United States Senate
WASHINGTON, DC 20510

September 29, 2021

Advait Shinde
Co-Founder and CEO
GoGuardian
2030 E. Maple Ave, Suite 100
El Segundo, CA 90245

Dear Addressee:

We are writing regarding your company's use of artificial intelligence and algorithmic systems to monitor students' online activity. Your company and other education technology companies have developed software that are advertised to protect student safety, but may instead be surveilling students inappropriately, compounding racial disparities in school discipline, and draining resources from more effective student supports. A new report from the Center for Democracy and Technology revealed that the recent expansion of remote learning increased the use of online monitoring software to track student activity, with 81% of teachers stating that their schools now use at least some type of monitoring software.[1] We are seeking information on: (1) the steps your company is taking to ensure that the products you are developing for use in schools are not unfairly targeting students and perpetuating discriminatory biases; and (2) how you are ensuring that your company, and school districts using your products, preserve student privacy and follow relevant federal laws.

As the country began to respond to the COVID-19 pandemic, state education agencies and school districts were forced to make a rapid transition to online learning.[2] This disruption in traditional classroom learning caused many school districts to search for and purchase new technologies to support a remote learning environment.[3] The upward trend of digital education platforms is likely to outlast the pandemic:[4] a Fall 2020 survey found that one in five school districts indicated they had adopted or were planning to adopt virtual school as part of their

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

[2] United Nations Educational, Scientific, and Cultural Organization, "Education: From disruption to recovery," https://en.unesco.org/covid19/educationresponse; World Economic Forum, "The COVID-19 pandemic has changed education forever. This is how," Cathy Li and Farah Lalani, April 29, 2020, https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/.

[3] 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.

[4] 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/?itid=lk_interstitial_manual_75.

district's educational strategy after the pandemic.[5] As school leaders look ahead toward the coming school years, they are evaluating whether and how to incorporate these online tools into their long-term plans. At the same time, they are also facing pressure to adopt or maintain new surveillance technologies as a part of school security efforts,[6] some of which involve local law enforcement and provide immediate access to live footage of children on school cameras.[7]

Your company and its peers have taken advantage of this pressure by marketing technology based on artificial intelligence and algorithmic systems, promising effective and efficient methods for keeping students safe. These technologies use artificial intelligence to monitor students' online activity to flag safety "threats" for parents, school administrators, and even law enforcement officials.[8] This includes tracking the websites students visit and identifying trends when students use school devices or are signed into school accounts.[9] These programs also scan students' activity across social media, e-mail accounts, chat messages and chats, online calendars, online file storage, e-mail attachments, search engines, web applications, and other account activity.[10] Several companies provide 24/7 monitoring of school-issued devices, whether the student is on or off campus, and many can even monitor a student's activity from personal devices.[11]

Specifically, Gaggle claims to offer "the most comprehensive student safety offering on the market," reviewing student activity across Google Workspace for Education, Microsoft 365, and Canvas including e-mail messages, attachments, images, documents, PDFs, links to websites, and more.[12] Similarly, Bark for Schools offers "powerful AI" that "scans G Suite and

[5] Rand Corporation, "Remote Learning Is Here to Stay," Heather L. Schwartz, David Grant, Melisa Kay Diliberti, Gerald P. Hunter, Claude Messan Setodji, December 2020, https://www.rand.org/pubs/research_reports/RRA956-1.html.

[6] 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/.

[7] Boston Globe, "'I don't want the police involved in my kids' education': A fight brews over video surveillance of students in Western Mass.," Pranshu Verma, July 13, 2021, https://www.bostonglobe.com/2021/07/13/business/i-dont-want-police-involved-my-kids-education-fight-brews-over-video-surveillance-students-western-mass.

[8] USA Today, "Can artificial intelligence prevent the next Parkland shooting?" Edward C. Baig, February 14, 2019, https://www.usatoday.com/story/tech/2019/02/13/preventing-next-parkland-artificial-intelligence-may-help/2801369002/.

