Constant Surveillance: Implications of Around-the-Clock Online Student Activity Monitoring

Prepared by Senators Elizabeth Warren and Ed Markey
March 2022

Contents

I. Executive Summary

The coronavirus disease 2019 (COVID-19) pandemic resulted in an explosion of remote learning, which was accompanied by the increased use of online monitoring software. Student activity monitoring tools may use artificial intelligence and algorithmic systems to "provide teachers and schools with the ability to filter web content, monitor students' search engine queries and browsing history, view students' email, messaging, and social media content, view the contents of their screens in real-time, and [use] other monitoring functionality,"[1] to track student activity. Some 81% of teachers in a recent survey indicated that their schools now use at least one type of monitoring software.[2]

Although there are potentially valuable uses of this software, studies have revealed numerous harmful consequences of student surveillance programs that may adversely impact vulnerable populations. Coupled with the increase in usage of these tools among school districts across the country, these findings raise concerns that student activity monitoring software could perpetuate racial and discriminatory biases. In October 2021, Senators Warren and Markey opened an investigation of this online student activity monitoring software, sending letters to four educational technology companies seeking information about the steps each company is taking to ensure the utility of its products and to mitigate discriminatory bias and other potential harms on students.[3]

This report, which contains the results of the investigation, identifies four key findings from the companies' responses:

- **Student activity monitoring software may be misused for disciplinary purposes and result in increased contact with law enforcement.** While the software companies claim that their products are not intended to be used for disciplinary purposes, a survey of teachers found that 43% reported that their schools are using these tools to identify violations of discipline policies.[4] Moreover, as indicated by the companies' responses, the design of these products and activity monitoring outside of school hours intentionally increases the likelihood of student contact with law enforcement. Several of the companies indicated that in certain cases, flagged activities will result in immediate contact of "law enforcement and/or [the National Center for Missing and Exploited Children],"[5] or "police dispatch for a wellness check."[6] Other companies indicated that some districts opt into immediate contact of law enforcement – either when it is "the only option available"[7] or when they "prefer that we contact public safety agencies directly in lieu of a district contact."[8] These products may be exacerbating the school-to-prison pipeline by increasing the involvement of law enforcement with students.

- **Companies have not taken any steps to determine whether student activity monitoring software disproportionately targets students from marginalized groups, leaving schools in the dark.** Data have long indicated that students from marginalized groups, particularly students of color, face disparities in discipline, and more recent studies indicate that algorithms are more likely to flag language used by people of color and LGBTQ+ students as problematic.[9] However, none of the companies have analyzed their algorithms for bias or even track whether their products over- or under-identify different groups of students, or whether their products are disproportionately targeting students of color, LGBTQ+ students.[10]

- **Schools, parents, and communities are not being appropriately informed of the use – and potential misuse – of the data.** Three of the four monitoring software companies indicated that they do not directly alert students and guardians of their surveillance.[11] Instead, parents and students are forced to rely on school districts' common practices of issuing broad notices stating that devices or networks are monitored or that users have "no reasonable expectation of privacy," which do not provide adequate information to families about the privacy risks from these software monitoring products.[12]

- **Regulatory and legal gaps exacerbate the risks of student activity monitoring software.** The concerns raised in this report regarding the use – and potential misuse – of student data and a lack of clear communication between schools and families demonstrate the need for increased coordination between federal agencies such as the Federal Communications Commission (FCC) and Department of Education (ED) to clarify and evaluate existing guidelines for protecting student safety and privacy. There are gaps in federal laws designed to protect students' online privacy, and there is an urgent need for better data collection to determine whether these products pose risks to students' civil rights, and to address these problems when they are found.

The report makes three recommendations. First, the FCC should issue new guidance related to compliance with the *Children's Internet Protection Act* (CIPA) to provide clarification regarding "monitoring the online activities."[13] Defining this term will better inform school districts about what type of monitoring or filtering is required by the law, what risks schools should consider when using student activity monitoring software, and how to appropriately communicate with parents and families about the use of this software. Second, ED should require local education agencies to track the potential impacts of these tools on students in protected classes, including data on the use of student activity monitoring tools for disciplinary purposes and other disparate effects.

Finally, companies that provide student activity monitoring software should use de-identified demographic data to examine the impact of their algorithms on protected classes of students and transparently share the results. This data would better inform schools and families of the risks and benefits of these products and allow the companies to continually refine their products to ensure that they protect students' safety and civil rights.

