly referring students who may benefit from mental health services to law enforcement instead furthers existing inequities and perpetuates the school-to-prison pipeline.

This means student groups who are already marginalized and vulnerable are the ones most likely to be flagged by monitoring systems, seen as at-risk or dangerous by school staff, disproportionately referred to law enforcement, and most likely to be harmed by this referral. Students who are minoritized or marginalized in terms of race/ethnicity, disability, sexual orientation, gender identity, gender expression, or socioeconomic status are known to be disproportionately criminalized in this way and, in turn, are most likely to suffer additional harm if monitoring technologies lead to contact with law enforcement rather than mental health support.[110] As discussed above, students who are English Language Learners or immigrants may be more likely to be mistakenly flagged by monitoring systems due to mistranslations or lack of cultural context. When this occurs, their safety or residency may be endangered through law enforcement contact.

Box 2. Intersections with Mental Health: Vulnerable students are likely to face disproportionate criminalization and harm from referral to law enforcement

Black students and other students of color are especially harmed by disciplinary actions and law enforcement interactions:

- Black students are suspended and expelled from school at three times the rate of their white peers.[111]
- Approximately one-third of all students arrested at school are Black, despite only comprising 16 percent of the nation's student population.[112]
- Black children are more than 5 times more likely to be detained or incarcerated than white children.[113]
- Native American and Native Hawaiian/Pacific Islander students are arrested in school at 2 times the rate of white students.[114]
- Black and Latino boys with disabilities comprise 3 percent of all students but 12 percent of all school arrests.[115]
- Native American girls are arrested in school 3.5 times more than white girls.[116]

Harsh exclusionary discipline, criminalization, and law enforcement interactions already disproportionately harm students with disabilities, as schools often mistakenly view them as threats.

- Children with learning and behavioral disabilities are arrested nearly three times more often than other students.[117]
- Children with disabilities comprise up to 85 percent of youth in juvenile detention centers,[118] while only 37 percent of them receive educational accommodations and services for their disability in school.[119]
- Students with disabilities are suspended from school approximately twice as often as students without disabilities.[120]
- A quarter of all children arrested at school are children with disabilities.[121]

LGBTQ students are already disproportionately criminalized and at risk of negative law enforcement interactions; referrals from monitoring programs to SROs and other law enforcement could increase this existing harm. LGBTQ students flagged through monitoring may face more likely referral to law enforcement, compared to non-LGBTQ students. Researchers have estimated 20 percent of youth involved in the juvenile justice system are LGBTQ, compared to 4–6 percent of youth in the general population[122]

Does the school district have a plan for providing transparent communication with parents and students, and how have they ensured that the communication plan meets the needs of their community?

Transparency is an essential part of any data initiative. If families and students are unaware of the self-harm monitoring program, schools risk losing their communities' trust and undermining the goals of their initiative. For example, if a student is flagged when their "mental health problems workbook" includes the word "suicidal," it may feel like a violation of the confidential relationship between that student and the counselor or therapist who assigned them that workbook.[123]

If school districts choose to adopt monitoring technology, they must do so transparently, in consultation with experts and community

stakeholders, and focus on narrow and straightforward indicators of imminent self-harm. Schools should clearly inform families and students how their online activities are monitored and ensure they know the potential in-school or out-of-school consequences of being flagged. Some monitoring companies have proactively enabled by-default transparency measures—for example, an icon that shows up near the top of a student's browser when they are being monitored—that can assist schools in providing this transparency.[124]

Schools and districts considering implementing a self-harm monitoring program should ensure families, students, and appropriate school staff understand how the technology works, the internal processes in place to respond to flagged material, which school staff have access to the information collected, and any opportunities students and parents may have for redress in the event of mistaken flags or harmful impacts of being flagged. In particular, when a student is flagged, they and their families deserve access to the information used to make that decision, as well as an opportunity to dispute it. Such proactive communication and transparency will allow students to make more informed decisions about how they use school devices in light of their school's monitoring policies and will allow students and their parents greater agency in mitigating risks and harms related to being flagged. In fact, some state legislatures have recognized the importance of community engagement around monitoring systems. In California, there is a legal requirement that school districts notify parents and hold a hearing before they can engage in a program to monitor student social media, even if student profiles are public.[125]

Finally, before implementing a self-harm monitoring program, schools and districts should ensure that their community has had a meaningful opportunity to provide input, raise concerns, and share their perspectives on the program. School leaders and administrators should consider students and their families as equal partners in selecting, vetting, and developing a self-harm monitoring program prior to implementation.

Box 3: Spotlight on COVID-19: Additional Considerations and Barriers to Effectiveness During Remote Learning

Context increasingly matters, as the COVID-19 pandemic and resulting shift to remote learning have placed both physical and emotional distance between students, educators, and other school staff. Many schools have turned to self-harm and suicide monitoring technologies in an attempt to fill any potential rifts created by remote learning[126] and in response to growing concern about the impact of the pandemic on student mental health.[127] For example, the number of users of the provider GoGuardian (across all its monitoring services, not just its self-harm monitoring product) has rapidly expanded by 60 percent during the pandemic[128] and it is now used by 23 of the 25 largest school districts in the country.[129] Some reports have suggested that this expanded monitoring is necessary, as educators may have felt better equipped to understand when a student required mental health assistance and intervene by using in-person cues, such as a student's demeanor and appearance, and may struggle to understand when their students may need help as they learn remotely.[130]

In reality, it is difficult to trace how precisely the pandemic has impacted student mental health.[131] Some students' mental health may have declined during the pandemic due to combined factors such as the pressures of isolation, the stress and challenges of trying to learn without direct access to teachers in person, anxiety about the pandemic generally, technology problems, COVID-related loss and illness in the family, and unstable home environments.[132] Regardless, these increased mental health-related concerns must be balanced with protecting student privacy.

Some well-meaning school administrators may consider these increased pandemic-related stressors as all the more reason to instate self-harm monitoring technology, regardless of whether teachers were previously able to pick up on in-person signs of mental health crisis accurately. However, it is important for school administrators to remember that self-harm monitoring technology is not evidence-based, and its implementation in the absence of privacy-protective practices and thoughtful implementation policies can in fact harm students, regardless of any greater mental health needs during the pandemic. School administrators should remember that these technologies should only be deployed as part of a multi-pronged program of well-developed mental health supports.

In addition to understanding the privacy and equity risks, school and district leaders should also be aware of the many practical challenges involved in implementing self-harm monitoring. As discussed above, the efficacy of monitoring technologies for reducing self-harm has not been fully evaluated and the technologies have not been substantiated by mental health professionals or clinicians as an effective tool for addressing mental health crises.

Beyond questions about the initial accuracy of identifying students in need of support, there are practical challenges to this identification actually leading to the students receiving support, including the widespread lack of qualified mental health personnel in schools. Flagging at-risk students can only be useful if effective follow-up plans and mental health resources are in place for the identified students.

Legal Considerations for School Districts

In addition to understanding privacy and equity impacts, schools should be aware of important legal implications associated with adopting monitoring technologies and collecting student information related to mental health and potential to self-harm. In addition to CIPA (see p. __), there are several federal laws and protections that may influence how school districts can implement self-harm monitoring programs, manage the student information collected through such programs, and interact with students identified through self-harm monitoring. Additional state laws may apply as well. Schools should be aware of federal and state regulations that may apply to student information collected through student monitoring technologies and weigh these legal implications when deciding whether to adopt monitoring programs. Schools should be sure to consider:

- **FERPA and Student Privacy.** The Family Educational Rights and Privacy Act (FERPA) is the main federal privacy law that applies to student information. In addition to requiring schools to safeguard student data and restricting the parties to whom schools can disclose personal information from student's education records without parental consent, FERPA affords students and their caregivers or parents certain rights regarding their information. Parents and caregivers have the right to access and correct their children's education records, and this right transfers to students when they reach the age of 18 or enroll in postsecondary school. Generally, FERPA protections, including limitations on disclosure of student information, apply to information gathered via self-harm monitoring technology. If parents submit a FERPA request for information collected and maintained via self-harm monitoring technology, the law would very likely require schools to provide the parent with the opportunity to inspect that information.
- **ADA and Section 504 Disability Discrimination.** The Americans with Disabilities Act (ADA) is a comprehensive non-discrimination law that provides civil rights protections in all areas of public life

to all individuals with disabilities. Likewise, Section 504 of the Rehabilitation Act provides civil rights protections to all individuals with disabilities in institutions that receive federal funding, which applies to most public schools.[133] Both the ADA and Section 504 define disability broadly as a physical or mental impairment that substantially limits one or more major life activities, a record of such an impairment, or being regarded as having such an impairment.[134] This means that under these two laws, mental illness is considered a disability, and disability discrimination includes differential treatment arising from the perception of someone having a mental illness, regardless of actual diagnosis.[135] This is important information for schools to consider. All children flagged as at risk for self-harm are, by definition, perceived by their school as having a mental health disability that impedes their safety, and are receiving differential treatment accordingly. As a result, school districts should be aware that two different disability-related protections may be triggered when a school flags a student as at risk for self-harm due to potential mental health problems. One is privacy protections that the ADA provides regarding disclosure of a perceived disability/mental health condition; the other is non-discrimination protections for these students under both laws. School districts should carefully consult with their legal counsel around disability protections and examine their follow-up practices to ensure they do not treat students flagged through monitoring in discriminatory ways.[136]

- **Fourth Amendment Considerations**. Whether monitoring students' use of school-issued devices and services at home constitutes an unreasonable search or seizure under the Fourth Amendment remains an open question. The Fourth Amendment implications are also exacerbated when many of the monitoring flags occur outside of school hours. In Minneapolis Public Schools, for example, approximately three quarters of incidents that the district's monitoring system reported to school officials took place outside of school hours.[137] In a recent survey of teachers whose schools use monitoring software, only 25 percent reported that monitoring is limited solely to school hours

...there are several federal laws and protections that may influence how school districts can implement self-harm monitoring programs, manage the student information collected through such programs, and interact with students identified through self-harm monitoring.

and 30 percent reported that their school monitors students all of the time.[138] As yet, no Supreme Court jurisprudence has addressed the question of whether monitoring students online while they are at home (whether they use a personal or school-owned device or whether they are connected to their personal or school-provided network) constitutes a Fourth Amendment violation.[139] This is especially important during the COVID-19 pandemic; in most cases, students are engaging in their virtual classrooms from the privacy of their homes. Schools and districts should keep in mind the unique sensitivities that arise when monitoring students while they are off campus or learning from home.

