STUDENT VOICES:
LGBTQ+ EXPERIENCES IN THE CONNECTED CLASSROOM

FEBRUARY 2023

LGBT TECH

FUTURE OF PRIVACY FORUM

AUTHORED BY

Jamie Gorosh, *Policy Counsel, Youth & Education Privacy, Future of Privacy Forum*
Chris Wood, *Executive Director & Co-Founder, LGBT Tech*

ACKNOWLEDGMENTS

The authors would like to thank Ellie Bessette, Jim Siegl, Juliana Cotto and Elijah Armstrong for their contributions to this report.

LGBT Tech encourages the continued adoption and use of cutting-edge, new, and emerging technologies by providing information, education, and strategic outreach for LGBTQ+ communities. We are a national, nonpartisan group of LGBTQ+ organizations, academics, and technology organizations whose mission is to engage with critical technology and public policy leaders for strategic discussions at all levels. LGBT Tech empowers LGBTQ+ communities and individuals and ensures that media, telecommunications, and technology issues of specific concern to LGBTQ+ communities are addressed in public policy conversations.

The Future of Privacy Forum (FPF) serves as a catalyst for privacy leadership and scholarship advancing responsible data practices in support of emerging technologies. FPF is based in Washington, DC, and includes an advisory board composed of leading figures from industry, law, and advocacy groups. The views herein do not necessarily reflect those of our supporters or our Advisory Board.

High school is different today than in years past. Computer labs have been replaced by individual school-provided devices, and classes may be held anywhere with an internet connection. Schools are increasingly concerned about technology's impact on students' safety and mental health. Consequently, the methods and technologies that districts use to filter and monitor student activity online have changed, with many schools adopting systems that seek to monitor students' network activity and social media use, analyzing signals that students might be subject to safety risks, including the risk for self-harm.[1] But the same tools that can mitigate risks for some students can create or amplify risks for others. Alongside a global conversation about how to protect personal information online, a parallel conversation about student privacy rights is unfolding. Many students, parents, advocates, and legislators alike are expressing concerns about the proliferation of student online activity monitoring technologies. These concerns are often heightened for students who are part of marginalized communities. The implications of privacy and access — or lack of access — to information will unquestionably impact students who identify as LGBTQ+ differently from their peers.

This white paper highlights structured, in-depth, qualitative interviews conducted by LGBT Tech and the Future of Privacy Forum (FPF) to better understand LGBTQ+ youths' perspectives about privacy in public schools. We interviewed recent high school graduates across the United States who identify as LGBTQ+, gathering firsthand accounts of how monitoring impacted the students' feelings of safety and privacy at school. These accounts can inform how educators, technology companies, and policy makers can work toward protecting the needs of some of our country's most vulnerable populations.[2] Beyond the vital task of giving voice to the individuals most directly impacted by these technologies, this valuable insight may be used to guide policy reform, conduct further research, and determine how to improve the default settings of student monitoring products. Perhaps most critically, the lived experiences of these students may serve as a signal to current LGBTQ+ students that they are not alone and the issues they face are not being overlooked, especially in the wake of anti-LGBTQ+ legislation being introduced and passed in states across the country.[3]

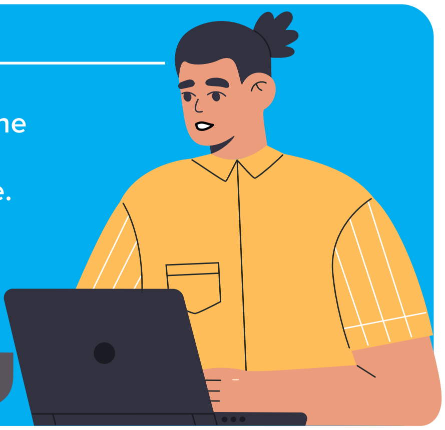
PART I: INTRODUCTION TO STUDENT FILTERING & MONITORING

Background

Student data is any identifiable information directly or indirectly related to a student that is collected and maintained in an educational context.[5] This traditionally encompassed data collected at school, but with increased use of online learning technologies, the educational context now includes data collected beyond the classroom. This can cover data from students' devices at home, from personal social media accounts, and from some school learning and collaboration platforms. Data collection may put students at risk for harms that may not be fully realized or discovered until later in life. Students may suffer physical, emotional, or reputational harm due to unauthorized access to their personal information.[6] Notably, it may create a permanent record and potentially tether students to their past in limiting or harmful ways, or it may reveal personal and sensitive student information that can result in stigmatization and bullying. This is especially true for LGBTQ+ students.[7] Young people value their privacy and while students may be savvy internet users, they require special privacy protections as they often are not fully equipped to weigh the potential benefits and risks of their internet use.[8] Even if they understand the risks, they still have to overcome their own strong susceptibility to social pressure that influences their behavior.[9]

Student data privacy refers to the responsible, ethical, and equitable collection, use, sharing, and protection of student data.[10] A positive relationship with one's privacy can support student success and give students agency over their own information and education.[11] However, consensus around what constitutes responsible data use remains an open question. There is inherent tension between the need to provide reasonable protections for students online and the boundary at which those protections become unnecessary surveillance. Further, the technologies have not remained static. Student use of the internet in the school context has evolved and so has the offering of products available to manage that use. The global COVID-19 pandemic accelerated these changes as school districts quickly pivoted, sometimes hastily implementing technology that would allow students to continue their education from home. It is useful to understand both the history of these technologies as well as the technology available today.