II. Introduction

As the COVID-19 pandemic forced schools into remote learning in early 2020, many school districts began to purchase new technologies to support a remote learning environment.[14] Many plan to continue to use these technologies post-pandemic, driven at least in part by increasing pressure to adopt new surveillance technologies as part of school security efforts.[15] Several educational technology companies have taken advantage of this pressure by marketing student activity monitoring software – which includes artificial intelligence and algorithmic systems to track students' online activity – as a tool to keep students safe. Gaggle describes its software as "the most proactive tool in digital student safety,"[16] while Securly promises that its "end-to-end solutions platform helps K-12 schools safeguard students, empower educators, and do more than they ever thought possible."[17] GoGuardian makes similar claims, offering products that will allow schools to "unify [their] filtering, classroom engagement, and school mental health tools into a single suite."[18] Gaggle and Bark for Schools even promote their products as tools that "save[s] student lives."[19]

While the intent of these products, many of which monitor students' online activity around the clock, may be to protect student safety, they raise significant privacy and equity concerns. Studies have highlighted unintended but harmful consequences of student activity monitoring software that fall disproportionately on vulnerable populations: artificial intelligence and algorithmic systems frequently mischaracterize students' activity and flag harmless activity as a "threat," and students from minority or marginalized communities, including students of color and LGBTQ+ students, are far more likely to be flagged.[20] Research has shown that language processing algorithms are less successful at analyzing the language of people of color, especially African American dialects.[21] This increases the likelihood that Black students and other students of color will be inappropriately flagged for dangerous activity.[22]

Student monitoring software is often included in a suite or package that may include filtering software that also has disproportionate impacts on marginalized groups. According to mental health advocates and experts, **LGBTQ+ students largely prefer to seek help online,[23] and these monitoring tools' website filtering features frequently prevent them from accessing the health information they seek[24] by flagging words and phrases related to sexual orientation.[25]** The impacts of these shortcomings range from disproportionate disciplinary rates of LGBTQ+ students to unintentional outing of LGBTQ+ students to parents and other adults.[26] In March 2021, a student newspaper in Minnesota reported that, as a result of flagged activity by Gaggle, school administrators outed a student to their parents without first talking to or alerting the student.[27]

In response to these concerns, Senators Warren and Markey wrote in October 2021 to four educational technology companies – Gaggle.net, Bark Technologies, GoGuardian, and Securly Inc. – regarding their student activity monitoring software products that use artificial intelligence (AI) and algorithmic systems to monitor students' online activity.[28] In the letters, the Senators questioned whether these products were surveilling students inappropriately, compounding racial disparities in school discipline, and draining resources from more effective student supports. The Senators expressed concern that the student activity monitoring software provided by these companies extends far beyond the requirement in federal laws to restrict online activity to protect children from exploitation and abuse. All four of these companies responded to the information request, and this report contains a summary of the findings from these responses.

III. Findings

A. Student activity monitoring software may be misused for disciplinary purposes and may result in increased contact with law enforcement, including outside of school hours.

A recent analysis by the Center for Democracy and Technology (CDT) found that a majority of teachers and 61% of parents agree that "student online activity monitoring could bring long-term harm to students if it is used to discipline them or is shared and used out of context."[29] Gaggle and GoGuardian both explicitly stated that their products were not intended to be used for discipline or punitive purposes, including to provide disciplinary recommendations.[30] However, **CDT found that 43% of teachers report that these tools are currently used to identify violations of disciplinary policy.[31]** Research has shown that language processing algorithms are less successful at analyzing language of people of color,[32] increasing the likelihood that students of color are inappropriately flagged for dangerous activity – and ultimately disciplined at higher rates.[33] A school district in Alabama, after beginning to use a social media scanning platform to investigate student accounts, expelled 14 students,[34] 12 of whom were Black students, though only 40% of the total student population is Black.[35] Similarly, one report by Bloomberg highlighted how some schools were monitoring students' online activity for violations of school policies, with one administrator noting that students may be placed in a "penalty box" without access to most online resources for up to an entire semester.[36] School disciplinary measures have a long history of targeting students of color,[37] and these products may contribute to those biases.

Further, **the nature of these products, which in many cases monitor student activity around the clock, allows educators and administrators to track and identify behaviors that may**

result in disciplinary action or referrals to law enforcement, even if they occur outside of schools and during non-traditional school hours. GoGuardian's Admin program has an "Out of School Mode," but the company reported that only 33% of schools use that mode.[38] GoGuardian's Beacon product does not offer an "Out of School Mode," and it continuously monitors activity as long as the student is signed into a school-managed account.[39] The company reported that the majority of alerts are flagged outside of school hours, with the peak volume alert around 5:00-6:00 pm.[40]

