UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Commissioner
Rebecca Kelly Slaughter

DISSENTING STATEMENT OF COMMISSIONER REBECCA KELLY SLAUGHTER

In the Matter of Zoom Video Communications, Inc.
Commission File No. 1923167
November 9, 2020

Most weekday mornings, my two elementary-age children log on to school through Zoom. Their faces, voices, and occasional silliness are all captured in the Zoom classroom. I try not to dwell on what might occasionally float through in the background of their camera or microphone, but, like many families, we've had moments in our home where we are very much live. After my older kids settle in for class, my own workday begins in earnest and typically involves a series of confidential discussions often made possible through a Zoom meeting. My experience is not unique: Zoom expanded from 10 million daily users last December to over 300 million daily participants this spring. Zoom's overnight expansion from a modest video conferencing company to a company providing critical infrastructure for business, government, education, and social connection raises important questions for the Commission's obligations to protect consumer security and privacy.

Years before the global pandemic would make Zoom a household name, the company made decisions that threatened the security and privacy of its longstanding core business customers. Yet the Commission's proposed settlement provides no recourse for these paying customers. When Zoom's user base rapidly expanded, its failure to prioritize privacy and security suddenly posed a much more serious risk in terms of scope and scale. This proposed settlement, however, requires Zoom only to establish procedures designed to protect user *security* and fails to impose any requirements directly protecting user *privacy*. For a company offering services such as Zoom's, users must be able to trust that the company is committed to ensuring security and privacy alike.

Because the proposed resolution fails to require Zoom to address privacy as well as security, and because it fails to require Zoom to take any steps to correct the deception we charge it perpetrated on its paying clients, I respectfully dissent.

Zoom's Practices

As set forth in the Commission's complaint, Zoom engaged in a series of practices that undermined the security and privacy of its users. First, we allege Zoom made multiple

misrepresentations about its use of encryption. As charged in the complaint, Zoom made false statements about its encryption being "end-to-end," the level of encryption that it offered, and the time it took to store recorded meetings in an encrypted server.[1]

Zoom's problematic conduct was not limited to deception. The complaint charges that beginning in July 2018, Zoom secretly *and unfairly* deployed a web server, called the "ZoomOpener," to circumvent certain Apple privacy and security safeguards enjoyed by Safari browser users. Because of these safeguards, Safari users who clicked on a link to join a Zoom meeting would receive an additional prompt that read, "Do you want to allow this page to open 'zoom.us'?" [2] That is until, we allege, Zoom overrode this feature through its secret ZoomOpener, which bypassed the Safari safeguard to directly launch the Zoom App.[3] The user was then automatically placed in the Zoom meeting, and, if the user had not changed her default video settings, her webcam was activated.[4]

In addition to these unfair and deceptive practices, which the Commission charged as law violations, there has been extensive public reporting on several other Zoom practices that raised serious privacy concerns. For example, Zoom business customers who subscribed to a service called "LinkedIn Sales Navigator" had access to LinkedIn profile data about other users in a meeting—even when the other user wished to remain anonymous.[5] Additionally, Security researchers found that Zoom-meeting video recordings saved on Zoom's cloud servers had a predictable URL structure and were thus easy to find and view.[6] And of course there was widespread coverage of "Zoom-bombing," in which uninvited users crashed Zoom meetings.[7] Zoom took steps to address these vulnerabilities after they surfaced by changing naming conventions, permanently removing the LinkedIn Sales Navigator app,[8] and requiring meeting passwords as the default setting for more Zoom users,[9] but these problems suggest Zoom's approach to user privacy was fundamentally reactive rather than proactive.

---

[1] *See* Complaint ¶¶ 16–33.

[2] Complaint ¶ 35. If the user selected "Allow," the browser would connect the user to the Zoom meeting. *Id*. This safeguard was not specific to Zoom; Apple had designed its Safari browser to help defend its users from malicious actors and popular malware by requiring interaction with a dialogue box whenever any website or link attempted to launch an outside app. *Id*. at ¶ 34.

[3] *Id*. at ¶ 36.

[4] *Id*. at ¶ 37.

[5] *See* Aaron Krolik and Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*, N.Y. Times (Apr. 2, 2020), https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html. Zoom subsequently stated that it had disabled the feature.

[6] *See* Paul Wagenseil, *Zoom security issues: Here's everything that's gone wrong (so far)*, Tom's Guide (Nov. 3, 2020), https://www.tomsguide.com/news/zoom-security-privacy-woes.

