GoGuardian

October 26, 2021

The Honorable Elizabeth Warren
U.S. Senate
309 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Edward Markey
U.S. Senate
255 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Richard Blumenthal
U.S. Senate
706 Hart Senate Office Building
Washington, D.C. 20510

Dear Senators Warren, Markey and Blumenthal:

Thank you for the opportunity to share information about GoGuardian. The topics you raise are important, and we hope the information in this letter is helpful to better understand GoGuardian's products and practices.

GoGuardian was founded in 2014 to help schools facilitate safe digital learning experiences. GoGuardian products are purpose-built for the K-12 environment, empowering educators to provide students with access to the vast learning resources available online while helping protect them from harmful and inappropriate content. By 2014, schools and educators had begun widely embracing digital tools for their ability to help educators facilitate student learning and better tailor instruction to meet the needs of diverse learners. With this understanding came the broad deployment of internet-connected devices in schools and classrooms. These devices quickly brought the power and the danger of the internet directly into classrooms and students' hands. GoGuardian's first product, GoGuardian Admin ("Admin"), allows school administrators to help protect students from accessing inappropriate content while allowing students to learn, explore, and collaborate freely online. GoGuardian Beacon ("Beacon") was introduced in 2019, building on the functionality of Admin while adding features that help designated school staff identify students who may be at risk for suicide or self-harm and potential threats of violence.

Educators turn to GoGuardian to manage the enormous challenge of balancing access to educational resources on the internet while blocking harmful content. Content proliferates

online at an incredible rate — more than 547,200 new websites are created globally every day[1] and 500 hours of new video are posted to YouTube every minute.[2] Given this, it is impossible for educators to continually assess what content has legitimate educational value and what is inappropriate for the classroom, or to always watch for signs in online activity that a student might be struggling with their mental health or have concerns for their physical safety. GoGuardian's technology is designed for the K-12 environment and allows educators to focus their limited time and resources where it matters most: connecting with students and helping them develop the skills needed to be successful in life.

Unlike broad internet filters that use simple keyword monitoring and website blocklists, Admin employs machine learning[3] to update and adapt dynamically for the internet's constantly changing content while ensuring educational resources remain accessible. Beacon builds on Admin's machine learning technology for a solution carefully designed to support student mental health. Developed in partnership with national mental health experts such as the American Foundation for Suicide Prevention and the American Association of Suicidology, Beacon uses machine learning to identify students who may be at risk of suicide or possible harm to others through threats, violence, and bullying. Beacon is intended to be one part of a school's larger suicide, self-harm, and violence prevention program and can serve as a vital data point within a school's overall student support and safety program — programs that the Department of Education[4] underscores are critical to addressing the mental health needs of students and that have become increasingly vital as schools contend with the possibility of pandemic-related mental health effects for years to come.[5]

To be sure, GoGuardian recognizes the trust educators place in us — trust that our technologies help schools protect students' safety and trust that the company protects students' privacy. For this reason, we provide all customers with best practices for setting their monitoring policy; templates for notifying students, parents/guardians, and the community (Admin[6] and

---

[1] Huss, Nick. "How Many Websites Are There around the World? [2021]." Siteefy, October 8, 2021. https://siteefy.com/how-many-websites-are-there/.

[2] Lalani, Farah, and Cathy Li. "How to Help Slow the Spread of Harmful Content Online." World Economic Forum, January 13, 2020. https://www.weforum.org/agenda/2020/01/harmful-content-proliferated-online/.

[3] The term machine learning is used throughout the response to refer to the subset of artificial intelligence techniques that can generally be thought of as models that improve accuracy by learning from error.

[4] Goldberg, Suzanne B. "Letter to Educators: Students at Risk for Self-Harm or Suicide." United States Department of Education, Office of Civil Rights. October 13, 2021. https://www2.ed.gov/about/offices/list/ocr/correspondence/stakeholders/educator-202110-students-suicide-risk.pdf

[5] Prothero, Arianna. "The Pandemic Will Affect Students' Mental Health for Years to Come. How Schools Can Help." Education Week. Education Week, March 31, 2021. https://www.edweek.org/leadership/the-pandemic-will-affect-students-mental-health-for-years-to-come-how-schools-can-help/2021/03.