Content that is flagged outside of school hours often bypasses school administrators who are unable to respond to flagged activity 24/7. Bark and Gaggle explained that, when an issue is flagged as "imminent," the company will attempt to contact school administrators or district-appointed emergency contacts.[41] But if those contacts do not reply, the company will immediately contact "law enforcement and/or [the National Center for Missing and Exploited Children],"[42] or "police dispatch for a wellness check."[43] **Other companies, including Bark and Securly, stated that some districts opt into immediate contact of law enforcement – either when they deem that doing so is "the only option available"[44] or when "districts prefer that we contact public safety agencies directly in lieu of a district contact."[45]**

Even more troubling, the companies did not provide information on how many law enforcement contacts their products have triggered, and school districts do not publicly disclose this information, making it impossible to know how many students have interacted with law enforcement as a result of student activity monitoring software. During a recent survey, CDT found that the majority of parents are very or somewhat concerned about student data being shared with law enforcement: "When asked about student data being shared with law enforcement, 61 percent of parents expressed that they were very or somewhat concerned; disaggregated by race, 69 percent of Black parents, 54 percent of Hispanic parents, and 62 percent of white parents expressed these concerns."[46]

This direct contact with law enforcement, and a reliance on tools that increase the use of law enforcement in school discipline and safety practices is concerning: **the presence of law enforcement in schools and school police officers have been linked to increased arrests for noncriminal behavior, exacerbating the school-to-prison pipeline.**[47] School police officers, or school resource officers, are "sworn law-enforcement officers with arrest powers" that work in school settings, and the vast majority are armed.[48] Baltimore City schools use the GoGuardian software, and a Baltimore City Councilperson, Ryan Dorsey, tweeted that the school district "monitors students' Chrome books for keyword searches indicating interest in self-harm, and then sends police – not qualified professionals – to intervene."[49] During the school day, GoGuardian alerts are sent to school-based clinicians, but are monitored by school police resource officers during after-school hours, weekends, and holidays.[50] Reports confirm that the city's use of GoGuardian software has resulted in police being sent to children's homes in response to their use of flagged keywords.[51] As of October 2021, GoGuardian had sent 786 alerts from the company's Beacon product, and school police had been sent to students' homes a dozen times.[52]

Surveillance outside of school hours is most likely to affect low-income students, who are more reliant on school-issued devices with these products already installed and less likely to be able to evade constant surveillance through the use of personal devices. GoGuardian explained that, "on personal devices owned by the student or family, the student and/or parent has the ability to disable Admin or Beacon by signing out of the school-managed account."[53] Securly similarly stated that "schools deploy these tools only on school devices, school email systems, and school document systems."[54] One school district even offers a "lease to own" program for school devices, allowing families who purchase a school device to turn off the monitoring software outside of school hours – but this is an opportunity only available to those who can afford to purchase a device.[55] As a result, students without access to personal devices – and the ability to disable these monitoring products – will be monitored at higher rates than students with access to personal devices.

B. Companies have not taken any steps to determine whether student activity monitoring software disproportionately threatens students from marginalized groups, leaving schools in the dark.

Despite evidence that students from marginalized groups, particularly students of color, face disparities in discipline, the software companies do not track the impact of their products by race and ethnicity,[56] meaning that they have no way of identifying or rectifying adverse impacts. In one response, Bark acknowledged the history of bias in school discipline issues, while asserting – without evidence – that its product has "substantially less bias than school personnel."[57] Similarly, the companies indicated that they are unable to identify these occurrences or determine whether LGBTQ+ students are disproportionately affected by their products. **Indeed, all four companies stated that they are unable to track disparate impacts of their products.**

All four companies cited privacy concerns as reasons they are not conducting studies on the bias or potential harmful effects of their products.[58] GoGuardian stated, "To protect the privacy of students, Admin and Beacon do not collect student-level demographic data."[59] The company continued, "Because the products are designed to collect minimal [personally identifiable information], GoGuardian cannot currently perform rigorous and precise analyses of algorithmic biases related to any student-level demographic or socio-economic data."[60] Similarly, Bark stated, "Because we do not collect any student sexual identity or preference information, we cannot analyze results by protected class." Securly similarly explained, "We do not collect data on student's race, ethnicity, or sexual orientation and therefore do not have access to information on how many flagged incidents come from students of color and/or LGBTQ+ students."[61] And in response to the question regarding how the company tracks disproportionate effects on students in a protected class, the company replied, "We do not track that information."[62] Finally, while Gaggle's CEO recently stated, "We're doing everything we can to make sure that we don't have any bias in our algorithms and our decision-making,"[63] the company's response indicated that the company is unable to track disparate impacts on marginalized students, stating, "We have no context or background on students when we first identify potential issues, ensuring that all students get the support they need – regardless of demographic factors like race, income level, or sexual orientation."[64]

But these excuses for the companies' failure do not make sense. Per their responses, all four of these companies are already collecting extremely sensitive personally identifiable information about students (e.g. whether a student is considering self-harm), so they could easily pair that sensitive information with student demographics to better understand if their product is inflicting disproportionate harm on students.[65] Moreover, in order for them to monitor student activity on behalf of school districts, school districts must maintain direct control of this information, which is typically accomplished through a data sharing agreement. Companies could add a limited set of student demographic variables like race and income to this agreement, and this information by comparison is less sensitive than some of the information these companies already collect.