- **Title VI**. Schools should be aware that monitoring students' online behavior could possibly implicate Title VI considerations. Title VI of the Civil Rights Act of 1964 prohibits discrimination on the basis of race, color, or national origin in any program or activity that receives Federal funds or other Federal financial assistance, which includes all public schools.[140] The use of these protected characteristics or close proxies of these protected characteristics (such as English Language Learner status) in monitoring

or profile-building could thus be a trigger for potential anti-discrimination concerns, particularly if students who are racial or ethnic minorities are disproportionately flagged by school's monitoring systems or receive disparate treatment as a result.

- **Other Legal Protections for English Language Learners**. Several laws protect the rights of English Language Learners. The Equal Educational Opportunities Act (EEOA) of 1974 prohibits discrimination against students. It also requires school districts and states' departments of education to take action to ensure equal participation for everyone, including removing language barriers for ELL students. Additionally, the Every Student Succeeds Act (ESSA) of 2015 authorizes the U.S. Department of Education to award grants to state education departments, which may issue them as subgrants to K–12 school districts. The subgrants are intended to go toward improving ELL students' instruction and abilities to meet state academic content and achievement standards. By accepting these federal funds, districts are required to provide language accommodations to non-English-speaking families. The Supreme Court case of *Plyler v. Doe* also provides protections and rights for students who are English Language Learners in schools.[141]

- **Title IX**. Schools should also be aware that monitoring students' online behavior could also potentially implicate Title IX considerations if monitoring has the effect of exposing the sexual orientation and gender identity of students in harmful, discriminatory, or disparate ways. Title IX of the Education Amendments of 1972 states that "No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving Federal financial assistance."[142] A recent Supreme Court decision, *Bostock v. Clayton County*, held that Title IX also encompasses discrimination based on sexual orientation.[143] As some monitoring systems and schools may include words or phrases related to sexual orientation or gender identity[144] that trigger alerts to school officials, that screening may implicate direct or proxy characteristics for protected classes under Title IX.

Recommendations for School Districts: How to Reduce Risks, Ensure Equity, and Protect Student Privacy when Implementing Self-Harm Monitoring Programs

As schools and districts attempt to protect students amid the strains of the pandemic on student well-being, education stakeholders should remember that privacy protections can enhance mental health support programs by encouraging students to feel they can safely ask adults for help because they know that the information shared will remain confidential. Before adopting monitoring technology, schools and districts should understand key facts about how the technology works, how its implementation may impact students with mental health needs or disabilities, and how to prioritize student privacy within their programs.

To foster a healthy school environment that strives to ensure students' mental well-being, schools must ensure that students and their communities support using monitoring systems for this purpose and are aware of how the program affects them and their associated rights. To create self-harm monitoring programs with those protections, schools and districts can take the following steps:

Education stakeholders should remember that privacy protections can enhance mental health support programs by encouraging students to feel they can safely ask adults for help because they know that the information shared will remain confidential....

- Develop a firm understanding of community values surrounding mental health, self harm, and monitoring by creating a dialogue with the school community *prior to adopting any monitoring program*. If a monitoring system has already been adopted without seeking input from students and families, school leaders

should begin to convene regular opportunities for student and family feedback on the district's monitoring policies, solicit community input on a regular basis as they periodically review the monitoring policy, and incorporate this input in periodic updates to the policy. If students and families are not aware of how and why they are being monitored, self-harm monitoring will feel like an administrative overstep and breach of trust. Students and families will be most affected by any self-harm monitoring program and should accordingly be centered and involved in developing their school district's monitoring plans and processes. Efforts to include the school community will help build trust, support, and transparency. This will ultimately increase student well-being and safety.

- Create trust among students and families by providing transparency about monitoring programs and practices. When considering online monitoring programs, schools should clearly define and communicate which information and activities the programs will track and why, who will have access to the information collected, how that information will be used, and how long it will be stored.
- School and district leaders should ensure that all school personnel understand student data privacy as a fundamental right, including in the context of self-harm monitoring programs. Districts should ensure that all educators know the requirements of FERPA, particularly its rules on sharing student information in health or safety emergencies.
- To fully protect student privacy, schools should do more than simply comply with the law; they should also establish careful privacy protocols and practices to build trust with their stakeholders and communities. In particular, districts and schools should consider incorporating the Principles for School Safety, Privacy, and Equity into their safety policies. Written by 40 education, privacy, disability rights, and civil rights organizations, these ten principles are designed to protect students' privacy, dignity, and right to an equal education. Several of the principles directly address issues relevant to mental health needs, such as the need to focus on prevention; to use monitoring programs that encourage evidence-based rather than knee-jerk responses; to use programs that include appropriate privacy protections; to provide mental health and behavioral services; and to avoid discriminatory practices and unnecessary involvement of law enforcement.

Before implementing self-harm monitoring programs, school district leaders need to consider many privacy, equity, and practical concerns. The extent to which such technology can filter and monitor students' online lives raises critical questions about students' rights to privacy and how much schools should access students' personal information. Scanning and monitoring all website activity, documents, searches, social media, emails, and online chats can make students feel excessively surveilled by their school, while inappropriately sharing and responding to student information collected from self-harm monitoring can put students' well-being at risk. Individual districts and states can and should set their own policies of whether and how to monitor students. However, privacy guardrails must be drawn so students and families can be reassured that their rights will be protected. It is imperative that school districts approach any self-harm monitoring system holistically, taking into account the totality of harms that could arise from hastily adopting technology without well-developed implementation policies and the necessary accompanying school-based mental health resources.

APPENDICES

The following appendices provide recommendations and resources for school districts to reference as they grapple with the difficult questions surrounding the use of monitoring.

APPENDIX A:
Key Questions School Districts Should Ask Monitoring Vendors Before Adopting a Monitoring Program

If school and district leaders are considering adopting self-harm monitoring software, we recommend they ask the software vendors the following key questions:

- **Can the vendor demonstrate the efficacy of its product?** Vendors of self-harm monitoring systems claim that their programs can prevent children from harming themselves.[145] What is the rate of false positives? What independent evaluations have they employed? What is the science and research behind their product? A best practice is for vendors to have their products evaluated by a third party to verify their claims about what the products can do. Otherwise, it will be difficult to know whether the product is an appropriate choice to help detect student self-harm and a worthy investment for schools.
- **How does the monitoring system generate and send alerts? Who is alerted?** What criteria is used to determine when students should be flagged? What control does the school have over this criteria? Does the monitoring company use an automated system to send alerts to school officials whenever a student has been flagged? Are there personnel in the monitoring company that review flagged material prior to initiating alerts about the student in question? If the software determines that someone is an imminent threat, there should be an established process for alerting the school. Who is designated to receive alert notifications? Is it more than one person? What are the qualifications for those notified? How are escalations handled? Are parents notified? Under what, if any, circumstances will law enforcement be notified?
- **What content does the monitoring system review?** Different monitoring systems can access and review a variety of materials, ranging from web searches to emails but also chats, collaborative documents, and social media. What content does the technology access? Is this content necessary, appropriate, and useful for the school to scan? Is content scanned 24-7, or is it only scanned during school hours? Is content only scanned on school devices, or also on personal devices if students are logged into their school accounts at home?
- **How long does the vendor and the school retain the data?** Schools should know whether vendors delete students' data immediately after an incident is acknowledged, annually, after students graduate, or at a specified point thereafter. Sometimes, self-harm monitoring companies want to use the data to improve their algorithms. However, schools should ask and know how long the information remains identifiable and traceable to students. Similarly, school districts should develop retention and deletion schedules for the student information they receive through self-harm monitoring and plan to delete information on a regular basis.
- **If a system uses keywords and categories to provide alerts, are they appropriate and useful for the purpose of self-harm monitoring?** It is important to consider whether the software's goals align with those of the school and community. If vendors extend their keywords to include terms related to sexual orientation or gender identity, for example, what is their reason for doing so? How is this flag relevant for detecting risks of self harm? Flagging such keywords can accidentally expose a student who is not ready or safe to disclose such information, without serving the goal of monitoring for mental health crises. Furthermore, will the software send an alert if a student simply posts a word such as "sad" or uses profanity? Schools should remember

APPENDIX A

that their goal is to keep students safe from self-harm and should refrain from tracking and flagging sensitive topics that have nothing to do with children's safety and mental health.