> [To me] privacy means that all of the information I share with someone or in a group is going to stay there. There is not going to be someone else that will have access to that, and that is going to be protected against hacking attacks.



[4]

The History and Evolution of Observing Student Activity Online

Long ago, legislators recognized the potential dangers of providing minors with unfettered access to the internet in public spaces such as schools and libraries. In response, Congress passed the Children's Internet Protection Act of 2000 (CIPA). CIPA mandates that schools receiving funding to support their internet access and capacity through the universal support services program, also known as "e-rate," must use a "technology protection measure" and implement an internet safety policy that prevents student exposure to inappropriate, obscene, or harmful content online.[12] The requirement of a "technology protection measure" necessitates the use of content blocking and filtering technology. The law also requires that schools hold a public hearing in advance of adopting their internet safety policy.[13]

Notably, while CIPA mandates an internet safety policy and protection from harmful content, it does not mention anything about *tracking* student activity online. In fact, no federal laws speak directly to this issue.[14] According to the National Conference of State Legislatures, 27 states have implemented internet content filtering laws that apply to publicly funded schools or libraries. However, the majority simply require school boards or public libraries to adopt policies that prevent minors from gaining access to sexually explicit, obscene, or harmful materials.[15] Absent guidance or further action from the Federal Communications Commission (FCC) or Congress, local administrators have full reign to set parameters for content filters, which allows for conscious or subconscious bias toward marginalized communities like the LGBTQ+ community. When evaluating CIPA within its historical context, it is notable that content filtering was adopted very soon after the internet arrived in the classroom. A February 1999 report by the National Center for Education Statistics reveals that in 1994, the Federal Government first began providing resources to connect public schools to the internet.[16] By the fall of 1998, 89% of schools had been connected[17] and with the 2000 legislation, content filtering became codified as the required norm. In the intervening 22 years, technologies and equitable laws have advanced immeasurably while CIPA has remained stagnant.

The Emergence of New Technologies

It is critical to draw a distinction between content filtering, student monitoring, and real time student monitoring as each has varying degrees of influence over students and thus an accompanying host of consequences for student privacy.

CONTENT FILTERING

The most ubiquitous practice is content filtering as mandated by CIPA for schools that receive E-rate funding. A search today for filtering software will produce dozens of options of third-party vendors boasting their products that will simplify CIPA compliance for schools. The legislation itself provides categorization of the types of websites that should be filtered, but the specifics of implementation largely rest in the hands of both the school and the vendor. In practice, this can result in overblocking akin to censorship whether it be deliberate or inadvertent. Although this type of filtering presents a First Amendment free speech issue that will not be fully explored here, it is important to demonstrate the types of battles over LGBTQ+ youth rights that have already played out at schools.

In 2011, the American Civil Liberties Union (ACLU) sounded the alarm on the frequent censorship of educational resources for LGBTQ+ students at school. An ACLU report explains,

> *"web filtering software frequently groups all websites—not just porn—into different categories based on the website's content. Most of these categories are innocuous, such as "history" or "science" or "news." But when websites are categorized based on their viewpoint, web filtering software can—intentionally or unintentionally—be used to block access to particular viewpoints in a discriminatory manner."*[18]

Given the large number of vendors providing content filtering services and the opaque nature of district use of these products, when LGBTQ+ content is restricted, it is done with limited guidance at the district level and with little federal direction. LGBT Tech has worked with members of Congress and the FCC to further understand where districts receive guidance around content filtering.[19] The broad direction from Congress does not specifically outline the difference between *supportive* LGBTQ+ material versus *potentially harmful* content as outlined in CIPA. Therefore, districts maintain the ability to blanket filter all LGBTQ+ content. Uncertainties persist: is the product itself designed to err on the side of caution and over-filter rather than risk excluding CIPA prohibited content? Did the school district simply retain pre-set maximums for content filters or did an administrator select additional sites to block? There is evidence that in response to the ACLU campaign, several of the vendors that comprise a large share of the market removed pre-set content filters that prevented LGBTQ+ student access to resources.[20] Although LGBT Tech has taken steps with members of Congress from 2016 to 2022 to introduce the "Don't Block LGBTQ Act,"[21] the ability to block these types of sites remains available to administrators, perpetuating this dangerous potential for individual bias.

STUDENT MONITORING

The 2023 classroom looks different from the 2000 classroom. Modern monitoring technologies, including content filtering, are no longer confined to the school's network. FPF identified the following methods by which schools may potentially track student online activity:

1. School-Issued Devices: Any device the school issues to a student, such as laptops or tablets, may be monitored. The monitoring system may access and process any online data from these devices, potentially including students' online activities when they use these devices at home.
2. School-Managed Internet Connections: Any online data from any school-managed internet connection may be monitored. Students who use personal devices may nonetheless have their online activities subject to monitoring if they connect to a school-managed network, whether at school or at home.
3. School-Managed Apps and Accounts: Certain student accounts that are managed by the school may be monitored (e.g., Microsoft 365 or Google Workspace), regardless of the internet connection or device that a student uses to access the accounts.

