United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

April 3, 2020

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580

Dear Chairman Simons:

I write to request that the Federal Trade Commission (FTC) open an investigation into Zoom Video Communications, Inc. (Zoom). Based on media reporting and the company's materials, I believe that the company is engaging in deceptive practices by inaccurately advertising end-to-end encryption of its virtual meetings and putting consumers' information and privacy at risk.

The technology industry has widely defined end-to-end (E2E) encrypted communication systems as ones where only the users doing the communicating can read or hear the messages[1]. For example, when a message is sent over an E2E encrypted service, it stays encrypted until it reaches its destination—phone providers cannot read the message.

In contrast, a communication system that uses in-transit encryption allows service providers to access the message.[2] These types of communication systems provide encryption between the user and the service provider, but an unencrypted copy of the message is stored on the service provider's devices.

Both Zoom's website[3] and published security white paper[4] 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."[5] The technical details provided by Zoom reveals that their video meetings use technologies that the industry would define as in-transit encryption, not the more private E2E encryption.[6] Zoom's April 1 blog post states that in some cases they "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."[7] However, this blog post actually continues Zoom's consumer deception by not clarifying whether it is technologically feasible for them (or a bad actor) to decrypt the meeting

[1] *See* https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.
[2] *See* https://blog.avast.com/end-to-end-encryption-for-text.
[3] *See* https://zoom.us/security.
[4] *See* https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf.
[5] *See* https://theintercept.com/2020/03/31/zoom-meeting-encryption/.
[6] *Id.*
[7] *See* https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/.

on the Zoom servers. True E2E encryption technology does not allow for any extraneous party to retain the ability to decrypt the message.

Zoom's representations appear to meet the elements for deception under the FTC Act: Zoom actively represents that it provides end-to-end encryption. That representation is likely to mislead consumers, and such representations about security of the services provided are material to consumers.[8]

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. Schools are educating remotely, consumers are increasingly relying on telehealth appointments, and video conferencing has replaced social gatherings with loved ones. Zoom's daily users have jumped from 10 million to 200 million in the past three months[9] and federal government leaders of the COVID-19 virus response have spent $1.3 million on Zoom licenses.[10] 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."[11]

The FTC has brought enforcement actions against other technology companies that misrepresent the security or privacy they are providing to their users.[12] Given the increased use of Zoom during this crisis, I ask that the FTC immediately open an investigation into what appears to be Zoom's deceptive representations about the security and privacy it provides to its users.

Thank you for your attention to this matter.

Sincerely,

Sherrod Brown

Sherrod Brown
Ranking Member

---

[8] *See* FTC Policy Statement on Deception, *available at* https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf; *see also FTC v. Tashman*, 318 F.3d 1273, 1277 (11th Cir.2003) (establishing FTC Act liability if there was representation, the representation was likely to mislead customers, and the representation was material); *In the Matter of James V. Grago, Jr*, 2019 WL 1932143, at *1 (where FTC found misrepresentations about data encryption deceptive), *see also In the Matter of BLU Products, Inc.*, 2018 WL 2042050, at *1 (where FTC found false representation about user information disclosure to be deceptive).

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

[10] *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/#6a849e3577e8.

[11] *See supra* n. 5.

[12] *See supra* n. 7.