[9] *Id.*

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

[11] The Guardian, "Under Digital Surveillance: How American Schools Spy on Millions of Kids," Lois Beckett, October 22, 2019, https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle; EdWeek, "Teachers are Watching Students' Screens During Remote Learning. Is That Invastion of Privacy?" Stephen Sawchuk, April 2, 20201, https://www.edweek.org/technology/are-remote-classroom-management-tools-that-let-teachers-see-students-computer-screens-intrusive/2021/04.

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

Microsoft 365 accounts (including emails, chats, and files),"[13] and "also provide[s] a web filtering feature that allows administration to block and allow domains at the IP and DNS level."[14] Beyond scanning activity linked directly to school accounts, because a large number of school districts use Chromebooks, Bark for Schools also offers a Chrome extension to monitor any activity conducted on this web browser.[15] The company explains, "while students can log out of G Suite or Office 365 accounts, Chromebook users are generally unable to circumvent our monitoring service because the browser is native to the device."[16] GoGuardian similarly claims to offer "the most powerful all-in-one suite to manage your school's 1:1 technology."[17] Beyond Google Chrome and Microsoft Office, GoGuardian Beacon "works across search engines, chat, social media, email, web apps, and more."[18] And Securly Inc. claims to go even farther, offering a range of products, from a "signature cloud-based web filter to the best 24/7 human-enhanced AI on the market—all in one end-to-end solution for any device, any browser" with unlimited data retention.[19] Each of these companies use artificial intelligence and algorithmic systems to monitor nearly all student activity under the guise of student safety.

We are concerned these products may extend far beyond the direction in federal laws to monitor online activity to protect children from exploitation and abuse. The Children's Internet Protection Act (CIPA), which Congress passed in 2000, requires schools and libraries that receive federal funding to filter and monitor online activity to prevent children from accessing material that is "harmful to minors."[20] Many education agencies use this law to justify the use of technologies such as yours. However, while your company claims to protect students from harmful content, we are concerned that your company's products may extend beyond the intent of CIPA to serve to surveil student activity or reinforce biases.

Because of the lack of transparency, many students and families are unaware that nearly all of their children's online behavior is being tracked.[21] When students and families are aware, they are often unable to opt out because school-issued devices are given to students with the software already installed, and many students rely on these devices for remote or at-home learning.[22] While some students are able to avoid constant monitoring of their online activity by using personal devices, this is a luxury that not all students and families are able to afford. The Center for Democracy and Technology found that 71% of teachers report using monitoring software on school-issued devices, while only 16% of teachers report using the software on

[13] Bark for Schools, "Bark for Schools," https://www.bark.us/schools.

[14] Bark for Schools, "Monitoring Accounts for School Safety: AI, Data, & Technology," https://bark-assets.s3.amazonaws.com/guides/AI_Data_Technology_BarkForSchools.pdf

[15] *Id.*

[16] *Id.*

[17] GoGuardian, "GoGuardian" https://www.goguardian.com/

[18] GoGuardian, "GoGuardian Beacon," https://www.goguardian.com/beacon/.

[19] Securly, "360 Cloud," https://www.securly.com/360-cloud-comparison.

[20] 47 CFR 54.520

[21] The Guardian, "Under Digital Surveillance: How American Schools Spy on Millions of Kids," Lois Beckett, October 22, 2019, https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

[22] 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.

personal devices.[23] This suggests that students in higher-poverty districts are likely subject to more monitoring than those in higher-income districts, who are more likely to have access to personal devices.[24]

Still, many of the programs also track students' activity on personal devices when they are signed into certain school accounts, which students often need to complete school assignments. In some cases, as long as students are using school-issued devices or are signed into their school Google Suite or Microsoft 365 accounts, regardless of students' geographic location and time of day, their activity is monitored 24/7.[25] The Center of Democracy and Technology found that only one in four teachers report that monitoring is specifically limited to school hours, with nearly one in three stating that student activity monitoring is conducted all of the time.[26] This is a clear invasion of student privacy, particularly when students and families are unable to opt out.

