MICHAEL F. BENNET
COLORADO

COMMITTEES:
AGRICULTURE, NUTRITION, AND FORESTRY
FINANCE
INTELLIGENCE

United States Senate
WASHINGTON, DC 20510-0609

WASHINGTON, DC:
261 Russell Senate Office Building
Washington, DC 20510
(202) 224-5852

COLORADO:
Cesar E. Chavez Building
1244 Speer Blvd, Suite
Denver, CO 80204
(303) 455-7600

http://www.bennet.senate.gov

April 6, 2020

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

Dear Mr. Yuan:

The outbreak of the novel Coronavirus Disease 2019 has required an unprecedented reliance on video conferencing platforms like Zoom. In the last three months, the number of daily of Zoom users has reportedly grown twenty-fold as Americans and people across the globe use the platform to work, learn, and stay connected during the pandemic.

However, the increased use of your platform has surfaced significant problems concerning user privacy and safety. Reports from Motherboard revealed that Zoom had shared user data with Facebook without their permission, and separately, had leaked the personal information of at least 1,000 users to strangers. The Federal Bureau of Investigation recently warned about the phenomenon of "Zoom-bombing", where strangers drop into Zoom calls, in some cases exposing users to threats, hate speech, and pornographic content. Another report found that Zoom misleadingly claimed that it used end-to-end encryption, when it did not. Last week, it was reported that Zoom had been automatically sending user data to a third-party for data-mining without their permission, including data for several high school students in Colorado.

These revelations have forced technical and policy responses from the company, from strengthening password protection to expanding the "waiting room" feature to block unauthorized participants. In case after case, these issues consistently stem from Zoom's deliberate decision to emphasize ease of use over user privacy and safety.

The latest issue to surface is among the most troubling. Last Friday, the Washington Post discovered that thousands of video recordings of Zoom calls were available on the open web for essentially anyone to view. Although this problem resulted from users uploading video recordings to insecure cloud storage, stronger safeguards for recording and storage could have limited the damage. Moreover, Zoom's uniform naming convention reportedly made these videos much easier to discover.

Many of these videos include intimate details of private businesses and personal relationships, potentially exposing users to significant financial, personal, and psychological harm. It is clear that many users in these videos did not intend whatsoever for their videos to become publicly

available. Yet thousands of Zoom calls are now viewable on widely-used websites such as YouTube and Vimeo. One such video shows a virtual classroom of second-grade children. With over 90,000 schools across the globe now using Zoom for distance learning, it is critical that Zoom correct these problems before more students and teachers end up in online videos against their express wishes.

To clarify Zoom's privacy and security policies, we respectfully ask that you provide answers to the following questions no later than April 15, 2020:

- Please describe all data that Zoom collects from users with and without accounts and please specify how long Zoom retains this data.

- Please list every third party and service provider with which Zoom shares user data and for what purposes and level of compensation, if any.

- Will Zoom require participants to provide affirmative consent if their calls are being recorded or will later be uploaded to the cloud or transcribed? When recorded calls are uploaded and transcribed, will Zoom provide all participants a copy along with an opportunity to correct errors in the recording?

- Does Zoom plan to change the naming convention that allowed thousands of videos to become easily searchable online?

- What steps has Zoom taken to notify users featured in videos that are now searchable online? And when users wish for these videos to be removed, what steps will Zoom take to do so, for example, by engaging the third parties where the videos are now viewable?

- Which privacy settings for users with and without accounts are activated by default, and which require them to opt-in? Does Zoom plan to expand its default privacy settings?

- What dedicated staff and other resources is Zoom devoting to ensure the privacy and safety of users on its platform?

Thank you for your attention to these matters.

Sincerely,

Michael F. Bennet