New monitoring technologies were developed with student safety and wellbeing in mind, primarily as "self-harm monitoring systems." Student data collected through school-managed devices, internet connections, or accounts is processed by a monitoring program's automated system that searches for concerning indicators. These indicators may include keywords associated with self-harm, suicide, depression, violence, bullying, pornography, hate speech, profanity, illegal behavior, and more.[22] Indicators may also be driven by machine learning. These systems can search student social media and website browsing activity, as well as email, chat, and documents stored in collaborative services from Google and Microsoft. Responses to the flagged content vary based on the type of product used and subscription tier. In some situations, content may be reviewed by a moderator employee to determine whether it was indeed appropriately flagged, but not always.

Depending on the nature of a detected indicator, the monitoring provider will take action in some combination of the following ways: send a warning to the student that their activity was flagged; block the content; and/or send an alert to adults. As the most severe escalation, alerting adults is most common when content related to self-harm or harm to others is flagged. Adults receiving these alerts may include school administrators, school IT professionals, parents, and law enforcement. Although some of the technology vendors claim that these monitoring products are not intended to serve as a conduit for punishing students, a study by the Center for Democracy and Technology (CDT) found that 43% of teachers reported using information gleaned from monitoring technology to identify student violations of disciplinary policy.[23] Within this framework, it is noteworthy that when student monitoring systems code terms like "gay" and "transgender" as sexual content, LGBTQ+ students will be monitored more regularly than their peers, and thus more subject to discipline. Some vendors have defended decisions to keep flagging these terms as a method of identifying and preventing cyberbullying,[24] though evidence of the efficacy of this strategy is unknown and the consequences are overt.

REAL TIME STUDENT MONITORING

Some student activity monitoring software goes beyond data collection and sharing. These systems, typically referred to as classroom management tools, may permit authorized teachers, administrators, and other school staff to see what students have open on their computer screens. The technology allows them to remotely open websites on a student's laptop, switch tabs, block sites, access communications, or view browsing histories.[25] While the stated purpose of these tools is to minimize distractions and maximize engagement in class, it places power in the hands of teachers and administrators like never before.

In one case, a now corrected design flaw associated with this technology granted a student's teacher the ability to remotely start a video session with a video preview, which allowed instructors to see into students' homes without their permission or awareness.[26] These types of scenarios were presented to individuals during their interview. Nearly all respondents commented that the ability for a teacher to control a student's device amounts to an invasion of privacy, even if it is on a school-issued device. Furthermore, nearly all felt that this kind of micromanaging would be distracting to the learning environment. Many students agreed this kind of scenario would trigger a "meltdown" or "shutdown" where they would stop engaging in class and ruminate.

Use of Technology Today

The use and management of student data has notably increased since the COVID-19 crisis. The shift to online learning during the pandemic was accompanied by a 28% increase in the number of school-managed devices used by students along with thousands of school-managed WiFi internet hotspots.[27] This increased technology use has led to more monitoring of student online activity.[28] A September 2021 study by CDT found 81% of K-12 teachers said their school uses some form of monitoring software.[29] Switching from an in-person school environment to "classrooms in the cloud" heightens the pressure on schools and districts to protect student privacy.[30] Experiences of internet content filtering are more common on school-issued devices or on school WiFi networks. Accordingly, students using school-issued devices are monitored to a greater extent than their peers using personal devices.[31] This exposes a deep equity issue in which already disadvantaged low-income students are surveilled to a higher degree than peers with more resources.

PART II: LGBTQ+ STUDENT EXPERIENCE WITH FILTERING & MONITORING

It is critical to consider the voices of the students themselves to truly understand what is at stake for LGBTQ+ youth when information that is intended to remain private is shared. Findings from our conversations with LGBTQ+ students will be highlighted throughout this section to describe the student experience. It is also noteworthy that in many areas, student responses revealed a lack of consensus among the participants. This serves as a reminder that no two experiences are exactly alike and that many intersecting factors will influence the ideas and opinions of each student.

> “I really feel that we never have a 100% privacy guarantee in any online environment.”

[32]

Privacy and LGBTQ+ Student Identity

High school is a formative time during which many teenagers are discovering themselves, growing, and changing. Unfortunately, many do not feel safe to explore all facets of their identity within their home or school environment. More than 18 million Americans identify as LGBTQ+ and more younger Americans than ever are identifying as such.[33] Research has found LGBTQ+ youth are more likely than their non-LGBTQ+ peers to seek identity-related resources and help online.[34] According to a 2017 Stonewall School Report, 96% of those surveyed agreed that the internet has helped them understand more about their sexual orientation and gender identity, and 90% said that they feel more comfortable being themselves online.[35] Young people today are generally aware of and concerned about student monitoring, but youth belonging to the LGBTQ+ community have unique concerns about these practices that primarily relate to their safety and well-being.