Recent studies have highlighted numerous unintended but harmful consequences of student surveillance programs that target vulnerable populations.[27] Artificial intelligence and algorithmic systems frequently mischaracterize students' activity and flag harmless activity as a "threat." Students from minority or marginalized communities, including students of color and LGBTQ+ students, are far more likely to be flagged.[28] Research has shown that language processing algorithms are less successful at analyzing language of people of color, especially African American dialects.[29] This increases the likelihood that Black students and other students of color will be inappropriately flagged for dangerous activity.[30] For example, a social media scanning platform used by a school district in Alabama to investigate student accounts resulted in

[23] 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.

[24] 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.

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

[26] 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.

[27] American Civil Liberties Union, "Student Surveillance Versus Gun Control: The School Safety Discussion We Aren't Having," Chad Marlow, March 4, 2019, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/student-surveillance-versus-gun-control-school.

[28] 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.

[29] 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.

[30] 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.

the expulsion of 14 students,[31] 12 of which were Black students, although only 40% of the total student population is Black.[32] School disciplinary measures have a long history of disproportionately targeting students of color, who face substantially more punitive discipline than their white peers for equivalent offenses.[33] These disciplinary records, even when students are cleared, may have life-long harmful consequences for students.[34] A majority of teachers and parents are concerned that online monitoring could harm students if it is used for discipline or is shared and used out of context.[35] It would be troubling if the use of online monitoring tools serves as yet another means to perpetuate racial bias and disproportionate disciplinary actions against marginalized students.

Additionally, the use of these tools may break down trust within schools, prevent students from accessing critical health information, and discourage students from reaching out to adults for help,[36] potentially increasing the risk of harm for students. According to mental health advocates and experts, LGBTQ+ students are more likely to seek help online,[37] and these tools frequently prevent them from accessing the health information they seek due to website filtering by student surveillance programs.[38] The policing of students' online activity may also be further discouraging students of color and LGBTQ+ students from reaching out to adults for help,[39] leaving students without critical information and support.

These escalations and mischaracterizations of crises may have long-lasting and harmful effects on students' mental health due to stigmatization and differential treatment following even a false report.[40] Research has shown that physicians treat patients who have been considered

[31] 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.

[32] *Id*.

[33] 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-growing-federal-data-shows/2018/04/24/67b5d2b8-47e4-11e8-827e-190efaf1f1ee_story.html.

[34] 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.

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

[36] The eQuality Project, "Digital Surveillance in the Networked Classroom," Valerie Steeves, Priscilla Regan, and Leslie Regan Shade, 2018, pp. 4-6, http://www.equalityproject.ca/wp-content/uploads/2017/05/7-Digital-Surveillance-in-the-Networked-Classroom.pdf.

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

[38] 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.

[39] The eQuality Project, "Digital Surveillance in the Networked Classroom," Valerie Steeves, Priscilla Regan, and Leslie Regan Shade, 2018, pp. 4-6, http://www.equalityproject.ca/wp-content/uploads/2017/05/7-Digital-Surveillance-in-the-Networked-Classroom.pdf.

[40] Yale Journal of Law and Technology, "Artificial Intelligence-Based Suicide Prevention," Mason Marks, https://yjolt.org/sites/default/files/21_yale_j.l._tech._special_issue_98.pdf.

"high-risk" differently from other patients, [41] and flagging students as "high-risk" may put them at risk of biased treatment from physicians and educators in the future. In other extreme cases, these tools can become analogous to predictive policing, which are notoriously biased against communities of color.[42] The resources that school districts are expending on these programs – which are reported to be up to $60,000 per year in some cases[43] – could instead be invested in local human support services, such as counselors or other school-based mental health professionals, who can develop relationships and trust with students to safeguard their well-being and prevent mental health episodes.

We strongly support measures that will protect students and ensure student safety, and we share the urgency that school districts are facing to identify ways to keep students safe. As school districts look ahead, they must decide which safety tools and systems to use in order to protect student safety. Under Title IV of the Every Student Succeeds Act (ESSA), U.S. school districts can use federal dollars to fund initiatives that protect student safety.[44] Many districts are even required to use some funding on technology, which can include student surveillance services.[45] It is crucial that the tools school districts select will keep students safe while also protecting their privacy, and that they do not exacerbate racial inequities and other unintended harms.