Additionally, the companies would not need to retain individual-level student demographics as nearly all of the companies described their processes for training the artificial intelligence and processing systems, which involve collecting and de-identifying personally identifiable data. **The companies explicitly stated that they use aggregated or de-identified data to train their products.**[66] **The same process of collecting aggregated data that includes student demographics and removing identifying information could also be used to study the disparate effects of these surveillance products on students in protected classes, either for all students using the product or for a representative sample.**

Nonetheless, the companies claim that they are unable to collect and use data to evaluate the bias of their products. This refusal to examine whether their algorithms reflect racial and societal biases ensures that schools and families will remain in the dark about any disproportionate impacts of surveillance on different protected groups of students. **Recent studies indicate that algorithms are more likely to flag language used by people of color and LGBTQ+ students as problematic.**[67] One study found that popular AI models were one-and-a-half times more likely to label tweets written by African Americans as offensive and twice as likely to flag tweets written in African American English.[68] Another study examined racial bias in hate speech detection datasets, and found similar evidence of racial bias against Black speech.[69]

C. Schools, parents, and communities are not being appropriately informed of the use – and potential misuse – of students' data.

Many schools rely on these software monitoring products, installing them on all school-issued devices and accounts, while failing to adequately communicate to parents and students the extent of the products' capabilities and the potential harm they may cause. **One in four parents surveyed by the CDT report that they are "not sure" if their school uses monitoring software.**[70] This suggests that school districts' common practice of issuing broad notices stating that devices or networks are monitored or that users have "no reasonable expectation of privacy" is not providing adequate information to families about the privacy risks from the software monitoring products they use.[71]

Three of the four software monitoring companies indicated that they do not directly alert students and guardians of their surveillance.[72] Bark stated that it "encourage[s] schools to be fully transparent with students and their parents about the usage of [its] products"[73]; Gaggle stated that it "makes available to schools and school districts the information that they need to provide sufficient notice to parents"[74]; and Securly stated it "provides a parent kit to all districts," "strongly encourage[s] these districts to send these kits to parents at the beginning of each school year," and "posts privacy policies, terms of use, and related materials to its website that outline how [the company] processes data among other things."[75] Bark and Securly also cited an inability to dictate how schools communicate with their students and parents and an indirect relationship with parents and students to justify their approaches.[76]

GoGuardian was the only company that affirmatively indicates when the technology is deployed and active on a device, via a GoGuardian Shield icon that appears in the device's toolbar.[77] GoGuardian also reported employing a session indicator that persistently appears on the browser window of school-managed devices, accounts, and networks to remind users that the device, account, or network is being monitored.[78] Like other companies, GoGuardian also provides schools with template parent letters that encourage schools to send technology acceptable use agreements to parents and students, and has a privacy and trust resource center available on their website.[79]

Students also expressed limited awareness of potential privacy implications around the use of this technology – and those that were aware indicated that they are self-censoring in response.[80] **Fifty eight percent of students surveyed agreed with the statement, "I do not share my true thoughts or ideas because I know what I do online is being monitored."**[81] **And 80 percent of students reported being "more careful about what I search online when I know what I do online is being monitored."**[82] When discussing his school's use of GoGuardian, one student stated, "I know everything I type into Google Docs is being sent to an algorithm to see if I have suicidal tendencies, so I have to rethink what I'm doing."[83] These findings raise concerns that students may be hesitant to search and access important online resources, including those related to mental health, if they are fearful that searches will result in flagged activity and, potentially, disciplinary action or other unintended consequences.[84]

Further, when asked if families are able to opt out of online monitoring, all four companies stated that the decision is up to school districts, who are able to implement opt-out policies at their discretion.[85] This is aligned with the companies' largely hands-off approaches to family communication. Overall, beyond publicly available or vague guidance, the companies do not have specific communication plans or requirements for school districts that use their software to inform students and their families about their use – and potential misuse – of student data.

