MIKE CRAPO, IDAHO, CHAIRMAN

RICHARD C. SHELBY, ALABAMA
PATRICK J. TOOMEY, PENNSYLVANIA
TIM SCOTT, SOUTH CAROLINA
BEN SASSE, NEBRASKA
TOM COTTON, ARKANSAS
MIKE ROUNDS, SOUTH DAKOTA
DAVID PERDUE, GEORGIA
THOM TILLIS, NORTH CAROLINA
JOHN KENNEDY, LOUISIANA
MARTHA McSALLY, ARIZONA
JERRY MORAN, KANSAS
KEVIN CRAMER, NORTH DAKOTA

SHERROD BROWN, OHIO
JACK REED, RHODE ISLAND
ROBERT MENENDEZ, NEW JERSEY
JON TESTER, MONTANA
MARK WARNER, VIRGINIA
ELIZABETH WARREN, MASSACHUSETTS
BRIAN SCHATZ, HAWAII
CHRIS VAN HOLLEN, MARYLAND
CATHERINE CORTEZ MASTO, NEVADA
DOUG JONES, ALABAMA
TINA SMITH, MINNESOTA
KYRSTEN SINEMA, ARIZONA

GREGG RICHARD, STAFF DIRECTOR
LAURA SWANSON, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON BANKING, HOUSING, AND
URBAN AFFAIRS

WASHINGTON, DC 20510–6075

April 3, 2020

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

Dear Mr. Yuan:

I write with concern that Zoom Video Communications, Inc. is inaccurately advertising the encryption technology used to secure the Zoom virtual meeting product, putting consumers' information and privacy at risk.

As you know, the technology industry widely defines end-to-end (E2E) encrypted communication systems as ones where only the users doing the communicating can read or hear the messages[1]. In contrast, communication systems that use in-transit encryption make it technologically feasible for service providers to access the contents.

Both Zoom's website[2] and published security white paper[3] tout end-to-end encryption capabilities for its meetings. On March 31, there were reports that a spokesperson for Zoom admitted: "Currently, it is not possible to enable E2E encryption for Zoom video meetings."[4] The details provided by your spokesperson imply Zoom's virtual meeting product uses technologies that the industry would define as in-transit encryption, not the more private E2E encryption.[5]

I acknowledge that your April 1 blog post states that in specific cases you "encrypt all video, audio, screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients."[6] However, that blog post left out critical technical details to accurately inform consumers of your encryption methodologies.

Due to the spread of the COVID-19 virus, social distancing and shelter-in-place requirements have forced Americans to move much of their day-to-day interactions online. As evidenced by Zoom's increase in daily users from 10 million to 300 million over a three-month period, consumers are entrusting your company with their private conversations[7]. It's not just the general public who is relying on your company to provide the encryption it promises—federal

[1] *See* https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

[2] *See* https://zoom.us/security.

[3] *See* https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf.

[4] *See* https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

[5] *Id.*

[6] *See* https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/.

[7] *See* https://www.reuters.com/article/us-health-coronavirus-zoom/zoom-pulls-in-more-than-200-million-daily-video-users-during-worldwide-lockdowns-idUSKBN21K1C7.

government leaders of the COVID-19 virus response spent $1.3 million of taxpayer money on Zoom licenses[8]. It is unthinkable that Zoom has betrayed consumers' trust by leading them to believe their conversations are private when, in fact, Zoom "has the technical ability to spy on private video meetings."[9]

To address these concerns, I respectfully request a response to the following questions no later than April 10, 2020.

1. Please describe the encryption algorithms and key management solutions used in Zoom's:
    a. Free virtual meeting product
    b. Healthcare virtual meeting product
    c. Government virtual meeting product
2. Do any of your products implement true end-to-end encryption where it is not technologically feasible to decrypt meeting contents on Zoom servers? If so, please provide details.
3. In which scenarios does the Zoom virtual meeting product display a green padlock indicator of security?
4. Does your company utilize a secure development lifecycle process? If so, please provide details.
5. Will you be updating your security white paper and marketing materials to more accurately reflect the encryption provided by your services. If so, please provide a timeline. If not, please explain.

Thank you for your attention to this matter.

Sincerely,

Sherrod Brown

Sherrod Brown
Ranking Member

[8] *See* https://www.forbes.com/sites/thomasbrewster/2020/04/02/why-zoom-really-needs-better-privacy-13-million-orders-show-the-us-governments-covid-19-response-is-now-relying-on-it/.

[9] *See supra* n. 4.