- **How does the monitoring system recognize context?** Monitoring systems cannot understand all the context and slang of different age groups from various communities across the nation. How will a system know whether a word is part of a song lyric or whether students are simply joking? Does the system process and rule out irrelevant flags, or are all flags forwarded to the school for evaluation? Does the school have the ability to adjust the alerts, for example alerting on self harm, but not profanity? Since these alerts could trigger serious consequences, it is important that vendors broadly examine the context of a post rather than simply flagging keywords. Likewise, schools should take into account and examine these processes when deciding whether to adopt a monitoring system and selecting a vendor.
- **How does the vendor process student content in non-English languages?** In many communities across the nation, some students and families are not fluent English speakers, may speak English as a second language, or speak multiple languages. It is impossible for vendors to have accurate translation software for all languages. In these cases, vendors must refrain from flagging content in non-English languages if the vendors and schools do not have personnel who are professionally fluent in those languages and can accurately assess whether the content represents a risk. This practice ensures that monitoring systems do not falsely target student content in non-English languages as a result of mistranslations and do not needlessly subject such students to the potential risks and harms associated with being flagged. Schools and vendors must ensure the trust and safety of the entire community by ensuring the monitoring system does not unfairly target students simply for speaking other languages.
- **How does the monitoring system interpret pictures?** It is possible that students could share posts in the form of a picture or video. In these cases, will the system also review student content that is not text-based? How will the system determine whether the content is threatening self-harm? Will students' pictures or videos be shared with personnel at the monitoring company if they are flagged? Will they be shared with school personnel?
- **Does the monitoring system match students with their schools on social media, and if so, how?** There are several ways that vendors can match students to particular school districts. For example, they can identify the users who follow a school's social media account and then identify the friends of those users. Another method is geofencing, defined as a virtual boundary around a real-life geographical area. Applied to self-harm monitoring, geofencing allows vendors to know which students attend certain schools by identifying active accounts on school grounds. For both these methods, schools should understand whether and how the vendor gathers information from private accounts and clearly communicate these practices to students and families. Before engaging with vendors that track student social media or use geofencing, schools should determine whether their community is comfortable with these forms of self-harm monitoring.
- **When, if ever, does the vendor turn over data to law enforcement?** Special provisions under FERPA limit which sort of information schools can forward to law enforcement and under what circumstances. For example, under FERPA, an education vendor may share FERPA-protected data with law enforcement in order to comply with a subpoena or court order, but the school must first make reasonable efforts to notify the parent prior to sharing the data. School districts should read vendors' terms of service closely to ensure that vendors do not have the authority to independently mark a situation as an emergency and turn monitoring information over to law enforcement without school involvement.

APPENDIX B:
Checklist for School Districts Developing Monitoring Plans and Policies

Before adopting any monitoring technology, school officials and policymakers should ensure they have a thoughtful policies surrounding the use of this technology that prevents unintended privacy violations, centers equity for all students, and clearly regulates the follow-up practices when students are flagged by the software.

School officials should ensure their monitoring plan and associated mental health policies:

- ✔ are based on tools and methods that have been independently validated and endorsed by mental health researchers and professionals, based on robust peer-reviewed and published medical evidence.
- ✔ are based on a needs assessment that defines specific, clear goals for adopting a monitoring system and establishes the need that the monitoring system will fulfill.
- ✔ are developed within the framework of existing school-based mental health resources and professionals (school psychologists, counselors, and social workers) that are able to provide support to any students who may be identified.
- ✔ have been transparently developed in consultation with experts and community stakeholders, particularly families, students, and teachers.
- ✔ have clear policies on which data are collected, who has access to them, how they will be used, and when they will be destroyed.
- ✔ have clear policies on how to act upon data collected via student monitoring.
- ✔ have clear policies on how school staff will review student information flagged by monitoring and who determines whether a flag is indicative of a true risk of self harm.
- ✔ have clear follow-up policies on how school staff will respond to monitoring flags that they do deem indicative of a true risk of self harm and how they will respond to flagged information that they determine is innocuous.
- ✔ have clear policies on sharing data, particularly limitations on sharing with school resource officers, law enforcement, and administration beyond the school level.
- ✔ make all of the policies easily available and accessible to students and parents in the Student Handbook/ Code of Conduct and on the school website, and available in multiple languages.
- ✔ are transparent and understandable to school staff, families, and students.
- ✔ include a robust training program for school officials responsible for handling sensitive student data.
- ✔ have policies, including clear consequences, for individuals who violate data protection and sharing protocols.
- ✔ do not stigmatize or reinforce biases against any groups of students based on race, religion, gender, disability status, sexual orientation, or other legally protected characteristics.
- ✔ provide opportunities for recourse for students identified as a threat or at risk of self-harm, including access to the information used to identify them and an opportunity to dispute findings.
- ✔ are compliant with all federal and state laws and protections, including FERPA, the ADA, Section 504, Title VI, and Title IX.
- ✔ are reviewed regularly to verify that it protects student safety and to ensure that unnecessary surveillance is discontinued.
- ✔ are reviewed prior to adoption and periodically after adoption to audit for civil rights and privacy rights compliance.

APPENDIX C:
Other Resources for Schools Developing Policies on Monitoring

School districts and education leaders may find the following resources helpful as they consider adopting a monitoring system and work to develop well-crafted, rigorous privacy and equity protections as part of a comprehensive implementation plan.

Future of Privacy (FPF) Resources:

- **School Safety & Privacy: An Animated Introduction.**
  This short video explores some technologies that schools use or are considering, privacy harms that can result from surveillance, and basic steps to help districts safeguard students' privacy.
- **Principles for School Safety, Privacy, and Equity.**
  Written by 40 education, privacy, disability rights, and civil rights organizations, these principals are designed to protect students' privacy, dignity, and right to an equal education.
- **Ensuring School Safety While Also Protecting Privacy.**
  This blog post highlights key recommendations from FPF's testimony before the Federal Commission on Student Safety.
- **Reopening Schools Issue Brief: Online Monitoring & COVID-19.**
  This brief covers the issues surrounding online monitoring during the COVID-19 pandemic.
- **Student Privacy and Special Education: An Educator's Guide During and After COVID-19.**
  Co-written by FPF and the National Center for Learning Disabilities, this report serves as a guide for educators in navigating the legal and ethical best practices for students both during the COVID-19 pandemic and beyond.
- **The Privacy Expert's Guide to Artificial Intelligence and Machine Learning.**
  This report is an introductory guide to understanding the basics of artificial intelligence and machine learning as they relate to privacy.
- **Surveillance Won't Save Our Kids, Humane Public Policy Can.**
  This blog outlines arguments against surveillance in schools, followed by alternative policy approaches.
- **A Closer Look: Network Monitoring.**
  This brief covers the issue of network monitoring in schools, supplemented by both FPF and external resources.
- **School Safety Measures Must Have Evidence, Be Specific, & Have Privacy and Equity Guardrails.**
  This brief discusses the balance between managing school safety and student privacy in schools in a way that minimizes student harm.
- **The Student Privacy Communications Toolkit** provides resources for school districts developing their student privacy approaches.

APPENDIX C

Other Resources:

- **School Surveillance: The Consequences for Equity and Privacy.**
  This publication by the National Association of State Boards of Education recommends key privacy principles in the context of surveillance technologies, including minimization, proportionality, transparency, openness, empowerment, equity, and training.
- **BluePrints for Healthy Youth Development.**
  Provides a comprehensive registry of scientifically proven and scalable evidence-based interventions to promote youth development and health, including mental health. School and education leaders can refer to the BluePrints program search to find evidence-based and independently validated strategies for preventing student self-harm and improving student mental health.
- **Children and the Internet: Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries.**
  This resource by the National Conference of State Legislatures gives a description of all the state laws that govern children's use of the Internet.
- **Fencing Out Knowledge.**
  This report by the American Library Association details findings that schools and libraries nationwide are filtering out more of the Internet than what is necessary by law.
- **Student Surveillance, Racial Inequalities, and Implicit Racial Bias.**
  This journal article by Jason P. Nance discusses the implications of student surveillance on perpetuating racial inequalities in schools.
- **Mixed Messages? The Limits of Automated Social Media Content Analysis.**
  This report by the Center for Democracy and Technology discusses the limitations of social media analysis, with recommendations for policymakers on how to govern the use of these tools.
- **Under Digital Surveillance: How American Schools Spy on Millions of Kids.**
  This piece by *The Guardian* unpacks the prevalence of surveillance in schools and how this could negatively impact students' success.
- **Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming.**
  This piece in *Education Week* discusses the use and potential avenues for abuse of surveillance systems in schools.
- **Student Privacy in Massachusetts K-12 Schools.**
  This report by the ACLU of Massachusetts outlines best practices and recommendations for Massachusetts public schools to balance technology use with student privacy.
- **Smart Investments for Safer Schools.**
  This piece by the Center for American Progress outlines previous responses to bolster school safety and how certain initiatives, while well intentioned, are not always in the best interest of students.
- **SAMHSA's Evidence-Based Practices Resource Center.**
  The Substance Abuse and Mental Health Services Administration provides resources that schools may use to seek evidence-based strategies to address student mental health issues.