D. Regulatory and legal gaps exacerbate the risks of student activity monitoring software.

School districts' intent in using student monitoring software to promote student safety is important.[86] However, as this report has highlighted, there are significant concerns regarding the use – and potential misuse – of student data and a lack of clear communication between schools and families. **These risks show the need for increased coordination between federal agencies to protect student safety and privacy.**

The *Family Educational Rights and Privacy Act* (FERPA) protects the privacy of student education records, such as grades, transcripts, and contact information.[87] However, student data such as browsing history and online activity may not be covered by this protection. There is currently no federal law designed to comprehensively protect students' online privacy.

Many education agencies purport to use student activity monitoring software as a compliance tool for the *Children's Internet Protection Act* (CIPA).[88] CIPA was intended to address concerns about children's access to obscene or harmful content over the Internet, and requires schools and libraries that receive federal funding to filter and monitor online activity to prevent children from accessing "visual depictions" that are constitutionally obscene, child pornography, or "harmful to minors."[89] CIPA is implemented by the Federal Communications Commission (FCC), which establishes rules for districts regarding what filtering and monitoring activity is necessary and appropriate.

However, these rules are not designed to address the myriad risks posed by student monitoring software, and the software's data collection is used for purposes that extend well beyond CIPA. For example, Securly indicated that "Congress' direction for always-on monitoring of school computers for harmful materials helps to protect students,"[90] though it is important to note that there is no language in CIPA that requires "always-on" monitoring. The company then states, "Securly's Filter product provides the traditional web filtering required by CIPA, but this is just a portion of the services that Securly offers to help schools protect students."[91] The company explained that its other surveillance programs, including Auditor and 24, are offered "not as CIPA compliance solutions but rather as tools that help schools monitor for indicators that could signal these behaviors," such as signs of anxiety or depression.[92] Because of the lack of clarity in the definition of "monitoring the online activities"[93] and an absence of regulations to prevent these products' unintended consequences, school districts believe that constant monitoring of student activity is required by CIPA,[94] when in fact it goes well beyond the original purpose of the law.

In addition, the lack of information regarding potential biases and disproportionate impacts on marginalized student groups raises concerns that student activity monitoring software could interfere with students' civil rights. Title IV of the *Civil Rights Act of 1964* prohibits discrimination based on race, color, and national origin, and Title IX of the Education Amendments of 1972 prohibits sex discrimination in educational institutions, including discrimination based on sexual orientation and gender identity.[95] Both statutes also protect students from policies or practices that may have disparate impacts on students due to their race, sex, or gender identities.[96] **If student surveillance products lead to disproportionate discipline and increased contact with law enforcement for students of color and LGBTQ+ students, then they may violate schools' obligations of equal access to education for these student groups.**

IV. Recommendations

Absent federal action, these surveillance products may continue to put students' civil rights, safety, and privacy at risk. Given these risks, the federal government should seek methods to track the potential impacts of student surveillance technology on students in protected classes, clarify the definition of "monitoring the online activities" as mentioned in CIPA,[97] and work to ensure that products used by schools maintain student safety and privacy.

First, the FCC should issue new guidance related to CIPA compliance. The FCC has issued guidance twice since the passage of CIPA, in 2001 and 2011,[98] but has yet to provide clarification regarding "monitoring the online activities."[99] Defining this term will better inform school districts by providing them with increased clarification regarding CIPA, including what type of monitoring or filtering is required by the law, risks that schools should consider when using student activity monitoring software, and appropriate communication with parents and families.

Second, the Department of Education (ED) should require local education agencies to track the potential impacts of these tools on students in protected classes. ED already uses existing surveys, such as the Civil Rights Data Collection, to identify disproportionate rates of discipline for students of color and students with disabilities.[100] Similarly, it should collect data on the use of student activity monitoring tools for disciplinary purposes and other disparate effects. Proposed Civil Rights Data Collection questions this year will already collect data on remote learning. As school districts emerge from the pandemic and re-examine the use of remote learning tools, including student activity monitoring software, the addition of questions related to potential biases and harmful effects of student activity monitoring software would provide meaningful insight into privacy and equity implications these tools have on students.

Finally, companies that provide student activity monitoring software should use de-identified demographic data to examine the impact of their algorithms on protected classes of students and transparently share the results. This data would better inform schools and families of the risks and benefits of these products and allow the companies to continually refine their products to ensure that they protect students' safety and civil rights.

Endnotes

[1] Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 21, 2021, pp. 1, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

[2] Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 21, 2021, pp. 2, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

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

[4] Center for Democracy and Technology, “Views on Student Activity Monitoring Software: Research and analysis from online surveys of teachers, parents, and students,” September 2021, pp. 7, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Polling-Research-Slides.pdf.

[5] Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

[6] Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21.

[7] Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

[8] Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final.