All participants were familiar with the practice of student monitoring and a majority recalled experiencing internet content filtering while at school. However, participants noted that they were not aware of their school’s specific use of filtering or monitoring technology until after they or a peer experienced it directly. In an environment ostensibly designed for learning and growth, knowledge of monitoring technology will have a chilling effect. A CDT study found that 80% of students are more careful about their online activities when they know they are being monitored. Further, 58% of students said that they do not share their true thoughts or ideas online because they know what they do is being monitored.[36]

The LGBTQ+ community experiences a paradox of privacy: societal expectation that one should keep a queer identity secret (or “in the closet”) until they “reveal themselves” as an LGBTQ+ individual. Staying secretive about one’s sexuality is often for protection, but this can perpetuate feelings of shame and guilt, which negatively impacts a person’s mental and physical health.[37] On the other hand, for many LGBTQ+ youth who are still selectively sharing their sexual orientation, privacy is of paramount concern. A privacy data breach that exposes someone’s sexual orientation can have far-reaching effects, including alienation at school, the loss of employment, loss of familial relationships and friendships, and even the potential for physical harm or death.[38] The internet gives individuals the opportunity to seek virtual resources while remaining “in the closet” but only if students do not need to worry about their search history being exposed or their activities being monitored. When LGBTQ+ online communities are flagged or blocked, it sends a message to students that their identity is not appropriate for school. These same LGBTQ+ students may have similar messages communicated to them at home regarding their sexual orientation or gender identity, leaving them little space to find resources or supportive information and feeling further isolated.[39]

Compounding this issue, it is becoming increasingly dangerous for students to express their LGBTQ+ identity in certain parts of the country. Bills have been introduced in at least 28 states and passed in 8 states with varying objectives ranging from preventing students and teachers from using a student’s preferred gender pronoun; restricting curriculum or library books that contain LGBTQ+ themes; and limiting the formation of school clubs for LGBTQ+ students.[40] Lawmakers are also targeting transgender youth by attempting to limit trans students’ participation on school sports teams, prohibiting them from using bathrooms and locker rooms based on their gender identity, and even limiting critical gender affirming health care.[41] In a survey conducted by the Trevor Project, 86% of LGBTQ+ youth felt that politics is impacting their wellbeing. The increasingly hostile political discourse over sexuality and gender identity reinforces the importance of student data privacy for LGBTQ+ youth.

Parent Access to Student Data

A majority of interviewees expressed concern about their LGBTQ+ peers’ safety at home. These concerns are valid; of the youth that come out to their parents, 48% say their families make them feel bad for being LGBTQ+.[43] Trans youth are more than twice as likely as their cisgender peers to be mocked by their families for their identity. LGBTQ+ youth are more likely to experience homelessness than their peers and most commonly say family conflict is the cause. A 2020 survey by the Trevor Project found that 29% of LGBTQ+ youth have experienced homelessness, been kicked out of their homes, or have run away.[44] These negative experiences are even more prevalent among LGBTQ+ youth of color. The legitimate fear of expressing their true identity at home makes it all the more critical that students are safe to seek out resources at school.

The interviewees generally agreed there is some benefit to schools using a monitoring system, but most of them requested that schools review any flagged material with them directly before

> “[I] wasn’t safe at home to come out so school was really the only place I could actually do research safely. If that was blocked and I couldn’t see any resources, it would be really harmful to me because community is important.”

[42]

approaching their parents/caregivers. This reflects a desire for autonomy and a value of privacy. Further, when automated alerts go out to parents, this can be dangerous for LGBTQ+ students. There have already been documented instances of students being outed to their parents based on alerts from monitoring systems.[45] This risk may discourage youth from seeking LGBTQ-affirming resources online. Participants shared that if flagged photos were immediately shared with their parents, they would feel frustrated, humiliated, angry, and that a boundary of privacy had been violated. If an AI system incorrectly flags content, students agree they should have an opportunity to correct the mistake by requesting that administrators delete records of the flagged content. Nonetheless, it remains concerning that these remedies rely on support from school administrators as they do not always create a safe space for LGBTQ+ students. In many cases, student monitoring will lead to more reprimanding and punishments from administrators, as well as increased parent involvement.

Even if a student is lucky enough to attend a school with the above safeguards in place and with school officials who are aware of and affirm the needs of LGBTQ+ students, parents still have mechanisms at their disposal to access information that their children do not want to share with them. The Family Educational Rights and Privacy Act (FERPA) was passed in 1974 to restrict who can access and use student information and to guarantee that parents have access to their children's education records.[46] Although a 1974 congress could not conceive of website browsing history as student records, today parents can request to inspect this information. As previously stated, this can "out" a student to their parents without student consent. This is also dangerous for students who have changed their gender pronouns at school but not at home. Even without an intent to collect this information, parents may request documentation that contains a record of the student's preferred pronoun. Although FERPA does have several limited exceptions, it largely grants parent access to all student educational records up until a student turns 18.[47]

> "I am not against monitoring for signs of intent or signs of behavior[s] actually taking place, but I'm concerned that there's going to be that one well-meaning counselor that comes up to the student and confronts them about it in all the wrong ways."

[48]

LGBTQ+ Student Safety

LGBTQ+ students are at greater risk for their online activity being flagged or blocked by content filtering and monitoring systems, which exposes them to more contact with school officials who may or may not be sensitive to their needs. This has the potential to lead to negative and even sometimes dangerous outcomes for students. To begin, even if their intent is to provide support to a student, often school counselors are not equipped to provide the type of care and guidance that LGBTQ+ students need. Some may not have the appropriate training and others may be subject to policies that prevent them from discussing sexual orientation and gender identity without parental consent. School officials should aim to foster an atmosphere of inclusivity where students feel affirmed and have the autonomy to determine how or if they want to come out in the school environment. In practice, a study by the Trevor Project revealed that fewer than half of LGBTQ+ identifying students feel comfortable sharing their identity with an adult at school.[49]

