October 15, 2021

The Honorable Elizabeth Warren
The Honorable Edward J. Markey
The Honorable Richard Blumenthal
U.S. Senate
Washington, DC 20510

Dear Senators:

Securly is committed to protecting students' safety and welcomes this opportunity to provide additional information about our products and how they enable and augment schools' efforts to protect students.

We fully support the efforts of Congress to help protect children from destructive online content while empowering them to use the Internet as a robust part of their education. Congress demonstrated impressive foresight when it passed the Children's Internet Protection Act of 2000 (CIPA), which required schools to develop and enforce Internet safety policies to protect against the use of school computers for access to "visual depictions that are—(I) obscene; (II) child pornography; or (III) harmful to minors;" 47 U.S.C. § 254(h)(5)(B)(i), "during any use of such computers by minors." 47 U.S.C. § 254(h)(5)(B)(ii). Congress' direction for always-on monitoring of school computers for harmful materials helps to protect students. 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.

Schools face challenges beyond the traditional web filtering imagined by CIPA. Schools increasingly rely on online tools as part of educational programs. School-issued devices, email accounts, and document systems are an important part of how students engage in guided or self-directed learning as well as with one another. While these tools only offer part of the student safety picture, they also present challenges for schools from a supervision standpoint. The volume, nature, and pace of students' online activities hinder traditional efforts to look for warning signs, particularly when teachers do not have the ability to observe students learning in virtual settings. The fact that today's students live in an era of increased social anxiety and depression for youth, extended by the upheaval of the COVID-19 pandemic, only magnifies such school supervision challenges.[1] School officials and counselors recognize that some of their students need help, but face resource constraints and have limited visibility into student activities on school-issued devices, email accounts, and document systems.

[1] *See, e.g.*, American Psychological Association, "Student Mental Health During and After COVID-19: How Can Schools Identify Youth Who Need Support?" September 22, 2020, https://www.apa.org/topics/covid-19/student-mental-health.

These concerns are the singular focus of Securly's Auditor and 24 offerings, which we offer not as CIPA compliance solutions but rather as tools that help schools monitor for indicators that could signal these behaviors. Auditor and 24 are not replacements for school-driven student safety programs. Instead, they supplement school programs and help schools catch warning signs before students suffer, uncovering student safety risks and concerns that might otherwise remain hidden from view.

We structure our flagging and alerting structures so that school administrators and officials are the focal point for alerting. Indeed, Securly's platform is both customizable and scalable by and for school officials. We offer our products and services in both public and private educational settings and work with schools to formulate protections that are consistent with the school's values—whether they are socially conservative, religious schools or exemplars of progressive education. Each school decides which of our products or services to use, how to configure them, and how broadly to deploy them as a supplement to existing school safety programs.

Regardless of the particulars, our Auditor and 24 offerings focus on assisting schools with student protection and not policing student conduct writ large. Our offerings flag warning signs of cyber bullying, self-harm, and violence for schools, and with respect to 24, our in-house experts review and assess alerts for potential escalation with those warning signs in mind. The vast majority of the alerts relate to suicide, self-harm, or depression – areas where we are sure you share our passion to protect children. Our offerings are not designed to flag and escalate other types of suspicious student activity, and we partner closely with our schools to empower them to use our offerings as they deem appropriate.

Along those lines, we have carefully considered this country's broad and diverse school-age population in building our products and services. The Securly leadership and its nearly 200 employees are deeply committed to diversity within the Securly family and in the academic communities that Securly supports. Machine learning is without question a nascent technology. While we work continuously to learn and improve our products and services, we recognize that there are inherent nuances in assessing student activity for indicators of risk, which is why schools are a focal point of our alerting structure. We firmly believe that Auditor and 24 can serve as a key part of any school's student safety toolbox.

The information on the following pages is intended to respond to the Senators' specific inquiries. A few of the inquiries implicate sensitive and confidential business information. For these inquiries, we can provide responses verbally and on a confidential basis.

We look forward to continuing our dialogue with your offices.