APPENDIX C

- **Mixed Messages? The Limits of Automated Social Media Content Analysis.**
  To understand the practical limitations of social media monitoring technology, schools and districts can consult the Center for Democracy & Technology report, which comprehensively examines the limitations of social media content analysis, lists questions to help organizations evaluate tools, and offers recommendations.
- **Healthy People 2020 Data.**
  Having an adult that a youth or child can talk to is part of Healthy People 2020, which outlines the U.S. government's national health goals.
- **Best Practices for Serving LGBTQ Students.**
  This report and toolkit by Learning for Justice provides best practices for educators to ensure that school policies support the mental health and well-being of LGBTQ students, and provides recommendations school leaders can follow to ensure use of a monitoring system does not inadvertently expose LGBTQ students to harm. Ensuring an inclusive and safe school climate for LGBTQ students helps reduce and prevent mental health challenges for this vulnerable group of students without relying on invasive monitoring.
- **Developing Policy to Prevent Youth Suicide.**
  This policy brief by the National Association of State Boards of Education provides guidance for education leaders developing model student suicide prevention policies.
- **Student Activity Monitoring Software: Research Insights and Recommendations.**
  The Center of Democracy & Technology (CDT) performed a survey of teachers, parents, and students about their experiences with, and attitudes toward, monitoring software.
- **Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software.**
  CDT interviewed nine individuals from five local education agencies about how schools could address privacy concerns arising from the use of monitoring software.

ENDNOTES

1 Rhitu Chatterjee, *Child Psychiatrists Warn That The Pandemic May Be Driving Up Kids' Suicide Risk*, KQED (February 2, 2021), Accessed February 8, 2021, https://www.kqed.org/mindshift/57343/child-psychiatrists-warn-that-the-pandemic-may-be-driving-up-kids-suicide-risk; Stephanie L. Mayne, Chloe Hannan, Molly Davis, Jami F. Young, Mary Kate Kelly, Maura Powell, George Dalembert, Katie E. McPeak, Brian P. Jenssen and Alexander G. Fiks, *COVID-19 and Adolescent Depression and Suicide Risk Screening Outcomes*, Pediatrics (2021), 148(3).

2 Aaron Leibowitz, *Could Monitoring Students on Social Media Stop the Next School Shooting?,* The New York Times, (September 6, 2018), Accessed December 17, 2019, https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html..

3 For the purposes of this report, we use the term "parent" expansively to also imply other legal guardians or caregivers that students may have.

4 ALCU, *Cops and No Counselors: How the Lack of Mental Health Staff is Harming Students,* (2019), Accessed September 20, 2021, https://www.aclu.org/sites/default/files/field_document/030419-acluschooldisciplinereport.pdf.

5 Jacqueline Ryan Vickery, *"I don't have anything to hide, but…" The Challenges and negotiations of social and mobile media privacy for non-dominant youth*, Journal of Information Communication, and Society (2014), 18: 281–294.

6 Erica L. Green, *Surge of Student Suicides Pushes Las Vegas Schools to Reopen,* The New York Times, (January 24, 2021), Accessed February 4, 2021 https://www.nytimes.com/2021/01/24/us/politics/student-suicides-nevada-coronavirus.html

7 US Department of Education Office of Educational Technology, *Power up and bring your own device,* DOE, (n.d.), Accessed July 27, 2021, https://tech.ed.gov/stories/power-up-and-bring-your-own-device/.

8 Caroline Knorr, *What to Ask When Your Kid Brings Home a School-Issued Laptop,* Common Sense Media, (August 26, 2019), Accessed July 27, 2021, https://www.commonsensemedia.org/blog/what-to-ask-when-your-kid-brings-home-a-school-issued-laptop

9 Sean Cavanagh, *School Districts Using Mobile Hotspots to Help Students Connect at Home,* EdWeek Market Brief, (February 14, 2014), Accessed July 27, 2021, https://marketbrief.edweek.org/marketplace-k- 12/school_districts_help_students_connect_outside_classroom_with_portable_wi-fi/.

10 Mark Keierleber, *Minneapolis School District Addresses Parent Outrage Over New Digital Surveillance Tool as Students Learn Remotely*, The 74, (October 28, 2020), Accessed June 7, 2021, https://www.the74million.org/minneapolis-school-district-addresses-parent-outrage-over-new-digital-surveillance-tool-as-students-learn-remotely/.

11 FCC, *FCC Announces Over $5 Billion in Funding Requests Received in Emergency Connectivity Fund Program*, (August 25, 2021), Accessed August 25, 2021, https://docs.fcc.gov/public/attachments/DOC-375210A1.pdf.

12 Techcrunch, *Another banner quarter as Chromebook shipments grow 75% YOY*, Brian Heater, Accessed September 21st, 2021, https://techcrunch.com/2021/07/29/another-banner-quarter-as-chromebook-shipments-grow-75-yoy/.

13 Bark's chief parenting officer said in The Guardian in 2019 that, "'Some parents want technology that will give them an exact record of every single text, every single email…[But Bark doesn't offer that.] We only alert parents and schools when there is a real issue that they need to know about.'" Lois Beckett, *Under digital surveillance: how American schools spy on millions of kids*, The Guardian, (October 22, 2019) Accessed September 20, 2021, https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle..

14 Florida House of Representatives, *HB 3217 (2021) - K-12 Suicide Prevention & Mental Health Early Notification Pilot Program*, (February 4, 2021), Accessed June 20, 2021, https://www.myfloridahouse.gov/Sections/Bills/billsdetail.aspx?BillId=71455.

15 NCASA, *NCGA Passes "Coronavirus Relief Act 3.0" Providing Additional COVID-19 Funding and Policy Relief For K12 Schools*, Accessed September 21, 2021, https://www.ncasa.net/cms/lib/NC02219226/Centricity/ModuleInstance/9/REVISED_H1105%20Summary%20Article_rev.pdf.

16 Edward Burch, *Wilson County Schools using technology to help at-risk students,* WSMV News4 Nashville, (February 12, 2019), Accessed December 17, 2019, https://www.wsmv.com/news/wilson-county-schools-using-technology-to-help-at-risk-students/article_8b608058-2f0d-11e9-9b46-df5432650424.html.

17 LightSpeed Systems, *K-12 Solutions Catalog*, (2021), Accessed September 20, 2021, https://s3.amazonaws.com/files.lightspeedsystems.com/collateral/K-12%20Solutions%20Catalog%202021%20%281%29.pdf (Lightspeed also has the related product "Lightspeed Alert," which "scans virtually everywhere students interact online for indicators of suicide, self-harm, and school violence").

18 Tiffany Lane, *Young student's suicide attempt shows reality of mental health crisis amid pandemic*, KSNV, (November 12, 2020), Accessed September 20, 2021, https://local12.com/news/nation-world/young-students-suicide-attempt-shows-reality-of-mental-health-crisis-amid-pandemic-11-12-2020.

19 Anya Kamenetz, *Software Flags 'Suicidal' Students, Presenting Privacy Dilemma,* National Public Radio, (March 28, 2016), Accessed December 17, 2019, https://www.npr.org/sections/ed/2016/03/28/470840270/when-school-installed-software-stops-a-suicide.

20 Specifically, CIPA requires that schools adopt an internet safety policy that must "include monitoring the online activities of minors."

21 47 U.S.C. § 254.

22 *How does Auditor work*, Accessed September 21, 2021, https://support.securly.com/hc/en-us/articles/115015796427-How-does-Auditor-work

23 Lois Beckett, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, The Guardian, (October 22, 2019) Accessed September 20, 2021, https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

24 "Securly…offers a free app for parents in the districts that use its technology that allows them to see exactly what websites their children have visited, what Google searches they have made, and what videos they are watching on YouTube, Jolley, Securly's safety director, said… [Gaggle's spokesperson said that the company's] bright line was offering monitoring of only students' official school emails and school documents. 'We shouldn't be looking at their private email. We shouldn't be looking at their private social media posts. But in the school, with school-issued tools, we should protect them.'" Lois Beckett, Under Digital Surveillance: How American Schools Spy on Millions of Kids, The Guardian (Oct. 22, 2019), Accessed September 20, 2021, https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

ENDNOTES

In marketing material, Lightspeed Systems, which offers web filtering and a specific self-harm and threat monitoring tool, claims that "Our patented device-level filtration creates more comprehensive cross-device security compared to the web crawlers deployed by competing solutions, and allows for visibility into all online activity, from web searches to activity in Google docs to web-based email." LightSpeed Systems, K-12 Solutions Catalog, (2021), Accessed September 20, 2021, https://s3.amazonaws.com/files.lightspeedsystems.com/collateral/K-12%20Solutions%20Catalog%202021%20%281%29.pdf.

In a case study of Lightspeed Filter, a district using the product said that it allows them to see "all the videos the kids watched, and all the searches they made,..[and there is] also an option for creating reports that showed you an overview of internet usage to see exactly what particular students are doing online." https://www.lightspeedsystems.com/case-study/dallastown-area-school-district/ https://www.lightspeedsystems.com/media-release/lightspeed-systems-wins-remote-learning-awards-2021/..