[9] Paul G. Allen School of Computer Science & Engineering, University of Washington, Machine Learning Department, Carnegie Mellon University, and Allen Institute for Artificial Intelligence, “The Risk of Racial Bias in Hate Speech Detection,” Maarten Sap, Dallas Card, Saadia Gabriel, Yejin Choi, Noah A. Smith, July 2019, https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf; arXiv, Cornell University, “Racial Bias in Hate Speech and Abusive Language Detection Datasets,” Thomas Davidson, Debasmita Bhattacharya, Ingmar Weber, May 2019, https://arxiv.org/pdf/1905.12516.pdf.

[10] “Letter From Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21; “Letter From Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final; “Letter from Bark to Senator Elizabeth Warren, October, 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.; “Letter From GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

[11] Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21; Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final; Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

[12] Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 2021, pp. 6, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

[13] 47 U.S.C. § 254(h)(5)(B).

[14] New York Times, “Online Schools Are Here to Stay, Even After the Pandemic,” Natasha Singer, April 11, 2021, https://www.nytimes.com/2021/04/11/technology/remote-learning-online-school.html.

[15] Washington Post, “How the pandemic is reshaping education,” Donna St. George, Valerie Strauss, Laura Meckler, Joe Heim, and Hannah Natanson, March 15, 2021, https://www.washingtonpost.com/education/2021/03/15/pandemic-school-year-changes/; KQED, “When School Safety Becomes School Surveillance,” Anya Kamenetz and Jessica Bakeman, September 12, 2019, https://www.kqed.org/mindshift/54396/when-school-safety-becomes-school-surveillance; Washington Post, “Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance,” Drew Harwell, April 1, 2020, https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/.

[16] Gaggle, “Gaggle Safety Management,” https://www.gaggle.net/safety-management?hsCtaTracking=6a2495bb-4095-4ea0-8238-60e5a008e2bc%7C1dbd8599-9c0b-404d-b939-1dce1151042f.

[17] Securly, “Securly,” https://www.securly.com/.

[18] GoGuardian, “GoGuardian,” https://www.goguardian.com/.

[19] Gaggle, “Gaggle,” https://www.gaggle.net/; Bark for Schools, “Content Monitoring for G Suite and Microsoft 365,” https://www.bark.us/schools/computer-content-monitoring.

[20] Center for Democracy and Technology, “Algorithmic Systems in Education: Incorporating Equity and Fairness when Using Student Data,” Hannah Quay-de la Vallee and Natasha Duarte, August 2019, pp. 12, https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf; Buzzfeed News, “Gaggle Knows Everything About Teens And Kids In School,” Caroline Haskins, November 1, 2019, https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education.

[21] arXiv, Cornell University, “Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English,” Su Lin Blodgett and Brendan O’Connor, June 30, 2017, pp. 1-2, https://arxiv.org/abs/1707.00061.

[22] Center for Democracy and Technology, “Algorithmic Systems in Education: Incorporating Equity and Fairness when Using Student Data,” Hannah Quay-de la Vallee and Natasha Duarte, August 2019, pp. 12, https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf.

[23] The Trevor Project, “The Trevor Project National Survey on LGBTQ Youth Mental Health 2019,” June 2019, pp. 6, https://www.thetrevorproject.org/wp-content/uploads/2019/06/The-Trevor-Project-National-Survey-Results-2019.pdf.

[24] Vice, “Schools Use Software That Blocks LGBTQ+ Content, But Not White Supremacists,” Todd Feathers, April 28, 2021, https://www.vice.com/en/article/v7em39/schools-use-software-that-blocks-lgbtq-content-but-not-white-supremacists.

[25] Id.

26 The Southerner, “Gaggle: MPS’s new student surveillance software brings possible protection and danger,” Khayaal Desai-Hunt, March 14, 2021, https://www.shsoutherner.net/features/2021/03/14/gaggle-mpss-new-student-surveillance-software-brings-possible-protection-and-danger/.

27 Id.

28 Office of Senator Elizabeth Warren, “Warren, Markey, Blumenthal Raise Concerns About Discriminatory Bias in EdTech Student Surveillance Platforms and Harmful Effects on Students’ Mental Health,” October 4, 2021, https://www.warren.senate.gov/oversight/letters/warren-markey-blumenthal-raise-concerns-about-discriminatory-bias-in-edtech-student-surveillance-platforms-and-harmful-effects-on-students-mental-health.

29 Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 21, 2021, pp. 2, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

30 Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21; Letter from GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

31 Center for Democracy and Technology, “Views on Student Activity Monitoring Software,” September 2021, pp. 7, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Polling-Research-Slides.pdf.

32 arXiv, Cornell University, “Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English,” Su Lin Blodgett and Brendan O’Connor, June 30, 2017, pp. 1-2, https://arxiv.org/abs/1707.00061.