Respectfully submitted,

Bharath Madhusudan
CEO and Co-Founder
Securly Inc.

securly

Responses to Specific Inquiries

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

Securly provides districts with two technology monitoring solutions that help deliver safer digital experiences for students.

- Securly's Auditor solution uses our advanced natural language processing technology to monitor for cyberbullying, self-harm, and violence across multiple channels, including emails and documents. Auditor's notification tools then direct alerts, which are based on a risk score, to the appropriate contacts within a school district who can choose whether and how to act on the alert.

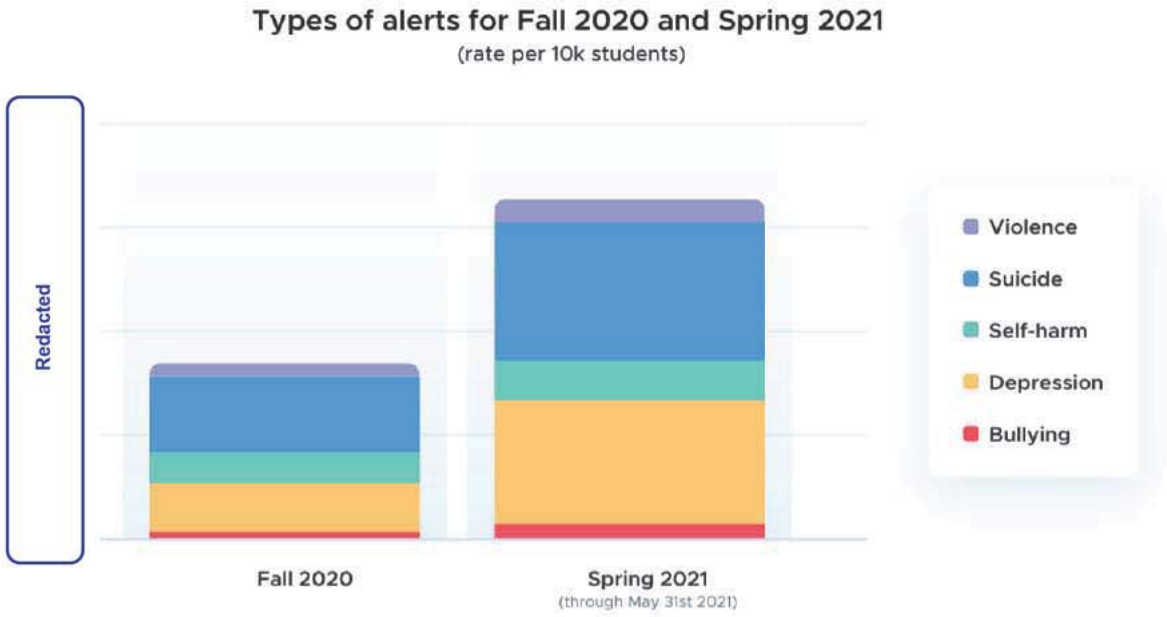
- Securly's 24 solution provides schools with access to a team of trained specialists who analyze the alerts and notifications around the clock, correlating them across time and providing schools with visibility into their students' well-being. Any alerts requiring immediate action are escalated to specialists designated by the schools.

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.

Auditor uses a multi-pronged approach to identify students at risk of harming themselves or others. We combine natural language processing and sentiment analysis to flag content related to cyberbullying, self-harm, and violence based on a correlated and synthesized risk score. Flagged activities are sent via email to designated school contacts trained to appropriately handle these alerts in accordance with district guidelines.

If a district uses Securly's 24 services, alerts are evaluated by our trained specialists. Depending on the urgency of the alert, our trained specialists reach out to the district's designated contact via SMS, call, or email. In select cases, districts prefer that we contact public safety agencies directly in lieu of a district contact. In these instances, we inform public safety agencies that we have a reason to believe a student may need help, and we request that they perform a welfare check.

The focus of our products is to identify students who need assistance, and roughly 80% our alerts are related to suicide, self-harm, and depression (as shown in the graph below).