[6] Communicating with Parents/Guardians about GoGuardian Admin: https://help.goguardian.com/hc/en-us/articles/360025398811-Communicating-with-Parents-Guardians-about-GoGuardian-Admin

Beacon[7]); transparency features in our products (School Session Indicator[8]); recommended guidelines for who should have access to student data and who should be notified of Beacon alerts (Beacon: What to Consider Help Center article[9], Beacon User Roles and Permissions Help Center article[10] and Beacon Rollout Best Practices Help Center article[11]); instructional webinars[12]; and much more as detailed in the answers below. In addition, GoGuardian is a proud signatory of the Student Privacy Pledge[13] and certified as compliant with the Family Educational Rights and Privacy Act ("FERPA") by the Internet Keep Safe Coalition.[14]

At GoGuardian, we fully understand and embrace the fact that schools must maintain control of their students' data. We take great efforts to collaborate with customers to provide them the ability to access, modify, and delete this data consistent with FERPA, the Children's Online Privacy Protection Act ("COPPA"), and all other applicable laws. In addition, schools have control over how they deploy GoGuardian software — including controlling where and when GoGuardian is active and determining how GoGuardian's filtering and monitoring capabilities help increase compliance with schools' policies concerning the responsible use of technology. More information can be found in GoGuardian's Trust & Privacy Center.[15]

GoGuardian is committed to creating technology that helps educators support all students on their learning journeys. As a company, we believe that education is the highest point of leverage to improve society and we envision a future where all learners are ready and inspired to solve the world's greatest challenges. These beliefs drive our decisions — from how our products are designed to how we thoughtfully and responsibly approach protecting student data and privacy.

Below, please find our answers to each question. We have responded as completely and accurately as possible, and we look forward to continuing to work with you on these important issues:

---

[7] Communicating with Parents/Guardians about Beacon: https://help.goguardian.com/hc/en-us/articles/360025096772-Communicating-with-Parents-Guardians
[8] School Session Indicator: https://help.goguardian.com/hc/en-us/articles/4408802348180-School-Session-Indicator
[9] Beacon: What to Consider Help Center article: https://help.goguardian.com/hc/en-us/articles/4408541417620-What-To-Consider
[10] Beacon User Roles and Permissions Help Center article: https://help.goguardian.com/hc/en-us/articles/360000688063-Beacon-User-Roles-and-Permissions
[11] Beacon Rollout Best Practices Help Center article: https://help.goguardian.com/hc/en-us/articles/360016085951-Best-Practices-Beacon-Rollout
[12] Instructional Webinars: https://www.goguardian.com/blog/conversations-about-student-privacy-and-safety
[13] Student Privacy Pledge: https://studentprivacypledge.org/privacy-pledge-2-0/
[14] Internet Keep Safe Coalition: https://ikeepsafe.org/
[15] GoGuardian Trust & Privacy Center: https://www.goguardian.com/privacy-information

1. What student activity monitoring software has your company developed for use in school districts?

GoGuardian was founded in 2014 with the aim of helping schools balance their need to provide students with greater access to the internet and their responsibility to keep students safe on school devices and technology. The two GoGuardian products used by school and district customers to monitor students' online activity on school-managed devices, accounts, and networks are GoGuardian Admin ("Admin") and GoGuardian Beacon ("Beacon"). The Admin product filters harmful or explicit content based on policies established by the school and generates alerts when searches for such harmful or explicit content occur. Beacon was built in partnership with mental health experts and seeks to alert designated school professionals if a student's online activity indicates they may be at risk of suicide or possible harm to others through threats, violence, and bullying.

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.

Admin generates alerts based on activity on school-managed devices, accounts, or networks. Admin uses machine learning algorithms to scan online content on school-managed accounts,[16] devices, and networks. If the algorithm detects inappropriate or harmful content on a website, the tool prevents the student from accessing that content and generates an "Explicit Content Smart Alert" in the Admin dashboard available to school administrators. Similarly, if the algorithm detects that a students' online activity may suggest the student is considering suicide or self-harm, then the tool generates a "Self-Harm Smart Alert" in the Admin dashboard for school administrators. Within the dashboard, the alert itself provides the designated school administrator with the online activity that generated the alert. School administrators determine, consistent with their policies, whether and how to respond to alerts. Admin, including both the dashboard and algorithms, is not designed to make disciplinary recommendations and does not provide access to individuals or agencies outside of the school administration.

