

United States Senate
WASHINGTON, DC 20510

April 8, 2020

Eric S. Yuan
Founder and Chief Executive Officer
Zoom Video Communications, Inc.
55 Almaden Boulevard, 6th Floor
San Jose, CA 95113

Dear Mr. Yuan:

We write to request more information on how Zoom Video Communications, Inc. (Zoom) is protecting the safety and privacy of students who use your service. As schools across the country have rapidly shifted to remote education due to the coronavirus disease 2019 pandemic, Zoom has seen a rapid increase in users, including teachers and children at more than 90,000 schools who are using the platform to continue instruction.¹ The platform is filling a critical need during the pandemic. But precisely because Zoom's technology has become such an invaluable – and in many cases, required - tool for learning and keeping students connected to their school communities during this crisis, we are concerned by recent reports that the platform may not be adequately safeguarding users' data and privacy.

On March 30, 2020, the Federal Bureau of Investigation (FBI)'s Boston division warned that two high schools in Massachusetts have experienced hijackings of Zoom classes.² In one incident, an unidentified individual entered the classroom and “yelled a profanity and then shouted the teacher's home address in the middle of instruction,” while in the other, an unidentified individual “was visible on the video camera and displayed swastika tattoos.”³ These incidents follow other reports of “Zoom-bombing,” in which intruders share pornographic images or racist and anti-Semitic slurs during Zoom meetings.⁴ While your website has shared some information with users about steps they can take to restrict meetings to authorized participants and prevent disruption,⁵ Zoom largely puts the onus on the user to manage the security of their classroom, adding an extra burden to teachers who are rapidly trying to shift

¹ Zoom Blog, “A Message to Our Users,” Eric S. Yuan, April 1, 2020, <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/>.

² FBI Boston, “FBI Warns of Teleconference and Online Classroom Hijacking During COVID-19 Pandemic,” March 30, 2020, <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic>.

³ *Id.*

⁴ USA Today, “Zoom issues: People hijacking streams, possible security flaws,” Mike Snider, April 1, 2020, <https://www.usatoday.com/story/tech/2020/04/01/zoom-demand-zooms-but-problems-coronavirus-drives-stay-home-video-chats-zoom-has-issues-beyond-deman/5102150002/>.

⁵ Zoom Blog, “Best Practices for Securing Your Virtual Classroom,” Ryan Gallagher, March 27, 2020, https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/?_ga=2.254100353.826396921.1585753460-2095267572.1584193490.

instruction to an entirely new format and to parents who are juggling a multitude of new challenges at home. We urge you to take all possible actions to prevent these disturbing intrusions, including by publicly releasing an independent, comprehensive review of your cybersecurity and privacy practices, including any data sharing arrangements, modifying default settings, permanently banning users who engage in this harassment, and publicly reporting data on the frequency and nature of these incidents.

These incidents add to Zoom’s track record of reported security vulnerabilities. In the past two weeks alone, media reports have revealed that Zoom has shared users’ data with Facebook without their knowledge,⁶ shared personal information with users who have email addresses using the same email domain,⁷ made misleading claims about whether your services use “end-to-end encryption,”⁸ and exposed Mac users’ cameras and microphones to potential access from hackers.⁹ These vulnerabilities led the New York Attorney General’s office to request information about Zoom’s data privacy and security practices¹⁰ and the New York City Department of Education to instruct schools to move away from using Zoom for remote instruction.¹¹ We appreciate your announced intention to address each of these issues,¹² but it is alarming that Zoom allowed these security breaches to affect millions of users and did not identify or resolve them until they became public.

The security and privacy of user data is of particular concern when the user is a child. The *Family Education Rights and Privacy Act* (FERPA) protects information about a student’s educational record from being disclosed to third parties without parental consent.¹³ The *Zoom for K-12 Schools and Districts Privacy Policy*, which applies specifically to Zoom Education users, notes that Zoom collects a significant amount of information about students, including the student’s “logins, clicks, messages, contacts, content viewed and shared, calls, use of video and screen sharing, meetings, cloud recording, and other feature usage information” and other data that users, including students, “upload, provide, or create while using the Service.”¹⁴ While you specify that schools are the owners of this information, as required by FERPA, the fact that Zoom stores this student data makes it vulnerable to data breaches and hacking that could expose

⁶ Vice, “Zoom iOS App Sends Data to Facebook Even If You Don’t Have a Facebook Account,” Joseph Cox, March 26, 2020, https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.

⁷ Vice, “Zoom is Leaking Peoples’ Email Addresses and Photos to Strangers,” Joseph Cox, April 1, 2020, https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos.

⁸ The Intercept, “Zoom Meetings Aren’t End-to-End Encrypted, Despite Misleading Marketing,” Micah Lee and Yael Grauer, March 31, 2020, <https://theintercept.com/2020/03/31/zoom-meeting-encryption/>.

⁹ TechCrunch, “Ex-NSA hacker drops new zero-day doom for Zoom,” Zach Whittaker, April 1, 2020, <https://techcrunch.com/2020/04/01/zoom-doom/>.