In order to better understand the efforts your company is taking to ensure the efficacy of your products and to mitigate potential harms they may impose on students, we are requesting answers to the following questions no later than October 12, 2021:

1. What student activity monitoring software has your company developed for use in school districts?
2. How do these products work to identify threats to or risks from students? Please describe the process for flagging content, including the use of artificial intelligence and human reviews; how those flags are reported to schools, law enforcement, or other entities; and what procedures are in place to protect students.
3. How many school districts have purchased and/or are currently using your products?
4. How much does your company charge school districts for use of your services?
    a. Please provide a comparison of the free and premium services you provide to schools. Please include whether data privacy measures differ across services.
5. How do you test for and correct bias in your products during the design and development process?
    a. In particular, do you test your training data and models for bias against particular groups of students, including students of color and LGBTQ+ students?

[41] *Id.*

[42] ACLU, "Statement of Concern about Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations," August 31, 20216, aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice.

[43] 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.

[44] National Association of Secondary School Principals, "Title IV – 21st Century Schools," https://www.nassp.org/a/title-iv-21st-century-schools/.

[45] *Id.*

   b. Please describe your process for training AI-powered tools.
   c. What steps do you take to mitigate bias in training data and models?

6. What types of data do your products collect and from where does it collect this data? Please include all categories of information collected, including any personally identifiable information (PII) of students, as defined in FERPA[46].
   a. How, specifically, does your company use PII and aggregate information (data from which all PII has been removed)?
   b. What steps does your company take to de-identify PII before using it for non-educational purposes or sharing it with third parties?
   c. With whom does your company share PII about students? With whom does your company share aggregated data from which PII has been removed?
   d. How long does your company retain student data, including both PII and aggregate data from which PII has been removed?
   e. How are student data stored, and what steps is your company taking to reduce cybersecurity breaches of student data and to prioritize students' privacy according to relevant federal laws, including FERPA[47] and COPPA?[48]
7. How does your company disclose monitoring of student activity to students and their guardians? Does your company make recommendations to its consumers regarding student privacy? If so, please explain and provide any relevant documentation.
8. Can students and families opt out of this online monitoring while using school-issued devices and/or school-issued accounts? If so, please explain how.
   a. What percentage of students and families choose to opt out?
9. Please explain how your company is prioritizing student equity and access.
   a. Do you track whether your product disproportionately flags students in a protected class, such as students of color and LBGTQ+ students?
   b. Does your company track whether schools' use of the information provided by your product disproportionately affects students in a protected class, such as students of color and LBGTQ+ students?
   c. Please describe any steps your company has taken to detect and mitigate the disproportionate impact of your product once it has been released.
10. In how many instances have your products flagged student activity? Please provide a breakdown of the number and types of flags across all your products, including reasons the activity was flagged.
   ~~a.~~ Please provide a demographic breakdown, including by race/ethnicity and LGBQT+ status (if known), of students whose activity has been flagged within the last twelve months.
11. When your products are made available to schools, are they set to continue monitoring students outside of school hours by default?
   a. If so, what percentage of schools and/or students opt out of this default setting?
   b. If not, are schools able to set the product to monitor students outside of school hours? What percentage of schools use this setting?

[46] 20 U.S.C. § 1232g; 34 CFR Part 99.
[47] *Id.*
[48] 15 U.S.C. §§ 6501–6506.

   c. Please provide a breakdown by day of the week and time of day that student activity has been flagged within the last twelve months, including the percentage of flags that occurred between 8 a.m. and 4 p.m. on weekdays.
   d. Have your company policies on student monitoring activities, or any guidance you provide to schools using your products, changed in light of the recent Supreme Court ruling protecting student off-campus speech?[49]

12. Please describe any differences in how your products operate on school-issued devices compared to students' personal devices.

Sincerely,

Elizabeth Warren

Elizabeth Warren
United States Senator

Edward J. Markey

Edward J. Markey
United States Senator

Richard Blumenthal

Richard Blumenthal
United States Senator

[49] Mahonoy Area School District v. B.L., 594 U.S. __ (2021).