Schools and districts implement Beacon as one tool in their safety and suicide prevention programs. Beacon uses machine learning algorithms to scan online activity on school-managed accounts, devices, and networks. Developed in partnership with mental health experts, including the American Foundation for Suicide Prevention and American Association of Suicidology, Beacon is a multi-classifier machine learning model that indicates whether online activity is suggestive of suicidality and classifies that activity along a clinically recognized spectrum of severity: active planning, suicide ideation, self-harm, self-help, and research. If Beacon detects

[16] A school-managed account is an online account held by the school and provided to students for access to online resources and school technology (e.g. Jane.Doe@schooldistrict123.state.gov). Depending on school policies, students may be able to sign in to school-managed accounts on personal computers.

that online activity may be indicative of "active planning," the tool notifies via email and/or text message a predetermined list of staff designated by the school to handle sensitive information. Beacon dashboard and email alerts provide designated school officials with context around an event (screenshots, the phase of suicide and self-harm ideation, and highlighted text) to enable the school staff to determine the next steps to help a student in need of support. To protect the privacy of students, text notifications to designated school officials only prompt that official to access the Beacon dashboard and do not display information about the individual student whose activity generated the alert. For schools that choose the Beacon 24/7 service plan, a dedicated team of trained safety support specialists — who are operating as agents of the school and are based in the United States — provide an additional layer of support: they review active planning alerts and begin notifying the school staff via phone call on the school's designated escalation list.

3. How many school districts have purchased and/or are currently using your products?

Approximately 6,700 schools/districts[17] use Admin and 500 schools/districts use Beacon.

4. How much does your company charge school districts for use of your services?

GoGuardian [redacted]

a. Please provide a comparison of the free and premium services you provide to schools. Please include whether data privacy measures differ across services.

Admin and Beacon are enterprise products. As such, there are no free versions of the products that differ from paid versions. In addition, there are no individual teacher accounts for either Admin or Beacon. All Admin and Beacon services are contracted between the school or school district and GoGuardian with a consistent set of privacy practices across contracts.

5. How do you test for and correct bias in your products during the design and development process?

GoGuardian recognizes that inequities and bias in the educational system are barriers for too many children in the United States. Part of the company's mission is to expand access to the

[17] Because GoGuardian customers can be individual schools or entire school districts, our response uses the phrase schools/districts to refer to any school or district customer.

internet for *all* students while also keeping them safe from harmful and inappropriate content. As an organization, we firmly stand against racism and bias.

Admin and Beacon operate on the internet browser of school-managed accounts and primarily use the content of webpages and the name of the school-managed account to function. In order to protect student privacy, Admin and Beacon do not collect demographic or socio-economic information about students. Rather, we strive for privacy-by-design and have strong principles surrounding data minimization. Our goal is to collect only the data necessary to perform the functions of the product. Given this privacy-enhancing limitation in our data, GoGuardian cannot currently perform rigorous and precise analyses of algorithmic biases related to any student-level demographic or socio-economic data. However, GoGuardian is aware of the potential of bias by machine learning and takes appropriate steps to identify and correct bias to the extent we can while balancing our strong commitment to protecting student privacy.

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?

As stated above, in order to maximize student privacy, Admin and Beacon do not collect any student-level demographic data. This means that GoGuardian cannot link a student's online activity to individual student-level demographics.

b. Please describe your process for training AI-powered tools.

GoGuardian uses industry best practices in machine learning to develop and train its models. To develop an initial proof-of-concept for the model, data scientists extract a relevant sample of data from our de-identified databases and work with a team of product managers, customers, and expert partners to determine the correct outputs (classes) the algorithm should identify. The data scientists will then recruit a small internal team to label the sample data records with a class only for the purpose of developing the proof-of-concept. Using the labeled sample data, the data scientists will then utilize a wide variety of modeling techniques to examine the feasibility of predicting the class for each data record and present their findings regarding the accuracy of the techniques attempted.