¹⁰ New York Times, “New York Attorney General Looks Into Zoom’s Privacy Practices,” Danny Hakim and Natasha Singer, March 30, 2020, <https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html>.

¹¹ CNN, “New York City schools won’t be using Zoom anymore because of security concerns,” Nicole Chavez and Sarah Jorgensen, April 4, 2020, <https://www.cnn.com/2020/04/04/us/nyc-schools-zoom-online-security/index.html>.

¹² Zoom Blog, “A Message to Our Users,” Eric S. Yuan, April 1, 2020, <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/>.

¹³ U.S. Department of Education, “Family Educational Rights and Privacy Act (FERPA),” March 1, 2018, <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.

¹⁴ “Zoom for K-12 Schools And Districts Privacy Policy,” March 18, 2020, https://zoom.us/docs/en-us/childrens-privacy.html?zcid=1231&_ga=2.186928929.826396921.1585753460-2095267572.1584193490.

private information about the children who use Zoom. Reporting on your security deficiencies is of heightened concern given that the *Children’s Online Privacy Protection Act* (COPPA) requires companies that have knowledge that they’re collecting children’s information to “establish and maintain reasonable procedures to protect the confidentiality, security, and integrity.”¹⁵

Moreover, the K-12 privacy policy applies only to users on the Zoom Education service. Users of the free service, including teachers, are subject to your general Privacy Policy, which was only recently updated to preclude sharing data with third parties, such as advertisers.¹⁶ This policy notes that “Zoom does not knowingly allow children under the age of 16 to sign up for their own accounts,”¹⁷ but Zoom also recently lifted its time limit on free Basic accounts for schools affected by coronavirus,¹⁸ which may encourage schools to use the free service with their students. While we appreciate Zoom’s efforts to ensure that all schools and students have access to this tool, this change makes it even more crucial to enhance the protections of the Zoom Education service and ensure that they apply to all users.

To better understand how Zoom is adapting to the recent increase in volume among student users and safeguarding private student data, we request answers to the following questions no later than April 22, 2020:

1. Has Zoom ever experienced a breach of user data? If so, please describe the breach and whether any student data was exposed.
2. As Zoom’s user volume has rapidly increased since the coronavirus public health emergency began, has Zoom made any changes to its process for storing user data? If so, please describe the changes made and how they may affect the security of data generated by K-12 students.
3. Prior to the March 29, 2020 update to Zoom’s general Privacy Policy,¹⁹ has Zoom ever shared user data with a third party, for advertising or any other purpose?
 - a. If so, how was the data screened to ensure that it did not include any data generated by children under the age of 18?
4. Is Zoom extending privacy protections offered under the Zoom Education service to schools that have taken advantage of the recent offer to lift the time limit on free accounts?
 - a. If so, please describe which privacy protections apply.

¹⁵ 16 CFR § 312.8

¹⁶ Consumer Reports, “Zoom Tightens Privacy Policy, Says No User Videos Are Analyzed for Ads,” Allen St. John, March 30, 2020, <https://www.consumerreports.org/privacy/zoom-tightens-privacy-policy-says-no-user-videos-analyzed-for-ads/>.

¹⁷ Zoom Blog, “Zoom’s Privacy Policy,” March 29, 2020, <https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/>.

¹⁸ Zoom, “K-12 School Time Removal Request FAQ,” https://support.zoom.us/hc/en-us/articles/360041264451?_ga=2.70525456.168760737.1586291405-2095267572.1584193490

¹⁹ Zoom Blog, “Zoom’s Privacy Policy,” March 29, 2020, <https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/>.

- b. If not, please describe how this information is communicated to school users.
5. How many incident reports has Zoom received of intruders interrupting classroom instruction while children under age 18 were present? Please provide the number of incidents that involved:
 - a. Incidents of harassment or discrimination based on race, national origin, religion, disability, or sex;
 - b. Incidents that included a threat of violence;
 - c. Incidents that resulted in a permanent ban of the user; and
 - d. Incidents that resulted in a report to law enforcement.
6. In your message to Zoom’s users on April 1, 2020, you committed to “conducting a comprehensive review with third-party experts and representative users to understand and ensure the security of all of our new consumer use cases.”²⁰ How will this review address concerns specific to children and students? Will you make the findings of this review public?
7. Please describe the steps that Zoom has taken to ensure that it is in compliance with COPPA. If Zoom maintains that it is not subject to COPPA because its terms of service prohibit users under the age of 16 from creating their own accounts, how do you reconcile that assertion with widespread reporting that schools serving young children, including children 12 and under who are covered by COPPA, are regularly relying on Zoom for everyday lessons?

Thank you for your consideration of this important matter.

Sincerely,

Elizabeth Warren
United States Senator

Edward J. Markey
United States Senator

²⁰ Zoom Blog, “A Message to Our Users,” Eric S. Yuan, April 1, 2020, <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/>.