The risks associated with seeking support frequently outweigh any perceived benefits. The ACLU has reported that LGBTQ+ students are overrepresented in school disciplinary incidents and in the juvenile justice system at large.[50] One participant expressed concern that many schools are underfunded and resort to “let’s just call the cops” during interactions with LGBTQ+ students. This comment may have stemmed from the fact that frequently, this call stays within the building as cops are already stationed in schools. Although FERPA does provide protection against sharing records with law enforcement absent a health and safety emergency, it does not apply in the same way for School Resource Officers (SROs) if they are designated as a “school official.”[51] The ACLU found that 1.7 million students attend schools with a police officer and no counselor; 3 million with a police officer and no nurse; 6 million with a police officer and no school psychologist; and 10 million with a police officer and no social worker.[52]

Many LGBTQ+ students cannot turn to their peers for support either. The American Psychological Association has reported that 64% of LGBTQ+ students feel unsafe in schools because of prejudice and harassment.[53] Consistent with the findings above, sixty percent of these students did not report incidents of bullying to school officials due to fear that the situation would be made worse or the school would take no action to help them.[54] The rise and prevalence of social media has expanded the reach and scope of this issue as bullying is no longer confined to school hallways or even school hours. A majority of the participants personally experienced cyberbullying. The students recognized the benefits of monitoring for cyberbullying, including cyberbullying prevention as well documentation of the facts in these cases. A few of the surveyed students expressed a hope that if schools have clear guidelines around social media monitoring, cyberbullying could be deterred. Still, two-thirds of the interviewees said they would feel it is an invasion of privacy for schools to monitor their personal social media accounts for signs of intent to self-harm, even while on school-issued devices.

> **[B]ack then I was trying to hide as much as possible. My school wasn’t the best at talking to people about [mental health] so if I ended up having a meeting with my counselor about it just out of the blue because they saw my social media...I would be upset.**

[55]

LGBTQ+ Student Health

Marginalized communities often experience barriers to adequate healthcare information that can be offset through online research. The LGBTQ+ community has always been more heavily reliant on internet connectivity and looking for healthcare is no different, with 81% of LGBTQ+ youth reportedly using the internet to search for health information.[56] Online servers such as Folx Health, Plume, and QueerDoc provide gender-affirming informational resources, therapy, mental health services, and more. RADRemedy.com allows LGBTQ+ people to share their experiences with healthcare providers, allowing for a digital word-of-mouth effect that might otherwise be difficult to create. Furthermore, access to gender-affirming, evidence-based healthcare through the internet, such as telehealth counseling sessions over video platforms, may mitigate current and further health disparities experienced by the LGBTQ+ community.[57]

One recent study on adolescent health examined youths’ use of online, text-based chat platforms to seek formal and informal LGBTQ-specific support and found that the pandemic has driven use of these community platforms to new heights. Two LGBTQ-specific platforms, Q Chat Space and the 24/7 crisis service of the Trevor Project, have reported increased user engagement.[58] Student isolation during the COVID-19 pandemic has certainly escalated concern for student mental health. 73% of LGBTQ+ youth surveyed by the Trevor Project said they experienced symptoms of generalized anxiety and 58% experienced symptoms of major depressive disorder in the last two weeks. 48% of these students had engaged in self harm in the past year, and 45% contemplated suicide within the last year.[59] Meanwhile, over 60% of these individuals were left without access to health care, often because of concerns related to parental permission.[60]

Monitoring technologies, originally introduced and still touted as products that can save students' lives and protect their health and well-being, ironically have a strong potential to undercut online access to care and critical resources. Further, over half of the participants, wary from their own personal experiences, expressed skepticism about a school's ability to effectively intervene in a student's intent to self-harm. Many have also argued that it is still unclear whether monitoring technologies are effective with identifying and assisting students who may be considering self-harm. Online activities alone are not the full picture. Even if monitoring technology can detect some at-risk students, it cannot identify all students who are in need of mental health support and services. It would be dangerous for districts to rely on monitoring technology as the only mechanism for detecting at-risk students.

PART III: RECOMMENDATIONS & CONCLUSION

We interviewed LGBTQ+ youth in order to understand their perspectives about technology privacy and to assist schools in developing policies that respect and reflect the views of LGBTQ+ students, while also balancing the need to establish safety in schools. In order to better understand the needs of LGBTQ+ students, it is critical to create an inclusive environment in which these students feel comfortable to directly communicate their needs and concerns. This section provides several additional recommendations for reform.

School districts should be more transparent with the school community about what technology they are using and how they are using it.

The majority of the student survey participants noted that their schools did not communicate about what type of filtering and/or monitoring technology they use. Parents are similarly unaware as one in four parents surveyed by CDT did not know if their child's school uses filtering or monitoring technology.[61]

Districts may take the following measures to improve transparency:

- Hold a public hearing before adopting new monitoring technologies so that students and their parents have the opportunity to provide input and have notice of any changes.
- Publish a clear policy on student monitoring — including information on which data are collected, who has access to them, how they will be used, and when they will be destroyed — and communicate the policy to parents and students on at least an annual basis.
- Have a discussion with students about monitoring practices and the specific intent for use. Encourage student questions and feedback.
- Do not assume that parent feedback also represents the views of their student.
- Engage a local or regional LGBTQ+ Center to inform the district about best practices for ensuring LGBTQ+ student safety.
- Provide students and parents with the name of the vendor they are using at the beginning of the school year and notify students and parents if anything changes.
- Ensure they are working with a vendor that is transparent about the algorithms used to determine what type of websites will be blocked and what activities will trigger or "flag" an alert to school officials or parents.
- Avoid blanket bans on filtering content related to sexual orientation and gender identity.
- Publish a list of the websites that will be blocked by filtering technology and have a procedure for students to contest the decision to block that site.
- Publish a list of the school officials who will have access to any content flagged by monitoring technology.