To move from proof-of-concept to developing the model, GoGuardian data scientists extract additional relevant information from our de-identified databases. Without the data leaving our securely-designed infrastructure, contracted data labelers utilize a user interface that shows one to twelve records at the time and asks them to label each according to the classifications. Once the new data set is labeled, the data scientists retrain the algorithm and continuously evaluate predictive performance.

c. What steps do you take to mitigate bias in training data and models?

As mentioned above, GoGuardian understands the potential for bias in machine learning. Because the products are designed to collect minimal Personally Identifiable Information (PII), GoGuardian cannot currently perform rigorous and precise analyses of algorithmic biases related to any student-level demographic or socio-economic data. When training the Admin and Beacon models, GoGuardian aims to mitigate individual bias in data labeling by requiring at least two human-provided labels for each data record and additional reviews if the first two reviews are not aligned.

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.

Admin and Beacon operate under contracts with our school customers in accordance with the Family Educational Rights and Privacy Act ("FERPA") and state student privacy laws. This means that we only collect students' PII from school-managed devices and school-managed accounts and treat all such data as subject to FERPA and applicable state student privacy laws. Specifically, Admin and Beacon collect the following information from students through their **school-managed accounts**: Name, school email address, school Google or Microsoft profile ID, school-managed Google profile image URL (if applicable), organizational unit[18], and device identifiers (which are necessary to associate students with certain devices and settings). Depending on a school's currently selected products, features, integrations, and settings, we may collect additional information, including student browsing history, IP address, and relevant online content. In addition, GoGuardian Admin may allow for schools to collect the geographic location of managed devices for the purposes of device recovery but that feature must be purposefully activated by school personnel to find and recover a specific device.

a. How, specifically, does your company use PII and aggregate information (data from which all PII has been removed)?

Students' PII always remains under the control of our school customers. In accordance with our contractual obligations to our school customers and FERPA, GoGuardian processes Student PII for the purposes of directly providing software services and support to our school customers. We use de-identified student data (data that cannot reasonably be used, alone or in combination, to identify an individual student) for research and development of our products. Without qualification, GoGuardian never sells (or otherwise monetizes) student data.

[18] In this context, an organizational unit (OU) is a subset of a school/district's full set of school-managed accounts. For example, a school/district may put elementary and high school students in different OUs in order to set different filtering policies for each.

b. What steps does your company take to de-identify PII before using it for non-educational purposes or sharing it with third parties?

GoGuardian uses a combination of technical, administrative, and legal controls prior to sharing de-identified data. For administrative controls, for example, we screen third-party partners such as nonprofits for alignment with our mission to help students and for sophistication in their privacy practices. For legal controls, for example, our contracts require controls on the use of data, including that any use of shared data must be in accordance with applicable student privacy laws as well as prohibitions against selling of data and attempting to re-identify information. For technical controls, we use different de-identification techniques, such as removing identifiable information, aggregating and blurring data, and controlling access to certain data fields to protect the privacy and identity of individuals.

c. With whom does your company share PII about students? With whom does your company share aggregated data from which PII has been removed?

GoGuardian only shares PII with contracted third-party service providers as needed to deliver our products. At all times, student PII remains within the United States. GoGuardian shares de-identified data with its third-party service providers and with contracted non-profits or other educational entities for the purposes of product improvement and making sure the products we supply meet the needs of our school and district customers. For example, we have shared de-identified data with mental health experts in order to improve our Beacon product's ability to respond in the best way possible to self-harm-related alerts. At the macro level, we use only highly aggregated and anonymous information, such as number of users, in public-facing documents.

d. How long does your company retain student data, including both PII and aggregate data from which PII has been removed?

Under FERPA, GoGuardian maintains Student PII at the direction of the applicable school or school district. The specific timing for de-identifying and/or deleting personally identifiable information varies depending on the specific contractual terms with a school or school district. If a school, through the contract or otherwise, has not requested data deletion 365 days after their license(s) expire, we will de-identify and delete that school or school district's data.

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 and COPPA?

GoGuardian is a proud signatory of the Student Privacy Pledge,[19] a set of student data privacy commitments. GoGuardian is also certified as FERPA-compliant by the Internet Keep Safe Coalition,[20] a third-party privacy consultant firm that works with both schools and EdTech providers.