33 Center for Democracy and Technology, “Algorithmic Systems in Education: Incorporating Equity and Fairness when Using Student Data,” Hannah Quay-de la Vallee and Natasha Duarte, August 2019, pp. 12, https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf.

34 Al.com, “Huntsville schools paid $157,000 for former FBI agent, social media monitoring led to 14 expulsions,” Challen Stephens, March 6, 2019, https://www.al.com/news/huntsville/2014/11/huntsville_schools_paid_157100.html.

35 Id.

36 Bloomberg Government, “Big Teacher Is Watching: Spyware Business Sneaks Into Schools,” Priya Anand and Mark Bergen, October 28, 2021, https://news.bloomberglaw.com/privacy-and-data-security/big-teacher-is-watching-spyware-business-sneaks-into-schools.

37 Washington Post, “Racial disparities in school discipline are growing, federal data show,” Moriah Balingit, April 24, 2018, https://www.washingtonpost.com/local/education/racial-disparities-in-school-discipline-are-growingfederal-data-shows/2018/04/24/67b5d2b8-47e4-11e8-827e-190efaf1f1ee_story.html.

38 Letter from GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

39 Id.

40 Id.

41 Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal; Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21.

42 Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

43 Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21.

44 Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

45 Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final.

46 Center for Democracy and Technology, “Navigating the New Normal: Ensuring Equitable and Trustworthy EdTech for the Future”, November 2021, https://cdt.org/wp-content/uploads/2021/11/CDT-Civic-Tech-Research-Online-Learning-Report-Final.pdf.

47 Brookings, “A better path forward for criminal justice: Reconsidering police in schools,” Ryan King and March Schindler, April 2021, https://www.brookings.edu/research/a-better-path-forward-for-criminal-justice-reconsidering-police-in-schools/; New York Times, “Do Police Officers Make Schools Safer or More Dangerous?,” Dana Goldstein, October 28, 2021, https://www.nytimes.com/2020/06/12/us/schools-police-resource-officers.html.

48 Education Week, “School Resource Officers (SROs) Explained,” Stephen Sawchuck, November 16, 2021, https://www.edweek.org/leadership/school-resource-officer-sro-duties-effectiveness#:~:text=A%20school%20resource%20officer%20is,restraints%20like%20handcuffs%20as%20well.

49 Tweet by Ryan Dorsey, September 29, 2021, https://twitter.com/ElectRyanDorsey/status/1443369691351760897?s=20&t=Yv-XMbTWuWLUY5TfGs9GhQ.

50 Tweet by Baltimore City Public Schools, September 30, 202, https://twitter.com/BaltCitySchools/status/1443613938000793603?s=20&t=S94-eiTMIseA52KEnnFD5g.

51 The Real News Network, “Cops in Baltimore Schools are Monitoring Students’ Laptops,” Jaisal Noor, October 4, 2021, https://therealnews.com/cops-in-baltimore-schools-are-monitoring-students-laptops.

52 Baltimore Sun, “Baltimore City student laptops are monitored for mentions of suicide. Sometimes, the police are called.,” Liz Bowie, October 12, 2021, https://www.baltimoresun.com/education/bs-md-laptops-monitoring-20211012-a2j3vsytijhhjj36n57ri5zdhi-story.html.

53 Letter from GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

54 Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final.

55 Education Week, “Teachers Are Watching Students’ Screens During Remote Learning. Is That Invasion of Privacy?” Stephen Sawchuk, April 2, 2021, https://www.edweek.org/technology/are-remote-classroom-management-tools-that-let-teachers-see-students-computer-screens-intrusive/2021/04.

56 “Letter From Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21; “Letter From Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final; “Letter from Bark to Senator Elizabeth Warren, October, 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal; “Letter From GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

57 Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

58 Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate-response-letter_10_12_21; Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final; Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal; Letter from GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

59 Letter from GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

60 Letter from GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

61 Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final.

62 Id.

63 NPR, “Remote learning ushered in a new era of online academic surveillance. What’s next?,” January 12, 2022, 25:50, https://the1a.org/segments/remote-learning-ushered-in-a-new-era-of-online-academic-surveillance-whats-next/.

64 Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21.

65 Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21; Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final; Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal; Letter from GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

66 Id.

67 Paul G. Allen School of Computer Science & Engineering, University of Washington, Machine Learning Department, Carnegie Mellon University, and Allen Institute for Artificial Intelligence, “The Risk of Racial Bias in Hate Speech Detection,” Maarten Sap, Dallas Card, Saadia Gabriel, Yejin Choi, Noah A. Smith, July 2019, https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf; arXiv, Cornell University, “Racial Bias in Hate Speech and Abusive Language Detection Datasets,” Thomas Davidson, Debasmita Bhattacharya, Ingmar Weber, May 2019, https://arxiv.org/pdf/1905.12516.pdf.