[7] *See* Jay Peters, *Zoom adds new security and privacy measures to prevent Zoombombing*, The Verge (Apr. 3, 2020), https://www.theverge.com/2020/4/3/21207643/zoom-security-privacy-zoombombing-passwords-waiting-rooms-default.

[8] *See* Eric S. Yuan, *A Message To Our Users*, Zoom Blog (Apr. 1, 2020), https://blog.zoom.us/a-message-to-our-users/.

[9] *See* Deepthi Jayarajan, *Enhanced Password Capabilities for Zoom Meetings, Webinars & Cloud Recordings*, Zoom Blog (Apr. 14, 2020), https://blog.zoom.us/enhanced-password-capabilities-for-zoom-meetings-webinars-cloud-recordings/.

Lack of Privacy Protections

Too often we treat data security and privacy as distinct concerns that can be separately preserved. In reality, protecting a consumer's privacy and providing strong data security are closely intertwined, and when we solve only for one we fail to secure either. The Commission's proposed order resolving its allegations against Zoom requires the company to establish an information-security program and submit to related independent third-party assessments. These provisions strive to improve data-security practices at the company and to send a signal to others regarding the baseline for adequate data-security considerations. Nowhere, however, is consumer privacy even mentioned in these provisions. This omission reflects a failure by the majority to understand that the reason customers care about security measures in products like Zoom is that they value their privacy.

Some might argue that sound data security practices should naturally guarantee consumer privacy. I disagree. Strong security is necessary for consumer privacy, but it does not guarantee its achievement. Zoom's launch of its "ZoomOpener" to undermine the Apple Safari browser protections is an instructive example. Zoom prioritized maintaining its one-click functionality for users over privacy and security protections offered by Apple. The Commission's proposed order tries to solve for this problem solely as a security issue and makes it difficult for Zoom to bypass third-party security features in the future. But the order does not address the core problem: Zoom's demonstrated inclination to prioritize some features, particularly ease of use, over privacy protections. Dumping Safari users automatically into a Zoom meeting, with their camera on, the first time they clicked on a link was not only a data-security failing—it was a privacy failing.

Similarly, we often discuss data encryption as a security issue, which of course it is, but we should simultaneously be recognizing it as a privacy issue. When customers choose encrypted communications, it is because they value their privacy in the content of their conversations. Treating encryption failures as a security-only issue fails to recognize the important privacy implications.

The FTC has approached privacy and security issues with related but distinct remedies: by imposing a comprehensive privacy program (as we did in *FTC v. Uber*) or by imposing a comprehensive information security program (as we did in *FTC v. Equifax*). This case provides a perfect example of a place where we ought to have required elements of both privacy and security programs. A more effective order would require Zoom to engage in a review of the risks to consumer *privacy* presented by its products and services, to implement procedures to routinely review such risks, and to build in privacy-risk mitigation before implementing any new or modified product, service, or practice. The Commission required this type of privacy-focused inquiry in the "Privacy Review Statement" provisions of its order in the *FTC v. Facebook* matter.[10] Privacy-focused provisions such as these should either be added to relevant data-privacy orders as a separate privacy program or review, or the Commission's information

[10] To be clear, I am not suggesting that Zoom's conduct giving rise to this matter and Facebook's order violations are equivalents. Nor do the companies share similar business models. But in terms of the importance of consumer privacy, hundreds of millions of users are entrusting Zoom with some of their most sensitive interactions, and they are doing so from their homes.

security programs should be modified to better integrate privacy and security.

When companies offer services with serious security and privacy implications for their users, the Commission must make sure that its orders address not only security but also privacy.

No Recourse for Customers

As of July 2019, Zoom had approximately 600,000 paying customers, and approximately 88% of those customers were small businesses with ten or fewer employees.[11] In securing these customers, the Commission charges that Zoom made express representations regarding its encryption offerings that were false. Yet, the proposed order does not require Zoom to take any steps to mitigate the impact of these statements we contend are false. Zoom is not required to offer redress, refunds, or even notice to its customers that material claims regarding the security of its services were false. This failure of the proposed settlement does a disservice to Zoom's customers, and substantially limits the deterrence value of the case.

Finally, I join Commissioner Chopra's call for the Commission to engage in critical reflection to strengthen our enforcement efforts regarding technology across the board—from investigation to resolution.[12]

[11] Complaint ¶ 9.

[12] Commissioner Chopra's dissenting statement sets forth an excellent list of *Recommendations and Corrective Actions* for the Commission to consider to improve the effectiveness of our enforcement efforts.