GoGuardian has implemented a robust security program with various technical, legal, physical, and administrative controls designed to protect students' personal information, in compliance with applicable federal and state privacy laws and overseen by an experienced security team. Specifically, GoGuardian has obtained attestation from a Qualified Security Assessor and Payment Application Qualified Security Assessor in good standing with the PCI Security Standards Council that our information security practices align with the NIST Cybersecurity Framework.

Network security includes leveraging an industry-leading database, including encrypted data in motion between product endpoints and at rest. Device security includes GoGuardian desktops and laptops utilizing two-factor and multi-factor authentication, full disk encryption, vulnerability management, centralized mobile device management, and virus control software. GoGuardian uses a third-party vendor that performs penetration tests on a regular basis, overseen by the GoGuardian security team.

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.

GoGuardian has developed a Privacy and Trust resource center (available at https://www.goguardian.com/privacy-information) that contains plain language descriptions of our data collection, use, and protection practices. This includes a link to a Parent Information Guide specifically designed to concisely provide parents/guardians with key information regarding our data practices. GoGuardian also provides resources to our school customers that can help them inform their students and parents/guardians about the technology being deployed on school-managed devices and accounts. Specifically, our Help Center includes templates for parent letters that our customers can use as a part of their communication plans (available in the GoGuardian Help Center[21]). The template parent letters encourage schools to send a technology acceptable use agreement (which schools create) to parents/guardians. We also

[19] Student Privacy Pledge: https://studentprivacypledge.org/privacy-pledge-2-0/
[20] Internet Keep Safe Coalition: https://ikeepsafe.org/
[21] Communicating with Parents/Guardians about GoGuardian Admin: https://help.goguardian.com/hc/en-us/articles/360025398811-Communicating-with-Parents-Guardians-about-GoGuardian-Admin

provide schools with a COPPA Notice & Disclosure Form (downloadable document[22]), and other product documents they can give to parents/guardians and students.

Prioritizing transparency, GoGuardian also proactively built two transparency features within our products. First, whenever GoGuardian is deployed to a school-managed device, the GoGuardian shield icon appears in the device's toolbar. Second, GoGuardian has built a School Session Indicator[23] that persistently appears on the browser window of a school-managed device, account, or network. The School Session Indicator is designed to remind users that the device, account, or network they are using is managed by the school.

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?

Yes. School administration has substantial flexibility regarding how monitoring features are deployed including the ability to develop opt-outs and alternatives for parents/guardians and families. Parents/guardians can work with their school administration to opt their students out of Admin and Beacon. At the technical level, the school technology administrator would assign students whose parents/guardians have opted them out to a separate organizational unit (OU) in the school's digital ecosystem that does not contain GoGuardian software. For students in this separate OU, GoGuardian will not be deployed to their school-managed account. Because this separate OU is not connected to GoGuardian products, we cannot accurately determine what percentage of students a school/district places in a separate OU outside of GoGuardian's purview.

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.

As stated above, to protect the privacy of students, Admin and Beacon do not collect student-level demographic data. Built with privacy-by-design principles, GoGuardian products are designed to only collect data necessary to perform the functions of the product. Admin and Beacon operate at the browser level on school-managed accounts and primarily use the content

---

[22] COPPA Notice & Disclosure form: https://help.goguardian.com/hc/en-us/article_attachments/4407990649492/GoGuardian_%252B_Pear_Deck_Children_s_Online_Privacy_Protection_Rule__COPPA__Disclosure_-_9-30-2021.pdf

[23] School Session Indicator: https://help.goguardian.com/hc/en-us/articles/4408802348180-School-Session-Indicator

of webpages and the name of the school-managed account to function. Because the products are designed to collect minimal PII, GoGuardian cannot currently perform rigorous and precise analyses of algorithmic biases related to any student-level demographic or socio-economic data.

GoGuardian fully believes that our schools and classrooms should be spaces where students are treated equitably and have the opportunity to learn and thrive. As a company, we are committed to continual due diligence and examination of our product development processes. Internally, in partnership with our Diversity, Equity, and Inclusion teams, we continually work to strengthen our product development process to ensure that we are creating products that are safe, accessible, and equitable. We leverage established best practices for product development and engage external experts in accessible and equitable design practices from academic and non-profit institutions as well as private firms to strengthen our internal resources.