25 *How does Auditor work*, Accessed September 21, 2021, https://support.securly.com/hc/en-us/articles/115015796427-How-does-Auditor-work

26 FPF, *The Spectrum of Artificial Intelligence*, Accessed September 2021, https://fpf.org/blog/the-spectrum-of-artificial-intelligence-an-infographic-tool.

27 *How Smarter Filtering Means Safer Learning,* Accessed September 21, 2021, https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/goguardian/how-smarter-filtering-means-safer-learning.pdf.

28 Securly Inc., 24, Accessed September 2021, https://www.securly.com/24/?utm_term=Securly_Brand_Search_Securly_Brand&utm_source=Securly_Brand_search_2021&utm_medium=cpc&utm_campaign=Securly_Brand_search_2021.

29 Caroline Haskins, *Gaggle Knows Everything About Teens and Kids In School*, BuzzFeed News, (November 1, 2019), https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education.

30 Ibid.

31 Lightspeed Systems, Lightspeed Alert™, Accessed September 2021, https://www.lightspeedsystems.com/solutions/lightspeed-alert/.

32 LightSpeed Systems, *K-12 Solutions Catalog*, (2021), Accessed September 20, 2021, https://s3.amazonaws.com/files.lightspeedsystems.com/collateral/K-12%20Solutions%20Catalog%202021%20%281%29.pdf (Lightspeed also has the related product "Lightspeed Alert," which "scans virtually everywhere students interact online for indicators of suicide, self-harm, and school violence") (p6); Securely, *Home Page*,(n.d.), Accessed September 20, 2021, https://www.securly.com/home-admin; "[Securely] created an 'emotionally intelligent' app that sends parents weekly reports and automated push notifications detailing their children's internet searches and browsing histories." Benjamin Herold, Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming, Education Week, (May 30, 2019), Accessed September 20, 2021, https://www.edweek.org/leadership/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05; Bark, *Parent Portal,* (n.d.), Accessed September 20, 2021, https://www.bark.us/schools/parent-portal-alerts.

33 John Harrington, *E-rate Supports 95% of K-12 Students,* Funds for Learning, (December 24, 2020), Accessed September 20, 2021, https://www.fundsforlearning.com/news/2020/12/e-rate-supports-95-of-k-12-students/./

34 Hugh Grant-Chapman, Elizabeth Laird, Cody Venzke, *Student Activity Monitoring Software: Research Insights and Recommendations, Center for Democracy & Technology* (September 21, 2021) https://cdt.org/insights/student-activity-monitoring-software-research-insights-and-recommendations/.

35 GoGuardian, *See what others are saying about GoGuardian*, GoGuardian, (n.d.), Accessed March 15, 2021, https://web.archive.org/web/20201129173238/https://www.goguardian.com/success-stories/.

36 Gaggle, *Home Page,* Gaggle, (n.d.), Accessed September 15, 2021, https://web.archive.org/web/20210915151304/https://www.gaggle.net/.

37 Caroline Haskins, *Gaggle Knows Everything About Teens and Kids In School*, BuzzFeed News, (November 1, 2019), https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education.

38 Lightspeed Systems, Lightspeed Alert™, Accessed September 2021, https://www.lightspeedsystems.com/solutions/lightspeed-alert/.

39 Ibid.

40 GoGuardian, *Beacon 24/7 Now Available*, GoGuardian, (March 2, 2020), Accessed February 4, 2021, https://www.goguardian.com/blog/news/beacon-24-7-now-available/.

41 ManagedMethods, *Student Self-Harm Detection*, ManagedMethods, (2021), Accessed August 18, 2021, https://managedmethods.com/use-cases/self-harm-detection.

42 *Could Monitoring Students on Social Media Stop the Next School Shooting?(*2018), Accessed September 21, 2021, https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html

43 Todd Feathers, *Schools Spy on Kids to Prevent Shootings, But There's No Evidence It Works,* VICE (2019), https://www.vice.com/en/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works; There are significant gaps in the data surrounding the effectiveness of internet monitoring programs as a school-based intervention method. The limited research that does exist tends to focus on suicide-related internet searches and school-based intervention methods generally. For example, a 2015 review by Katherine Mok, Anthony F Jorm, and Jane Pirkis concluded that the internet is in fact used to search for suicide-related information and to discuss related matters. In a similar study, Hajime Sueki, Naohiro Yonemoto, Tadashi Takeshima, and Masatoshi Inagaki identified a corollary between suicidal ideation and internet seraches relating to suicide or mental health help. Finally, research from Jianhong Luo, Jingcheng Du, Cui Tao, Hua Xu, and Yaoyun Zhang identified potential risk factors that can be deduced from social media patterns. While these studies offer insight about internet searches relating to suicide and potential mental health indicators, they do not address the impact of monitoring such seraches or online behavior, nor do they discuss monitoring in school settings. With regard to school intervention methods generally, a 2019 article by Ida Sund Morken, Astrid Dahlgren, Ingeborg Lunde, and Siri

ENDNOTES

Toven acknowledges that there exists some evidence that school-based intervention methods can have short-term and potentially long-term impacts in suicide preventon, but that the research and data in this space is ultimately lacking. While some evidence-based school interventions may certainly be preventative, evidence is currently lacking or nonexistent with regard to school-based monitoring technology as an intervention technique. Katherine Mok, Anthony F Jorm, and Jane Pirkis, *Suicide-related Internet use: A review*, The Australian and New Zealand Journal of Psychiatry (2015), 49 (8): 697-705; Hajime Sueki, Naohiro Yonemoto, Tadashi Takeshima, and Masatoshi Inagaki, *The impact of suicidality-related internet use: a prospective large cohort study with young and middle-aged internet users,* PloS one (2014), 9 (4); Jianhong Luo, Jingcheng Du, Cui Tao, Hua Xu, and Yaoyun Zhang, *Exploring temporal suicidal behavior patterns on social media: Insight from Twitter analytics*, Health Informatics Journal (2020), 26 (2):738-752; Ida Sund Morken, Astrid Dahlgren, Ingeborg Lunde, and Siri Toven, *The effects of interventions preventing self-harm and suicide in children and adolescents: an overview of systematic reviews,* F1000Research (2019), 8, 890/

44 Lois Beckett, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, The Guardian (Oct. 22, 2019), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

45 Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning — and Now Won't Leave*, The 74, (September 14, 2021), Accessed September 20, 2021, https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/.

46 Lois Beckett, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, The Guardian (Oct. 22, 2019), Accessed September 20, 2021, https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

47 Benjamin Herold, *Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming,* Education Week, (May 30, 2019), Accessed September 20, 2021, https://www.edweek.org/leadership/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05..

48 The 74 reported in September 2021 that "only about a quarter of incidents reported to [Minneapolis Public School] officials [took place on] school days between 8 a.m. and 4 p.m." Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning — and Now Won't Leave*, The 74, (September 14, 2021), Accessed September 20, 2021, https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/.

49 Mark Keierleber, *'Don't Get Gaggled': Minneapolis School District Spends Big on Student Surveillance Tool, Raising Ire After Terminating Its Police Contract*, The 74, (October 28, 2020), Accessed June 7, 2021, https://www.the74million.org/article/dont-get-gaggled-minneapolis-school-district-spends-big-on-student-surveillance-tool-raising-ire-after-terminating-its-police-contract/; Mark Bergen, *Tiger Global Plows $200 Million Into EdTech Firm GoGuardian*, Bloomberg, (August 5, 2021), Accessed September 21, 2021, https://www.bloomberg.com/news/articles/2021-08-05/tiger-global-plows-200-million-into-edtech-firm-goguardian.

50 Erica Green, *Surge of Student Suicides Pushes Las Vegas Schools to Reopen*, The New York Times, (January 24, 2021), Accessed September 23, 2021, https://www.nytimes.com/2021/01/24/us/politics/student-suicides-nevada-coronavirus.html; Lisa Railton, *Students and the Pandemic: What is Gaggle Seeing?,* Gaggle, (April 20, 2021), Accessed September 23, 2021, https://www.gaggle.net/blog/students-and-the-pandemic-what-is-gaggle-seeing. Isabelle Barbour, *Surveillance Won't Save Our Kids*, Humane Public Policy Can, Student Privacy Compass, (September 17, 2021), Accessed September 20, 2021, https://studentprivacycompass.org/surveillance-wont-save-our-kids-humane-public-poliy-can/.

51 A CDC study found that "from 1991 to 2017, suicide attempts by Black adolescents rose by 73 percent, while for young Black males, injury from suicide attempt rose by 122 percent." National Center for Health Statistics, *Increase in Suicide Mortality in the United States, 1999–2018*, Center for Disease Control and Prevention, (April 2020), Accessed February 12, 2021, https://www.cdc.gov/nchs/products/databriefs/db362.htm. In 2020, a survey conducted by The Trevor Project found that in 2020, 40 percent of LGBTQ respondents seriously considered attempting suicide, with more than half of transgender and nonbinary youth seriously considering suicide. Nearly half of LGBTQ youth reported engaging in self-harm in the past year, with over 60 percent of transgender and nonbinary youth reporting the same. The Trevor Project, *2020 National Survey on LGBTQ Youth Mental Health*, The Trevor Project, (2020), Accessed February 4, 2021, https://www.thetrevorproject.org/survey-2020/?section=Introduction. In 2017, a study found that "school-age children and youth who are homeless are three times more likely to attempt suicide than students who live at home with a parent or guardian." National Health Care for the Homeless Council, *Suicide and Homelessness - Data Trends in Suicide and Mental Health Among Homeless Populations*, National Health Care for the Homeless Council, (May 2018), Accessed February 12, 2021, https://nhchc.org/wp-content/uploads/2019/08/suicide-fact-sheet.pdf.