Below are two examples of individual student activity related to self-harm that resulted in a phone call to designated school district contacts:

Student #1:

- Searched for
  - Visited
- Searched for
- Searched for
- Searched for
- Searched for
  - Visited
- Searched for
  - Visited
- Searched for

Redacted

Student #2:

- Searched for
- Searched for

Redacted

- Visited
- Visited
- Visited
- Searched for
  - Visited

Redacted

Alerts that fall outside the scope of self-harm are held to similarly well-vetted standards, and only items that have the potential to harm others are flagged for further review. As an example, 'how do I build a bomb' would be escalated to schools' designated contacts, but 'how do I buy weed' would not. Below is an example of one student's activity related to violence that resulted in a phone call to the designated school district contact:

Student #3

- Searched for
- Searched for
  - Visited
- Searched for
  - Visited
- Searched for
  - Visited
- Searched for
- Searched for
- Searched for

Redacted

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

We are unable to respond to this question in an open letter due to its commercially sensitive nature, but we can provide the information confidentially.

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.**

We are unable to respond to this question in an open letter due to its commercially sensitive nature, but we can provide the information confidentially.

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?

We do not collect any student information related to race, ethnicity, or sexual orientation.

Instead, to minimize the potential for bias, we identify negative keywords based on internal analysis as well as school and community feedback, and we take steps to account for those keywords within our alerting framework.

In addition, we take steps to solicit and receive feedback from school districts and students alike to enhance our technology offerings. To take just one example, earlier this year, our Director of Engineering and our Director of Student Safety personally met with a student to listen to concerns around how sites are categorized. Some, but not all, of the student's concerns did have merit. As a result of this meeting our company took immediate action to correct the issues by adjusting certain categorizations.

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

We continually train our engines based on the feedback from our school partners and students. When items have been flagged inappropriately, we aim to address these concerns as soon as possible—meeting with everyone from district leaders to students to discuss areas of potential bias.

It is our mission to ensure our technology is built to protect students. As an example of the work we have put into training our tools, our software is designed not to flag searches wherein a student may be exploring their sexual orientation. It will flag, however, any communications in which a student may use derogatory terms related to another student's sexual orientation within the context of cyberbullying.

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

As previously mentioned, we introduce negative key words into our training set and process feedback from school staff and students. We are vigilant for issues in our data and models that

require adjustment, and our Auditor and 24 products remain focused on warning signs for cyberbullying, self-harm, and violence.

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 FERPA46.

The types of data we collect in connection with the Auditor and 24 products are described at a high level in our public COPPA Privacy Policy, available here: https://www.securly.com/childrensPrivacy. This includes information collected regarding a student's device as well as information collected automatically from their activity while using school devices or systems.

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

We use the data we collect to provide services to schools. Our company uses student names only in order to provide our student safety services. When a flagged activity merits that we communicate to the school's designated contact, we will mention a student's first and last name in that private communication to the designated school contact.

We also may use aggregate or de-identified information to monitor and analyze our services, for technical administration, to understand student usage or other research and analytical purposes, and to improve our services.

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

This is not applicable. We do not de-identify PII for purposes unrelated to the services we provide to schools. We do not share PII with third parties other than those who are helping us provide these services (e.g., PII is encrypted on our servers hosted by AWS).

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

This is not applicable. We do not share PII or de-identified or aggregated student information with third parties other than service providers (i.e., vendors who support us in our provision of the services to schools).

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

Securly collects and retains information at the direction of the schools to whom we provide services. We rely on schools to inform us when retention of such data is no longer necessary to fulfill Securly's obligations to provide the services, at which point Securly purges the identified data in question.

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?

We take the security of data very seriously. Information is encrypted on our servers hosted by AWS. We are SOC 2 Type 2 certified; our information security practices, policies, procedures, and operations have been audited by a leading national accounting and advisory firm and found to meet SOC 2 Type 2 standards. In particular, we have a comprehensive information security program including written policies and procedures that we review, adjust, and update periodically as appropriate based on technological and service-related changes as well as the cybersecurity threat landscape.

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.