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.

In 2020, approximately 9.5 million school-managed accounts were on Admin and 1.5 million school-managed accounts were on Beacon. Over the course of 2020, Admin generated 44 million alerts or approximately 4.6 alerts per student over 2020. Of these alerts, approximately 90% were for explicit or inappropriate content and approximately 10% were for self-harm. Beacon, over the course of 2020, generated approximately 10,000 alerts for active planning of suicide.

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.

As discussed above, in order to protect the privacy of students, Admin and Beacon do not collect any student-level demographic data. Admin and Beacon operate at the browser level on school-managed accounts and primarily use the content of webpages and the name of the school-managed account to function. Built with privacy-by-design in mind, GoGuardian products are designed to only collect data necessary to perform the functions of the product. Given this privacy-enhancing limitation in our data, GoGuardian cannot perform rigorous and precise analyses of algorithmic biases related to any student-level demographic or socio-economic data.

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?

Admin has an "Out of School Mode" that can be used to disable monitoring outside of school hours and on weekends. Out of School Mode is configured and implemented by school administrators who set the parameters regarding when it is active. When Out of School Mode is enabled, Admin will continue to restrict access to harmful or explicit content on school-managed devices, accounts, and networks. It will not, however, collect any browsing activity or generate individual alerts based on student activity. When we work with our school customers to configure their specific instance of GoGuardian, our implementation team provides an overview of all the scheduling features, including how to create and activate the Out of School Mode. Approximately 33% of our customers use this Out of School Mode to disable monitoring of school-managed accounts after hours or when out of range of the school's IP addresses.

By design, Beacon does not have an Out of School Mode. The product is designed to help school counselors, administrators, and student support professionals identify students who may be struggling with mental health issues. If a school/district chooses to deploy Beacon, that tool will be active on school-managed accounts, devices, and networks for the duration of the deployment.

In addition, when students are on a personal device, Admin and Beacon are only enabled when students sign into their school-managed account on that device. And, as described in response to Question 7, GoGuardian has built and deployed a School Session Indicator that persistently appears on the browser window of a school-managed device, account, or network when Admin or Beacon are enabled. The School Session Indicator is designed to remind students and anyone using the device, that the device, account, or network they are using is managed by the school. 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.

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.

Most alerts occur on weekdays, with approximately 84% of alerts occurring Monday through Friday. The lowest volume of alerts is generally around 8 am with approximately 1% of alerts occurring that hour. The peak alert volume is around 5-6 pm with approximately 8% of alerts occurring in each of those hours.

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?

GoGuardian is aware of *Mahanoy Area School Dist. v. B. L.*, 594 U.S. (2021) and the Supreme Court's ruling protecting the speech of students when they are off-campus and on personal accounts. As described throughout this response, GoGuardian operates only on school-managed accounts and devices, not on individuals' personal accounts. More specifically as it relates to *Mahanoy*, GoGuardian would not enable a school to monitor a student's personal cell phone usage off campus.

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

Admin and Beacon operate only on school-managed accounts, school-managed devices, and school-managed networks. As such, they are designed to provide a consistent experience for students when they are logged into their school-managed accounts. When students log into their school-managed account, Admin and Beacon begin to operate on the browser. If a student logs into their school-managed account on their personal computer, Admin and Beacon only monitor and filter the internet content associated with the student's school-managed account. When a student logs off of their school-managed account on their personal computer, Admin and Beacon will no longer be active on that device. In addition, Admin and Beacon do not operate on personal cell-phones.

* * *

Thank you for this opportunity to explain more about GoGuardian and our products. We fundamentally believe that digital learning can meaningfully advance educational outcomes, and this can only be achieved through a thoughtful balance of empowering students to explore the multitudes of vibrant learning opportunities on the internet while also protecting them from harm. We remain committed to privacy and equity in service of our mission to support all students on their learning journey and would be happy to discuss our products and practices further.

Sincerely,

Advait Shinde
Chief Executive Officer and Co-Founder