RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS

United States Senate
WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, SUITE 304
BRIDGEPORT, CT 06604
(203) 330-0598
FAX: (203) 330-0608

http://blumenthal.senate.gov

March 31, 2020

Eric S. Yuan
CEO and Chairman
Zoom Video Communications, Inc.
55 Almaden Boulevard, 6th Floor
San Jose, CA 95113

Dear Mr. Yuan,

I write with concern and to seek information regarding how Zoom handles the personal data of its users and protects against security threats and abuse against its services. The millions of Americans now unexpectedly attending school, celebrating birthdays, seeking medical help, and sharing evening drinks with friends over Zoom during the Coronavirus pandemic should not have to add privacy and cybersecurity fears to their ever-growing list of worries.

Zoom is increasingly being used by schools and healthcare providers that have shut down or limited their operations to stop the spread of Coronavirus, raising questions about how its services comply with federal and state privacy laws protecting students, patients, and consumers. While Zoom has recently taken commendable steps to clarify how it handles this information, its privacy policy still grants it broad discretion to use personal data for other purposes than providing video conferences. For example, Zoom states that it "does use certain standard advertising tools on our marketing sites which, provided you have allowed it in your cookie preferences, sends personal data to the tool providers, such as Google." Parents, patients, and families should not have to worry that their children's information, their health condition, or their private discussions are being used for advertising and other unintended purposes.

Zoom has a troubling history of software design practices and security lapses that have posed significant risks to the privacy and safety of its users. Until last week, Zoom's iOS apps routinely sent personal data about its users to Facebook, whether or not they had a Facebook account, in order to track their behavior and target advertising. Zoom has also previously failed to respond in a timely and diligent manner to security vulnerabilities in its Mac client that allowed malicious attackers to silently eavesdrop on Zoom users, crash their computers, and

install unwanted programs. When Zoom did issue an initial fix, that patch did not fully resolve the vulnerability, requiring Apple to step in to protect its users.

Moreover, Zoom has not fully addressed pressing questions about how it protects users from intrusions and abuse. Colleges, children's groups, and others have reported alarming campaigns of harassment from uninvited intruders, called "Zoombombing," hijacking and disrupting meetings, including anti-Semitic attacks against a Massachusetts Jewish student organization. Additionally, despite claims in security white papers and advertisements that Zoom offers end-to-end encryption for its meetings, technical analysis from The Intercept found that it does not protect the privacy of communications using this form of encryption. Zoom users deserve clear and correct answers about how it protects the safety of its users and meetings.

Given the sensitivity of its services and the role of Zoom in our lives during the Coronavirus pandemic, I respectfully request a written response to the following questions by April 14, 2020:

1. What personal data and session information does Zoom collect and retain from Zoom users and video conferences? What does Zoom share with third parties, such as the marketing partners described in its privacy policy? Please provide the list of the marketing partners that are provided personal data and specific types of information.

2. Has Zoom made the privacy rights guaranteed under the California Consumer Privacy Act (CCPA) and the E.U.'s General Data Protection Regulation (GDPR) available to all American users?

3. What parental consent requirements, limitations on data collection, data access features, and other safeguards are provided under the Zoom for Education service? What steps has Zoom taken to ensure that schools use its Zoom for Education service, rather than the consumer version? How can parents and guardians exercise privacy rights for their children with Zoom for Education?

4. Does Zoom provide end-to-end encryption, as the term is commonly understood by cybersecurity experts, for video conferences? Please describe when end-to-end encryption is available for users and how this personal data is encrypted.

5. What measures has Zoom put into place to detect and prevent Zoombombing – intrusions and abuse targeting Zoom meetings? What are the policies governing such abusive behavior, what detection mechanisms are in place, how can users report abusive intrusions, and how quickly does Zoom respond to such incidents?

6. What contact information, bug bounties, and other procedures does Zoom maintain to receive reports and information about security vulnerabilities?

Thank you for your attention to these important issues. I look forward to your response.

Sincerely,

Richard Blumenthal
United States Senate