52 Teddy Hartman, *4 principles school leaders can follow when balancing student safety and privacy,* District Administration, (August 27, 2021), Accessed September 21, 2021, https://districtadministration.com/4-principles-school-leaders-balance-student-safety-privacy-goguardian-tact/.

53 The American Civil Liberties Union, *Cops and No Counselors*, ACLU, (March 4, 2019), Accessed February 8, 2021 https://www.aclu.org/issues/juvenile-justice/school-prison-pipeline/cops-and-no-counselors.

54 Support at Securly, *How does Securly use AI across its products?*, Securly, Accessed September 21, 2021, https://support.securly.com/hc/en-us/articles/360026432394-How-does-Securly-use-AI-across-its-products.

55 Ana-Maria Bucur and Liviu P. Dinu, *Detecting Early Onset of Depression from Social Media Text using Learned Confidence Scores*, arXiv preprint (2020), https://arxiv.org/abs/2011.01695; Ajay K. Gogineni, S. Swayamjyoti, Devadatta Sahoo, Kisor K. Sahu, and Raj kishore, *Multi-Class classification of vulnerabilities in Smart Contracts using AWD-LSTM, with pre-trained encoder inspired from natural language processing*, (2020), IOP SciNotes, 1(3), 035002.

56 Aditya Joshi, Samarth Agrawal, Pushpak Bhattacharyya and Mark Carman, *Expect the unexpected: Harnessing Sentence Completion for Sarcasm Detection*, In International Conference of the Pacific Association for Computational Linguistics (2017): 275-287.

57 Aaron Leibowitz, *Could Monitoring Students on Social Media Stop the Next School Shooting?,* The New York Times, (September 6, 2018), Accessed December 17, 2019, https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html. This is the case with the self-harm monitoring system provided by Gaggle, which flags keywords such as "bomb," "glock,"

ENDNOTES

and "going to fight," and sends alerts to school administrators when a student uses these terms. Mark Keierleber, *Minneapolis School District Addresses Parent Outrage Over New Digital Surveillance Tool as Students Learn Remotely*, The 74, (October 28, 2020), Accessed June 7, 2021, https://www.the74million.org/minneapolis-school-district-addresses-parent-outrage-over-new-digital-surveillance-tool-as-students-learn-remotely

58 Valerie Steeves, Priscilla Regan and Leslie Regan Shade, *Digital Surveillance in the Networked Classroom*, The Equality Project, (May 7, 2017), Accessed September 21, 2021, http://www.equalityproject.ca/wp-content/uploads/2017/05/7-Digital-Surveillance-in-the-Networked-Classroom.pdf.

59 Nasser Eledroos & Kade Crockford, Social Media Monitoring in Boston: Free Speech in the Crosshairs, Privacy SOS (2018), https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs; Jonathon W. Penney, *Whose Speech Is Chilled by Surveillance?*, Slate (July 07, 2017), Accessed September 20, 2021, https://slate.com/technology/2017/07/women-young-people-experience-the-chilling-effects-of-surveillance-at-higher-rates.html.

60 Lois Beckett, *Under digital surveillance: how American schools spy on millions of kids*, The Guardian, (October 29, 2019), Accessed February 15, 2021, https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

61 Caroline Haskins, *Gaggle Knows Everything About Teens And Kids In School*, Buzzfeed, (November 1, 2019), Accessed September 20, 2021, https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education; Todd Feathers, *Schools Use Software that Blocks LGBTQ+ Content but not White Supremacists,* Motherboard, Tech by Vice, (April 28, 2021), Accessed July 27, 2021, https://www.vice.com/en/article/v7em39/schools-use-software-that-blocks-lgbtq-content-but-not-white-supremacists; Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning — and Now Won't Leave*, The 74, (September 14, 2021), Accessed September 20, 2021, https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/;
Lois Beckett, Under Digital Surveillance: How American Schools Spy on Millions of Kids, The Guardian (Oct. 22, 2019), Accessed September 20, 2021, https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

62 Todd Feathers, *Schools Use Software that Blocks LGBTQ+ Content but not White Supremacists,* Motherboard, Tech by Vice, (April 28, 2021), Accessed July 27, 2021, https://www.vice.com/en/article/v7em39/schools-use-software-that-blocks-lgbtq-content-but-not-white-supremacists.

63 Support at Securly, *How does Auditor work?,* Securly, Accessed September 21, 2021, https://support.securly.com/hc/en-us/articles/115015796427-How-does-Auditor-work.

64 Betsy Morris, *Schools Wrestle with Privacy of Digital Data Collected on Students*, The Wall Street Journal, (July 10, 2019), https://www.wsj.com/articles/one-parent-is-on-a-mission-to-protect-children-from-digital-mistakes-11562762000.

65 Mohit Varshney, Ananya Mahapatra, Vijay Krishnan, Rishab Gupta and Koushik Sinha Deb, *Violence and mental illness: what is the true story?*, Journal of Epidemiology & Community Health, (2016), 70(3).

66 Mohit Varshney, Ananya Mahapatra, Vijay Krishnan, Rishab Gupta and Koushik Sinha Deb, *Violence and mental illness: what is the true story?*, Journal of Epidemiology & Community Health, (2016), 70(3).

67 Perpetual Baffour, *Counsel or Criminalize?*, Center for American Progress, (September 22, 2016), Accessed February 8, 2021, https://www.americanprogress.org/issues/education-k-12/reports/2016/09/22/144636/counsel-or-criminalize/.

68 Marjory Stoneman Douglas High School Public Safety Act of 2018, Florida CS/SB 7026, (2018).

69 Marjory Stoneman Douglas High School Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives and Senate President*, (January 2, 2019), Accessed September 20, 2021, http://www.fdle.state.fl.us/MSDHS/CommissionReport.pdf.

70 Julio Ochoa, *Parents Are Leery Of Schools Requiring 'Mental Health' Disclosures By Students*, NPR (2018) https://www.npr.org/sections/health-shots/2018/09/21/648828034/parents-are-leery-of-schools-requiring-mental-health-disclosures-by-students.

71 Bazelon Center for Mental Health Law, *Nott v. George Washington University*, Bazelon Center for Mental Health Law, (n.d.), Accessed February 4, 2021, http://www.bazelon.org/nott-v-george-washington-university/.

72 The American Civil Liberties Union, *Cops and No Counselors*, ACLU (March 4, 2019), Accessed February 8, 2021 https://www.aclu.org/issues/juvenile-justice/school-prison-pipeline/cops-and-no-counselors..

73 Hugh Grant-Chapman, Elizabeth Laird, Cody Venzke, *Student Activity Monitoring Software: Research Insights and Recommendations*, Center for Democracy & Technology (September 21, 2021) https://cdt.org/insights/student-activity-monitoring-software-research-insights-and-recommendations/

74 USA Facts, *4.4 million households with children don't have consistent access to computers for online learning during the pandemic,* USA Facts, (September 28, 2020), Accessed July 27, 2021, https://usafacts.org/articles/internet-access-students-at-home.

75 Department of Justice, *United States Departments of Justice and Education Release Joint Guidance to Ensure English Learner Students Have Equal Access to a High-Quality Education,* United States Department of Justice, (January 7, 2015), https://www.justice.gov/opa/pr/united-states-departments-justice-and-education-release-joint-guidance-ensure-english-learner..

76 Jennifer Keys Adair, *The Impact of Discrimination on the Early Schooling Experiences of Children from Immigrant Families,* Migration Policy Institute, (September 2015), https://www.scribd.com/document/279980674/The-Impact-of-Discrimination-on-the-Early-Schooling-Experiences-of-Children-From-Immigrant-Families..

77 Corey Mitchell, *Discrimination at Schools Harms Development of Young ELLs, Study Says,* Education Week, (September 10, 2015), Accessed September 21, 2021, https://www.edweek.org/leadership/discrimination-at-school-harms-development-of-young-ells-study-says/2015/09..

78 Larry Ferlazzo, *Don't Make Assumptions About Your ELL Students,* Education Week, (November 2, 2020) https://www.edweek.org/teaching-learning/opinion-dont-make-assumptions-about-your-ell-students/2020/11.

ENDNOTES

79 Clara Vania, Moh. Ibrahim and Mirna Adriani, *Sentiment Lexicon Generation for an Under-Resourced Language*, IJCLA (2014) 59-72; Mehrnaz Siavoshi, *The Importance of Natural Language Processing for Non-English Languages*, Towards Data Science, (September 21, 2020), Accessed September 20, 2021, https://towardsdatascience.com/the-importance-of-natural-language-processing-for-non-english-languages-ada463697b9d..