Districts should be selective when using monitoring technology to protect student safety and wellbeing, and should develop safeguards for how information is used and who it is shared with.

There are many products on the market to choose from, each with different methods for flagging and reporting. Participants emphasized the importance of school officials confronting students directly about any flagged content before going to parents or law enforcement.

Districts may take the following measures:

» Consider the efficacy of a monitoring product before purchasing, including whether the technology has been evaluated by a third party to back the claims they make.

» Carefully consider what the monitoring system reviews and who has access to notifications.

» Determine why LGBTQ+ related terms are included in a vendor's flagging system, and determine whether flagging those terms will actually help identify situations of student danger or self-harm.

» Consider whether monitoring systems can interpret the context of a statement before flagging and understand how the system interprets photos and text in non-English languages.

» Understand the vendor's policies and procedures for sharing information with law enforcement.

» Include a robust training program for school officials responsible for handling sensitive student data. Bearing in mind that data is only a sliver of the problem, human intervention always includes the potential for bias and thus a solution-oriented mindset must include training to ensure proper data use.

» Adopt policies that prohibit or limit automatic notification to parents when monitoring technology flags student content.

» When appropriate, inform students immediately when content is flagged and provide them with an opportunity to discuss the content with a school counselor or administrator.

» Develop and communicate procedures for correcting or deleting records if they have been mistakenly flagged.

» Inform students whenever sensitive records will be disclosed pursuant to FERPA.

As student data privacy concerns continue to arise, legislative reform is a powerful tool for improving the lives of LGBTQ+ students.

States should pass legislation that emulates California Assembly Bill 1442, "Pupil records: social media." This 2014 law requires that when districts are considering gathering or maintaining records obtained from student social media accounts, students and their parents must be notified first and given the opportunity to provide comments at a public meeting.[62] It also requires districts to limit the information gathered to that which pertains to school or student safety and provide the student with access to the information that has been collected. Finally, it restricts the third-party vendor from selling or sharing any information gathered and provides instructions on the destruction of data.[63] These types of protections serve as a safeguard against unauthorized or excessive use of student information, and provide guidelines for how districts can develop their own policies.

In the absence of comprehensive federal student privacy legislation, there is room for reform within the existing structure. Congress could consider amending FERPA[64] to create a student safety exception to grant students the right to prevent the disclosure of records to parents when certain sensitive topics are discussed with, or discovered by, a school official in a manner that would be reflected in or transferred to a student record. For LGBTQ+ youth who reside in abusive or intolerant households, this exception could be critical in preserving the students' physical and emotional wellbeing. This exception should be accompanied by an obligation for school officials to inform students of such a right to restrict disclosure whenever a sensitive topic is discovered through monitoring or discussed by the student.

Congress should also pass the "Don't Block LGBTQ Act. As previously mentioned, LGBT Tech has worked with members of Congress to introduce this legislation every year since 2016. The bill would prohibit elementary schools, secondary schools, or libraries that receive discount rates for telecommunications services under the E-rate program from blocking internet access to lesbian, gay, bisexual, transgender, or queer resources. The bill does not prohibit schools or libraries from blocking content that is obscene, pornographic, or harmful to minors.

Districts should invest in more robust mental health services and support for LGBTQ+ students, and train school administrators to ensure they are competent in dealing with the unique needs of these students.

LGBTQ+ specific experience in schools is a larger issue that underlies discussions about student monitoring. Privacy is a societal concern, and our culture is still in the process of reckoning with how much privacy youth should have, especially in the school context. However, absent consensus it is important to listen to the students themselves as they have the most at stake. LGBTQ+ individuals should be able to fully express themselves and receive support in a protected environment, like a school. Schools should ensure that the monitoring technology they are using aligns with 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. When schools develop programming specifically aimed at providing resources and mental health care to LGBTQ+ students and create an overall environment of acceptance and inclusivity, that may make all the difference.

Endnotes

[1] A Closer Look: Network Monitoring, Future of Privacy Forum (Oct. 23, 2019) https://studentprivacycompass.org/issuebriefnetworkmonitoring/; A Closer Look: Social Media Monitoring, Future of Privacy Forum (Oct. 30, 2019) https://studentprivacycompass.org/closerlook2/; The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies, Future of Privacy Forum (Sept. 27, 2021) https://studentprivacycompass.org/resource/self-harm-monitoring/.

[2] While our analysis highlights student voices that bring valuable perspectives to discussions about data protection, we acknowledge the limitations of our approach, which include a small sample size (12 recent graduates) and a focus on US students. Indeed, we recognize that no research approach can convey the full diversity of views held by all LGBTQ+ students.

[3] *Legislation Affecting LGBTQ Rights Across the Country*, American Civil Liberties Union (Dec. 22, 2022) https://www.aclu.org/legislation-affecting-lgbtq-rights-across-country-2022?redirect=legislation-affecting-lgbtq-rights-across-country.

[4] LGBT Tech Student Interview (on file with authors).