In the context of the Auditor and 24 products, Securly does not have a direct relationship with parents or students; instead, Securly acts as a service provider to school districts. Student use of district-owned technology, however, is typically governed by district-level acceptable use policies. Beyond that, Securly provides a parent kit to all districts. The kits include details regarding the functioning and purpose of Securly's products and options for parental visibility through Securly's products. We strongly encourage these districts to send these kits to parents at the beginning of each school year.

Securly also posts privacy policies, terms of use, and related materials to its website that outline how Securly processes data among other things. Securly provides school districts with access to or copies of these materials, and school districts agree to or acknowledge these materials as part of Securly's typical engagement process. Rather than recommendations, Securly provides school districts with options to configure and customize the products in various ways, based on their facilities' specific needs and safety programs as well as concerns relating to privacy consistent with community-specific factors.

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.

Districts may adopt their own opt-out policies at their own discretion. Examples of such policies can be found on the Internet.

a. What percentage of students and families choose to opt out?

We do not track this data. It is within the school's discretion to provide an opt-out to their acceptable use policy.

9. Please explain how your company is prioritizing student equity and access.

The Securly leadership and its nearly 200 employees are deeply committed to diversity within the academic communities that Securly supports. We have taken steps to consider this country's broad and diverse school-age population as part of our products and services. We believe in protecting all students from the harms of cyber bullying, self-harm, and violence, particularly in an era of increased social anxiety and depression for youth.

a. Do you track whether your product disproportionately flags students in a protected class, such as students of color and LBGTQ+ students?

We do not collect data on a 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.

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?

We do not track that information. Our intent is to provide schools with the information necessary to protect students, and our Auditor and 24 products focus on warning signs of cyber-bullying, self-harm, and violence.

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 mentioned previously, we opt for proactive efforts to mitigate bias. We are also open to and regularly engage in conversations with school districts and students on these issues and remain vigilant for additional ways to enhance these efforts. Although we do not collect any student data related to race, ethnicity, or sexual orientation, in the event that students, districts, or others in our

community report that bias may exist in our algorithms, our team investigates such reports and takes appropriate action.

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.

We have partnered with schools to provide immediate safety assistance in connection with 1,393 student alerts, in addition to more commonplace flagged warning signs. As outlined in response to Question 2 above, roughly 80% of our alerts are related to suicide, self-harm, and depression. More generally, we are unable to respond to this question in an open letter due to its commercially sensitive nature, but we can provide further information confidentially.

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 mentioned, we do not collect data on a 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.

11. When your products are made available to schools, are they set to continue monitoring students outside of school hours by default?

Due to the nature of the Auditor and 24 products, we monitor students both during and outside of school hours. By purchasing Auditor and 24, schools are able to deploy our solutions to flag, assess, and alert for warning signs outside of school hours, but schools deploy these tools only on school devices, school email systems, and school document systems.

a. If so, what percentage of schools and/or students opt out of this default setting?

Schools can customize various details relating to the alerts they receive, including the extent to which and how they receive alerts after hours, but we do not systematically track school decision-making on these points. Student opt-out options vary depending on the district's acceptable use policy.

b. If not, are schools able to set the product to monitor students outside of school hours? What percentage of schools use this setting?

As mentioned above, Auditor and 24 are deployed only school devices, school email systems, and school document systems.

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.

Please see below for a high-level breakdown.

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?

Securly is certainly sensitive to the need to protect student off-campus speech, and we have not had any need to make changes in response to the recent Supreme Court ruling. Securly's offerings are focused on warning signs of bullying, self-harm, and violence, and our alerts are designed to flag those warning signs and not other types of student conduct or speech that were more squarely the focus of the ruling. As the Court in *Mahanoy Area School District v. B. L., 594 U.S. ___ (2021*), made clear, "circumstances that may implicate a school's regulatory interests include serious or severe bullying or harassment targeting particular individuals" and "threats aimed at teachers or other students." These are the areas that we monitor in order to protect students.

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

Our products monitor channels that are tied to school-issued devices and school-owned accounts, such as email accounts or document systems. Monitoring of school-owned accounts used on personal devices is limited to activities associated with those accounts, whereas monitoring on school devices will include channels such as Internet usage.