80 90 Day Korean, *Korean Drama Phrases – Top 28 Words & Expressions for K-Drama Fans,* (n.d.) Accessed September 20, 2021, https://www.90daykorean.com/korean-drama-phrases/; The Junkie, *Top 40 Korean Conversational Phrases You Need To Know Part 4*, (August 9, 2013), Accessed September 20, 2021, https://www.linguajunkie.com/korean-language/top-40-korean-conversational-phrases-you-need-to-know-part-4.

81 Southern Poverty Law Center, *Costly and Cruel: How Misuse of the Baker Act Harms 37,000 Florida Children Each Year,* SPLC, (2021), Accessed July 27, 2021, https://www.splcenter.org/sites/default/files/com_special_report_baker_act_costly_and_cruel.pdf.

82 Su Lin Blodgett and Brendan O'Connor, *Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English,* Presented as a talk at the 2017 Workshop on Fairness, Accountability, and Transparency in Machine Learning (2017), https://arxiv.org/abs/1707.00061..

83 Anna Woorim Chung, *How Automated Tools Discriminate Against Black Language,* Civic Media, (January 24, 2019), Accessed September 21, 2021, https://civic.mit.edu/2019/01/24/how-automated-tools-discriminate-against-black-language/

84 Nia West-Bay and Stephanie Flores, *"Everybody Got Their Go Throughs": Young Adults on the Frontlines of Mental Health*, CLASP, (June 2017), Accessed September 21, 2021, https://www.clasp.org/sites/default/files/publications/2017/08/Everybody-Got-Their-Go-Throughs-Young-Adults-on-the-Frontlines-of-Mental-Health.pdf.

85 Nia West-Bay and Stephanie Flores, *"Everybody Got Their Go Throughs": Young Adults on the Frontlines of Mental Health*, CLASP, (June 2017), Accessed September 21, 2021, https://www.clasp.org/sites/default/files/publications/2017/08/Everybody-Got-Their-Go-Throughs-Young-Adults-on-the-Frontlines-of-Mental-Health.pdf.

86 High-surveillance can include a host of different school policies and practices premised on suspicion in students and the perceived need to exert law and order. These measures can be structural, such as having security cameras, metal detectors, barred windows, and automatically locking doors. They can also include practices such as subjecting students to random drug testing, wand sweeps, and dog sniffs. High-surveillance schools may also have policies that further enshrine a culture of surveillance, such as barring students from leaving campus for lunch or entering class buildings during lunch, enforcing strict dress codes, requiring students to carry transparent book bags, and requiring identification badges for students. For more, see: Sarah D. Sparks, *'High-Surveillance Schools Lead to More Suspicions, Lower Achievement,* Education Week, (April 21, 2021), Accessed September 21, 2021, https://www.edweek.org/leadership/high-surveillance-schools-lead-to-more-suspensions-lower-achievement/2021/04.

87 Whitney Bunts, *Defund Police in Schools and Expand School-Based Mental Health*, The Center for Law and Policy, (July 2, 2020), Accessed September 21, 2021, https://www.clasp.org/blog/defund-police-schools-and-expand-school-based-mental-health.

88 Melinda D. Anderson, *When School Feels Like Prison*, The Atlantic, (September 12, 2016), Accessed September 21, 2021, https://www.theatlantic.com/education/archive/2016/09/when-school-feels-like-prison/499556/.

89 Sarah D. Sparks, *'High-Surveillance Schools Lead to More Suspicions, Lower Achievement,* Education Week, (April 21, 2021), Accessed September 21, 2021, https://www.edweek.org/leadership/high-surveillance-schools-lead-to-more-suspensions-lower-achievement/2021/04.

90 Sarah D. Sparks, *'High-Surveillance Schools Lead to More Suspicions, Lower Achievement,* Education Week, (April 21, 2021), Accessed September 21, 2021, https://www.edweek.org/leadership/high-surveillance-schools-lead-to-more-suspensions-lower-achievement/2021/04.

91 American Psychological Association, *School-Based Risk and Protective Factors for Gender Diverse and Sexual Minority Children and Youth: Improving School Climate,* American Psychological Association, (2015), Accessed July 27, 2021, https://www.apa.org/pi/lgbt/programs/safe-supportive/lgbt/risk-factors.pdf.

92 The Trevor Project, *Research Brief: Fostering the Mental Health of LGBTQ Youth,* The Trevor Project, (2019), Accessed July 27, 2021, https://www.thetrevorproject.org/2019/05/30/research-brief-fostering-the-mental-health-of-lgbtq-youth/.

93 The Trevor Project, *National Survey on LGBTQ Youth Mental Health,* The Trevor Project, (2019), Accessed September 21, 2021, https://www.thetrevorproject.org/wp-content/uploads/2019/06/The-Trevor-Project-National-Survey-Results-2019.pdf.

94 The Trevor Project, *National Survey on LGBTQ Youth Mental Health,* The Trevor Project, (2019), Accessed September 21, 2021, https://www.thetrevorproject.org/wp-content/uploads/2019/06/The-Trevor-Project-National-Survey-Results-2019.pdf.

95 National Association of School Psychologists, *Policy Recommendations for Implementing the Framework for Safe and Successful Schools*, NASP, (2017), Accessed September 21, 2021, https://www.nasponline.org/resources-and-publications/resources/school-safety-and-crisis/a-framework-for-safe-and-successful-schools/policy-recommendations-for-implementing-the-framework-for-safe-and-successful-schools.

96 Jacqueline Ryan Vickery, *"I don't have anything to hide, but…" The Challenges and negotiations of social and mobile media privacy for non-dominant youth*, Journal of Information Communication, and Society (2014), 18: 281–294.

97 DeVan Hankerson, Cody Venzke, Elizabeth Laird, Hugh Grant-Chapman, Dhanajar Thakur, *Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software*, Center for Democracy & Technology, (September 2021), https://cdt.org/insights/ report-online-and-observed-student-privacy-implications-of-school-issued-devices-andstudent-activity-monitoring-software/.

98 In one research study, teachers were found to falsely identify approximately 16% and 17% of students as showing symptoms of depression and anxiety, respectively. The researchers noted that "these findings suggest teachers can identify approximately half of children who experience at-risk levels of depression and anxiety, but substantial miss rates call into question this method for use as either an alternative to universal screenings or as an initial step (gatekeeper role) in a multi-modal identification process." Jennifer M. Cunningham and Shannon M. Suldo, *Accuracy of Teachers in Identifying Elementary School Students Who*

ENDNOTES

Report At-Risk Levels of Anxiety and Depression, School Mental Health (2014) 6: 237-250; Sharon Ward, Judith Sylva, and Frank M. Gresham, *School-Based Predictors of Early Adolescent Depression*, School Mental Health (2010), 2: 125-131.

99 Several states have model protocols (e.g. Virginia Board of Education, Suicide Prevention Guidelines for Virginia Public Schools, Accessed September 20, 2021, https://www.doe.virginia.gov/support/prevention/suicide/suicide-prevention-guidebook.pdf) which are implemented at the district level in policies and guidance such as that of Albemarle County Public Schools (Albemarle County Public Schools, *Self-Harm / Suicide Intervention Guidance Document*, (2019), Accessed September 20, 2021, https://inside.k12albemarle.org/dept/instruction/schoolcounseling/Documents/Suicide%20Intervention%20Guide%204_2019.pdf).

100 Mark Keierleber, *'Don't Get Gaggled': Minneapolis School District Spends Big on Student Surveillance Tool, Raising Ire After Terminating Its Police Contract*, The 74, (October 28, 2020), Accessed June 7, 2021, https://www.the74million.org/article/dont-get-gaggled-minneapolis-school-district-spends-big-on-student-surveillance-tool-raising-ire-after-terminating-its-police-contract/.

101 Gaggle, *Home Page,* Gaggle, (n.d.), Accessed September 15, 2021, https://web.archive.org/web/20210915151304/https://www.gaggle.net/

102 Gaggle, *Home Page,* Gaggle, (n.d.), Accessed September 15, 2021, https://web.archive.org/web/20210915151304/https://www.gaggle.net/.

103 Amanda Ripley, *How America Outlawed Adolescence*, The Atlantic, (November 2016), https://www.theatlantic.com/magazine/archive/2016/11/how-america-outlawed-adolescence/501149/.

104 Southern Poverty Law Center, *Costly and Cruel: How Misuse of the Baker Act Harms 37,000 Florida Children Each Year*, SPLC, (2021), Accessed July 27, 2021, https://www.splcenter.org/sites/default/files/com_special_report_baker_act_costly_and_cruel.pdf.

105 ACLU, *Cops and No Counselors: How the Lack of Mental Health Staff is Harming Students,* (2019), Accessed September 20, 2021, https://www.aclu.org/sites/default/files/field_document/030419-acluschooldisciplinereport.pdf.

106 ACLU of Florida, Equality Florida, Florida Social Justice in Schools Project, Southern Poverty Law Center, & League of Women Voters of Florida, *The Cost of School Policing*, ACLU (September 3, 2020), Accessed February 9, 2021, https://www.splcenter.org/presscenter/new-study-reveals-floridas-school-policing-mandate-has-increased-negative-outcomes.

107 ACLU of Florida, Equality Florida, Florida Social Justice in Schools Project, Southern Poverty Law Center, & League of Women Voters of Florida, *The Cost of School Policing*, ACLU (September 3, 2020), Accessed February 9, 2021, https://www.splcenter.org/presscenter/new-study-reveals-floridas-school-policing-mandate-has-increased-negative-outcomes.