[5] *Student Privacy Primer*, Student Privacy Compass (Oct. 5, 2021). https://studentprivacycompass.org/resource/student-privacy-primer/.

[6] Id.

[7] Emily S. Rueb, *A Teenager Killed Himself After Being Outed as Bisexual. His Family Wants Justice*, New York Times (September 2019), https://www.nytimes.com/2019/09/30/us/channing-smith-suicide-bisexual-tennessee.html.

[8] Santer et al. *Early Adolescents' Perspectives on Digital Privacy*, Algorithmic Rights and Protections for Children (Jun. 29, 2021) https://wip.mitpress.mit.edu/pub/early-adolescents-perspectives-on-digital-privacy/release/1.

[9] Id.

[10] *Student Privacy Primer*, Student Privacy Compass (Oct. 5, 2021), https://studentprivacycompass.org/resource/student-privacy-primer/.

[11] Park et al. *Student Privacy Communications Toolkit: For Schools & Districts*. Student Privacy Compass, Jan.12, 2021. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/. Accessed Apr. 14, 2022.

[12] Children's Internet Protection Act (CIPA), Federal Communications Commission (Dec. 30, 2019) https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

[13] Id.

[14] Id.

[15] *State Internet Filtering Laws*, National Conference of State Legislators (Jan. 20, 2022) https://www.ncsl.org/research/telecommunications-and-information-technology/state-internet-filtering-laws.aspx.

[16] *Internet Access in Public Schools and Classrooms: 1994–98*, National Center for Education Statistics (Feb 1999) https://nces.ed.gov/pubs99/1999017.pdf.

[17] Id.

[18] Nanette K. Laughrey, *Don't Filter Me,* The American Civil Liberties Union (Feb. 15, 2012), https://www.aclu.org/sites/default/files/field_document/dont_filter_me-2012-1001-v04.pdf.

[19] *Congressional Letter to the FCC regarding LGBT Content Filtering in Public Schools and Libraries*, Rep. Mike Honda Letter to Chairman Wheeler, (Sept. 24, 2014) https://www.lgbttech.org/dont-block-lgbt-act-of-2022.

[20] Jenna Zwang, *Companies respond to ACLU's 'Don't Filter Me' campaign*, eSchool News (Jun. 16, 2011) https://www.eschoolnews.com/2011/06/16/companies-respond-to-aclus-dont-filter-me-campaign/2/.

[21] *Don't Block LGBTQ Act*, LGBT Tech, https://www.lgbttech.org/dont-block-lgbt-act-of-2022.

[22] The *Administrator's Guide to Bark for Schools*, Bark for Schools. (Last Accessed Jan 30, 2023). https://s3.amazonaws.com/bark-assets/guides/Administrators_Guide_BarkForSchools.pdf. (Last Accessed Jan 30, 2023).

[23] Senators Elizabeth Warren & Ed Markey, *Constant Surveillance: Implications of Around-the-Clock Online Student Activity Monitoring*, The United States Senate (Mar. 2022), https://www.warren.senate.gov/imo/media/doc/356670%20Student%20Surveillance.pdf.

[24] Mark Keierleber, *Inside the Harrowing World of Online Student Surveillance*, Fast Company (May 4, 2022), https://www.fastcompany.com/90748240/gaggle-school-content-moderation-privacy.

[25] *CDT CRDC Letter*, Center for Democracy & Technology, (Feb. 11, 2022). https://cdt.org/wp-content/uploads/2022/02/2022-02-11-CDT-CRDC-Letter.pdf.

[26] Nader Issa, *CPS Teachers Could Look Inside Students' Homes — Without Their Knowledge — Before Fix*. Chicago Sun Times (Oc.t 5, 2020) https://chicago.suntimes.com/education/2020/10/5/21497946/cps-public-schools-go-guardian-technology-privacy-remote-learning.

[27] Sharifi, Siegl, Vance, *Understanding Student Monitoring*. Future of Privacy Forum Student Privacy Compass (Oct. 27, 2021) https://studentprivacycompass.org/resource/understanding-student-monitoring/.

[28] Id.

[29] *CDT CRDC Letter*, Center for Democracy & Technology (Feb. 11, 2022), https://cdt.org/wp-content/uploads/2022/02/2022-02-11-CDT-CRDC-Letter.pdf.

[30] Future of Privacy Forum Staff, *Student Privacy Communications Toolkit: For Schools & Districts*, Student Privacy Compass (Jan.12, 2021), https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/.

[31] Madrigal et al., Report - *Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software*, Center for Democracy and Technology (Sep. 21, 2021) https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/.

[32] LGBT Tech Student Interview (on file with authors).

[33] Jeffrey M. Jones, *LGBT Identification Rises to 5.6% in Latest U.S. Estimate*, Gallup (Feb. 24, 2021), https://news.gallup.com/poll/329708/lgbt-identification-rises-latest-estimate.aspx.

[34] Future of Privacy Forum Staff, *The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies: Recommendations for Schools*, Student Privacy Compass, (Sept. 2021), https://studentprivacycompass.org/wp-content/uploads/2021/09/FPF-Self-Harm-Report-R4.pdf.

35 *Staying Safe Online: Practical Strategies to Best Support All Children and Young People Online, Including Those Who Identify as LGBT*, Stonewall & Childnet International (2020), https://www.stonewall.org.uk/system/files/stonewall_staying_safe_online_april2022.pdf.