68 Paul G. Allen School of Computer Science & Engineering, University of Washington, Machine Learning Department, Carnegie Mellon University, and Allen Institute for Artificial Intelligence, “The Risk of Racial Bias in Hate Speech Detection,” Maarten Sap, Dallas Card, Saadia Gabriel, Yejin Choi, Noah A. Smith, July 2019, pp. 4, https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf.

69 arXiv, Cornell University, “Racial Bias in Hate Speech and Abusive Language Detection Datasets,” Thomas Davidson, Debasmita Bhattacharya, Ingmar Weber, May 2019, https://arxiv.org/pdf/1905.12516.pdf.

70 Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 2021, pp. 5, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

71 Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 2021, pp. 6, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

72 Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21; Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final; Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

73 Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

74 Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21.

75 Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final.

76 Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal; Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final.

77 Letter from GoGuardian to Senator Elizabeth Warren, October 26, 2021, https://www.warren.senate.gov/download/goguardian-response-_-re_edtech-letter.

78 Id.

79 Id.

80 Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 2021, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

81 Center for Democracy and Technology, “CDT Original Research Examines Privacy Implications of School-Issued Devices and Student Activity Monitoring Software,” September 21, 2021, https://cdt.org/insights/cdt-original-research-examines-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/.

82 Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 2021, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

83 Education Week, “Teachers Are Watching Students’ Screens During Remote Learning. Is That Invasion of Privacy?,” Stephen Sawchuk, April 2, 2021, https://www.edweek.org/technology/are-remote-classroom-management-tools-that-let-teachers-see-students-computer-screens-intrusive/2021/04.

[84] Id.

[85] Letter from Gaggle to Senator Elizabeth Warren, October 12, 2021, https://www.warren.senate.gov/download/gaggle_senate_response_letter_10_12_21; Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final; Letter from Bark to Senator Elizabeth Warren, October 22, 2021, https://www.warren.senate.gov/download/bark_-letter-to-senators-warren-markey-and-blumenthal.

[86] KQED, “When School Safety Becomes School Surveillance,” Anya Kamenetz and Jessica Bakeman, September 12, 2019, https://www.kqed.org/mindshift/54396/when-school-safety-becomes-school-surveillance; Washington Post, “Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance,” Drew Harwell, April 1, 2020, https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/.

[87] 20 U.S.C. § 1232g; 34 CFR Part 99.

[88] Center for Democracy and Technology, “Student Activity Monitoring Software: Research Insights and Recommendations,” September 21, 2021, pp. 6, https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Research-Insights-and-Recommendations.pdf.

[89] 47 U.S.C. § 254(h)(5)(B); Federal Communications Commission, “Children’s Internet Protection Act (CIPA),” updated December 30, 2019, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

[90] Letter from Securly to Senator Elizabeth Warren, October 15, 2021, https://www.warren.senate.gov/download/securly-senate-response-final.

[91] Id.

[92] Id.

[93] 47 U.S.C. § 254(h)(5)(B).

[94] Center for Democracy and Technology, “Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software,” September 2021, pp.11-12, https://cdt.org/wp-content/uploads/2021/09/Online-and-Observed-Student-Privacy-Implications-of-School-Issued-Devices-and-Student-Activity-Monitoring-Software.pdf.

[95] Bostock v. Clayton County, 140 S. Ct. 1731 (2020); U.S. Department of Education, “Enforcement of Title IX of the Education Amendments of 1972 With Respect to Discrimination Based on Sexual Orientation and Gender Identity in Light of Bostock v. Clayton County,” 86 Fed. Reg. 32637, June 22, 2021, https://www.federalregister.gov/documents/2021/06/22/2021-13058/enforcement-of-title-ix-of-the-education-amendments-of-1972-with-respect-to-discrimination-based-on.

[96] 34 CFR § 100.3(b)(2) (Title VI); 34 C.F.R. § 106.21(b)(2), 106.36(b), 106.52 (Title IX).

[97] 47 U.S.C. § 254(h)(5)(B).

[98] Federal Communications Commission, “Children’s Internet Protection Act (CIPA),” updated December 30, 2019, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

[99] 47 U.S.C. § 254(h)(5)(B).

[100] U.S. Department of Education, Office for Civil Rights, “An Overview of Exclusionary Discipline Practices In Public Schools for the 2017-18 School Year,” June 2021, https://www2.ed.gov/about/offices/list/ocr/docs/crdc-exclusionary-school-discipline.pdf.