108 ACLU of Florida, Equality Florida, Florida Social Justice in Schools Project, Southern Poverty Law Center, & League of Women Voters of Florida, *The Cost of School Policing*, ACLU (September 3, 2020), Accessed February 9, 2021, https://www.splcenter.org/presscenter/new-study-reveals-floridas-school-policing-mandate-has-increased-negative-outcomes.

109 Gi Lee and David Cohen, *Incidences of Involuntary Psychiatric Detentions in 25 U.S. States*, Psychiatric Services (2021), 72(1): 61-68.

110 Christopher A. Mallett, *The School-to-Prison Pipeline: Disproportionate Impact on Vulnerable Children and Adolescents*, Education and Urban Society, (April 19, 2016), 49 (6): 563-592.

111 Julianne Hing, Race, Disability, and the School-to-Prison Pipeline, Colorlines (May 13, 2014), https://www.colorlines.com/articles/race-disability-and-school-prison-pipeline..

112 Julianne Hing, Race, Disability, and the School-to-Prison Pipeline, Colorlines (May 13, 2014), https://www.colorlines.com/articles/race-disability-and-school-prison-pipeline.

113 Molly Knefel, Youth Incarceration in the United States, by the Numbers, Teen Vogue (October 4, 2017), https://www.teenvogue.com/story/youth-incarceration-in-the-united-states-by-the-numbers.

114 ACLU, *Cops and No Counselors: How the Lack of Mental Health Staff is Harming Students,* (2019), Accessed September 20, 2021, https://www.aclu.org/sites/default/files/field_document/030419-acluschooldisciplinereport.pdf..

115 ACLU, *Cops and No Counselors: How the Lack of Mental Health Staff is Harming Students,* (2019), Accessed September 20, 2021, https://www.aclu.org/sites/default/files/field_document/030419-acluschooldisciplinereport.pdf.

116 ACLU, *Cops and No Counselors: How the Lack of Mental Health Staff is Harming Students,* (2019), Accessed September 20, 2021, https://www.aclu.org/sites/default/files/field_document/030419-acluschooldisciplinereport.pdf..

117 Daja E. Henry and Kimberly Rapanut, *How Schools and the Criminal Justice System Both Fail Students with Disabilities*, Slate, (October 21, 2020), Accessed July 27, 2021, https://slate.com/news-and-politics/2020/10/students-disabilities-criminal-justice-system.html.

118 National Council on Disability, *Breaking the School-to-Prison Pipeline for Students with Disabilities*, National Council on Disability, (June 18, 2015), Accessed July 27, 2021, https://ncd.gov/publications/2015/06182015.

119 Rachel Anspach, *Disabled Youth Are More at Risk of Being Incarcerated*, Teen Vogue, (October 9, 2017), Accessed September 20, 2021, https://www.teenvogue.com/story/why-disabled-youth-are-more-at-risk-of-being-incarcerated.

120 Daja E. Henry and Kimberly Rapanut, *How Schools and the Criminal Justice System Both Fail Students with Disabilities*, Slate, (October 21, 2020), Accessed July 27, 2021, https://slate.com/news-and-politics/2020/10/students-disabilities-criminal-justice-system.html.

121 Valerie Strauss, *Why are we criminalizing behavior of children with disabilities?*, (April 25, 2017), Accessed September 20, 2021, https://www.washingtonpost.com/news/answer-sheet/wp/2017/04/25/why-are-we-criminalizing-behavior-of-children-with-disabilities/.

122 Angela Irvine and Aisha Canfield, *The Overrepresentation of Lesbian, Gay, Bisexual, Questioning, Gender Nonconforming and Transgender Youth Within the Child Welfare to Juvenile Justice Crossover Population*, Journal of Gender, Social Policy & the Law, (2016), 24 (2): 242–61. https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1679&context=jgspl.

123 Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning — and Now Won't Leave*, The 74, (September 14, 2021), Accessed September 22, 2021, https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/.

124 GoGuardian, Trust & Privacy Center, Commonly Asked Questions, "When does GoGuardian operate on my child's device or account?, Accessed September 22, 2021, https://www.goguardian.com/privacy-information.

ENDNOTES

125 *See* Cal. Educ. Code §49073.6 ("[A] school district, county office of education, or charter school that considers a program to gather or maintain in its records any information obtained from social media of any enrolled pupil shall notify pupils and their parents or guardians about the proposed program and provide an opportunity for public comment at a regularly scheduled public meeting of the governing board of the school district or county office of education, or governing body of the charter school, as applicable, before the adoption of the program.")

126 Erica L. Green, *Surge of Student Suicides Pushes Las Vegas Schools to Reopen*, The New York Times, (January 24, 2021), Accessed February 4, 2021, https://www.nytimes.com/2021/01/24/us/politics/student-suicides-nevada-coronavirus.html.

127 Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning – and Now Won't Leave,* The 74, (September 14, 2021), https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/.

128 Caitlin Cook, *EdTech Start-Up GoGuardian Raises $200 Million, Despite Privacy Concerns,* dot.LA, (August 5, 2021), https://dot.la/goguardian-raise-2654471296/particle-2.

129 Mark Bergen, *Tiger Global Plows $200 Million Into EdTech Firm GoGuardian*, Bloomberg, (August 5, 2021), https://www.bloomberg.com/news/articles/2021-08-05/tiger-global-plows-200-million-into-edtech-firm-goguardian..

130 Donna St. George and Valerie Strauss, *Partly hidden by isolation, many of the nation's school children struggle with mental health*, The Washington Post, (January 21, 2021), Accessed February 8, 2021, https://www.washingtonpost.com/local/education/student-mental-health-pandemic/2021/01/21/3d377bea-3f30-11eb-8db8-395dedaaa036_story.html.

131 Isabelle Barbour, *Surveillance Won't Save Our Kids, Humane Public Policy Can*, Student Privacy Compass, (September 17, 2021), Accessed September 20, 2021, https://studentprivacycompass.org/surveillance-wont-save-our-kids-humane-public-policy-can/.

132 Sarah D. Sparks, *Data: What We Know About Student Mental Health and the Pandemic*, EducationWeek, (March 31, 2021), Accessed September 20, 2021, https://www.edweek.org/leadership/data-what-we-know-about-student-mental-health-and-the-pandemic/2021/03.

133 US Department of Education Office for Civil Rights, *Parent and Educator Resource Guide to Section 504 in Public Elementary and Secondary Schools,* US DOE, (2016), Accessed July 27, 2021, https://www2.ed.gov/about/offices/list/ocr/docs/504-resource-guide-201612.pdf.

134 Cornell Law School Legal Information Institute, *42 U.S. Code § 12102 – Definition of Disability,* Cornell Law School, (n.d.), Accessed July 27, 2021, https://www.law.cornell.edu/uscode/text/42/12102.

135 Sharan E. Brown, *What Does It Mean to Be "Regarded as Having an Impairment" Under the Americans with Disabilities Act (ADAAA),* ADA National Network, (2021), Accessed July 27, 2021, https://adata.org/legal_brief/regarded-as-having.

136 ADA National Network, *Mental Health Conditions in the Workplace and the ADA,* ADA National Network, (n.d.), Accessed July 27, 2021, https://adata.org/factsheet/health; ADA National Network, *Disability Rights Laws in Public Primary and Secondary Education: How Do They Relate?*, ADA National Network, (n.d.), Accessed July 27, 2021, https://adata.org/factsheet/disability-rights-laws-public-primary-and-secondary-education-how-do-they-relate.

137 Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning – and Now Won't Leave,* The 74, (September 14, 2021), https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/.

138 DeVan Hankerson, Cody Venzke, Elizabeth Laird, Hugh Grant-Chapman, Dhanajar Thakur, *Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software*, Center for Democracy & Technology, (September 21, 2021), *https://cdt.org/insights/ report-online-and-observed-student-privacy-implications-of-school-issued-devices-andstudent-activity-monitoring-software/*.

139 J. William Tucker and Amelia Vance, *School Surveillance: The Consequences for Equity and Privacy*, NASBE Education Leaders Report, (October 2016), Accessed February 9, 2021, https://eric.ed.gov/?id=ED582102.

140 42 U.S.C. 2000d et seq.

141 Learning for Justice, *ELL 101*, (2017), https://www.learningforjustice.org/magazine/spring-2017/ell-101; The United States Department of Justice, *United States Departments of Justice and Education Release Joint Guidance to Ensure English Learner Students Have Equal Access to a High-Quality Education*, (2015), https://www.justice.gov/opa/pr/united-states-departments-justice-and-education-release-joint-guidance-ensure-english-learner.

142 20 U.S.C. §§ 1681-1688.

143 *Bostock v. Clayton County*, 520 U.S. ___ (2020).

144 For example, "lesbian," "gay," and "queer" are included among Gaggle's keywords that would trigger a flag for questionable content. Caroline Haskins, *Gaggle Knows Everything About Teens and Kids In School*, BuzzFeed News, (November 1, 2019), Accessed September 22, 2021, https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education.

145 Aaron Leibowitz, *Could Monitoring Students on Social Media Stop the Next School Shooting?,* The New York Times, (September 6, 2018), Accessed December 17, 2019, https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html.


FUTURE OF
PRIVACY
FORUM