36 Senators Elizabeth Warren and Ed Markey, *Constant Surveillance: Implications of Around-the-Clock Online Student Activity Monitoring*, The United States Senate (Mar. 2022) https://www.warren.senate.gov/imo/media/doc/356670%20Student%20Surveillance.pdf.

37 Campbell & Cowan, *The Paradox of Privacy: Revisiting and Core Library Value in an Age of Big Data and Linked Data*. FIMS Publications, (2016), https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1085&context=fimspub.

38 Carlos Gutierrez, *Data Privacy is Crucial for the LGBT Community*, National Cybersecurity Alliance (Feb. 20, 2019) https://staysafeonline.org/blog/data-privacy-crucial-lgbt-community/.

39 *National Survey on LGBTQ Youth Mental Health 2021*, The Trevor Project (2021), https://www.thetrevorproject.org/survey-2021/.

40 The State Legislative Attacks On LGBTQ+ People, Human Rights Campaign (2022) https://www.hrc.org/campaigns/the-state-legislative-attack-on-lgbtq-people.

41 Legislative Tracker, Freedom for All Americans (2022) https://freedomforallamericans.org/legislative-tracker/.

42 LGBT Tech Student Interview (on file with authors).

43 Gabrielle Levy, *LGBTQ Teens Feel Unsafe and Unwelcome, Despite Growing Support for Rights*, U.S. News (May 15, 2018), https://www.usnews.com/news/national-news/articles/2018-05-15/lgbtq-teens-feel-unsafe-and-unwelcome-despite-growing-support-for-rights.

44 *National Survey on LGBTQ Youth Mental Health 2020*, The Trevor Project, https://www.thetrevorproject.org/survey-2020/?section=Housing-Instability. (Last accessed Jan. 30, 2023).

45 Khayaal Desai-Hunt, *Gaggle: MPS's New Student Surveillance Software Brings Possible Protection and Danger*, The Southerner (Mar. 14, 2021), https://www.shsoutherner.net/features/2021/03/14/gaggle-mpss-new-student-surveillance-software-brings-possible-protection-and-danger/.

46 The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99, https://www.law.cornell.edu/uscode/text/20/1232g.

47 Id.

48 LGBT Tech Student Interview (on file with authors).

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

50 *Cops and No Counselors: How the Lack of School Mental Health Staff Is Harming Students*, The American Civil Liberties Union, https://www.aclu.org/sites/default/files/field_document/030419-acluschooldisciplinereport.pdf. (Last accessed Jan. 30, 2023).

51 *Does FERPA distinguish between School Resource Officers (SROs) and other local police officers who work in a school*?, U.S. Department of Education https://studentprivacy.ed.gov/faq/does-ferpa-distinguish-between-school-resource-officers-sros-and-other-local-police-officers-who. (Last accessed Jan. 30, 2023).

52 *Cops and No Counselors: How the Lack of School Mental Health Staff Is Harming Students*, The American Civil Liberties Union, https://www.aclu.org/sites/default/files/field_document/030419-acluschooldisciplinereport.pdf. (Last accessed Jan. 30, 2023).

53 School-Based Risk and Protective Factors for Gender Diverse and Sexual Minority Children and Youth, The American Psychological Association https://www.apa.org/pi/lgbt/programs/safe-supportive/lgbt/risk-factors.pdf. (Last accessed Jan. 30, 2023).

54 Future of Privacy Forum Staff, *The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies: Recommendations for Schools*, Student Privacy Compass (Sept. 2021), https://studentprivacycompass.org/wp-content/uploads/2021/09/FPF-Self-Harm-Report-R4.pdf.

55 LGBT Tech Student Interview (on file with authors).

56 *LGBTQ+ Americans Need Universal Broadband*, LGBT Tech (Oct. 14, 2022) https://www.lgbttech.org/post/lgbtq-americans-need-universal-broadband.

57 Pankey et al. *Gender-Affirming Telepsychology During and After the COVID-19 Pandemic: Recommendations for Adult Transgender and Gender Diverse Populations*, National Library of Medicine (Oct. 16, 2021) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8520334/.

58 Fish et al., "*I'm Kinda Stuck at Home With Unsupportive Parents Right Now": LGBTQ Youths' Experiences With COVID-19 and the Importance of Online Support*, Journal of Adolescent Health, Vol.67, Iss.3 (Sept. 2020) https://www.sciencedirect.com/science/article/pii/S1054139X20303116#sec3.

59 *National Survey on LGBTQ Youth Mental Health 2020*, The Trevor Project, https://www.thetrevorproject.org/survey-2020/?section=Suicide-Mental-Health. (Last accessed Jan. 30, 2023).

60 Id.

61 Senators Elizabeth Warren & Ed Markey, *Constant Surveillance: Implications of Around-the-Clock Online Student Activity Monitoring*, The United States Senate (Mar. 2022) https://www.warren.senate.gov/imo/media/doc/356670%20Student%20Surveillance.pdf.

62 Pupil records: social media, Assembly Bill No. 1442 (Sept. 29, 2014) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140AB1442.

63 Id.

64 Darian Pierre, Amendment to FERPA Needed to Better Serve LGBT Youth, Common Sense (Nov. 26, 2021) https://wearemillardsouth.com/1821/focus/ferpa/.

FUTURE OF PRIVACY FORUM

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | info@fpf.org