ALSTON & BIRD

WWW.ALSTON.COM

Consumer Protection/FTC ADVISORY ■

NOVEMBER 18, 2020

Three Key Takeaways from the FTC's Settlement with Zoom

By Kathleen Benway and Nameir Abbas

The Federal Trade Commission (FTC) recently announced a settlement with Zoom Video Communications Inc., the company that provides the well-known video conferencing platform Zoom, to settle allegations that the company engaged in a series of deceptive and unfair practices that undermined the security of its users. The vote to approve the settlement was a 3–2 split along party lines, with the three Republicans voting in favor of the settlement and the two Democrats voting against.

FTC's Complaint

The complaint alleges that Zoom made deceptive representations about its encryption practices since at least 2016. Zoom claimed in blog posts, in the Zoom app, on the Zoom website, and in other Zoom documentation that it uses "end-to-end" encryption and repeated these claims to customers that asked questions about Zoom's security practices. However, Zoom acknowledged in April 2020 that its services were generally incapable of end-to-end encryption. Zoom also claimed to use 256-bit encryption, but according to the complaint used weaker 128-bit encryption. The complaint also alleged that although Zoom claimed to store recordings of meetings in Zoom's cloud storage in an encrypted format, it actually stored them in an unencrypted format for 60 days on Zoom's servers before transferring them to the cloud to be stored in an encrypted format.

According to the FTC, Zoom also unfairly circumvented third-party privacy and security safeguards and deceptively failed to disclose that a July 2018 update would install a local hosted web server (called "ZoomOpener"). More specifically, Zoom updated its Mac application in a way that allowed Zoom to directly launch a Zoom meeting when the Safari user clicked a link *without* the user receiving the typically required additional prompt to either allow or cancel the launch. Users could therefore inadvertently click a link that opened a Zoom meeting without their permission, which would in turn activate the user's webcam without their knowledge. Furthermore, according to the FTC, ZoomOpener installed software updates without properly validating that the updates were downloaded from a trusted source, putting some users at risk of remote-control execution attacks or local denial of service attacks. ZoomOpener would also remain on a user's system even if a user uninstalled the Zoom application using standard instructions and would automatically reinstall the application if the user later accessed a Zoom meeting.

Consent Order

The FTC's consent order will require Zoom to maintain a comprehensive written information security program with specified components – relating to governance, risk assessment, and safeguards to address identified risks. These safeguards must include the implementation of a "security review" for specified software and software updates before release. One aspect of this review is that it must determine whether the software or software update is designed to "circumvent or bypass" third-party security features such that they no longer provide users with the same protections from unauthorized activity or other compromise of the users' information and assess the associated risks. Furthermore, Zoom is required to implement policies, procedures, and any applicable technical measures to ensure that Zoom does not implement new software or software updates that circumvent or bypass security features unless there is no associated material risk or Zoom implements offsetting or mitigating security measures.

Another notable required safeguard is that Zoom must implement policies, procedures, and technical measures "designed to reduce the risk of online attacks resulting from the misuse of valid Credentials by unauthorized third parties," including the use of "automated tools to identify non-human login attempts," "rate-limiting login attempts," and "implementing password resets for known compromised" credentials.

Dissenting Commissioners' Statements

The FTC's two Democratic commissioners, Rebecca Slaughter and Rohit Chopra, voted against the settlement and issued dissenting statements. Each dissent argues that the consent order did not provide sufficient relief to address Zoom's practices.

Slaughter suggests that a "more effective order" would require Zoom to review the risks that its products and services pose to consumer *privacy*, in addition to security. She cited a number of examples, including that Zoom allowed business subscribers to view LinkedIn information on users in a Zoom meeting even when the users wished to remain anonymous, storage of Zoom meeting video recordings using a predictable URL structure rendering the recordings easy to find and view, and not implementing meeting passwords as a default setting, making it easy for uninvited users to "crash" Zoom meetings, that "suggest Zoom's approach to user privacy was fundamentally reactive rather than proactive."

Chopra's dissent focuses on harm to the marketplace, arguing that the deceptions alleged in the FTC's complaint helped to generate a massive windfall for the company (and served to limit competition) that was not addressed by the consent order. Chopra also suggests that the FTC should have sought additional protections or remedies for small businesses and other users. Chopra suggests measures the FTC could take in the future to enhance its enforcement, "especially when it comes to large players in digital markets," including strengthening orders to emphasize help for individual consumers and small businesses, investigating firms "comprehensively" across the FTC's mission (i.e., through its legal authorities related to data protection, consumer protection, and competition together), and increasing cooperation with international, federal, and state partners.

The majority statement in favor of the settlement notes that the additional forms of relief proposed by the dissenting commissioners could have required protracted litigation and that it made more sense to seek timely relief to protect users' privacy and security now.

Key Takeaways

The Zoom settlement and the commissioners' statements raise a few interesting points about the direction of FTC enforcement, particularly as we move into 2021 and a new Administration.

First, the consent order appears to be highly tailored in at least two areas that were particularly relevant to the allegations against Zoom, demonstrating the continued enhanced specificity of the FTC's consent orders. For example, the "security review" that the consent order requires must specifically include an assessment of whether a piece of software or update is designed to circumvent or bypass a third-party security measure. This requirement clearly flows from Zoom's usage of a local web server to get around web browser safeguards that would have otherwise asked the user for permission before opening Zoom. As another example, the consent order will require the company to implement safeguards designed to reduce the risk of online attacks resulting from the "misuse of valid" credentials by "unauthorized third parties," referencing the use of automated tools to identify non-human login attempts and other measures to protect against brute-force attacks. While not completely clear, these requirements could flow from the company's large online user base and the risks consumers face from brute-force or credential-stuffing attacks.

Second, the dissenting statements could signal an interest in addressing privacy and security concerns in a more holistic fashion. While Slaughter's dissent emphasizes the intertwined risks to security and privacy posed by Zoom's practices, Chopra's dissent focuses more on the lack of relief for past conduct and for the damage to the marketplace allegedly already caused. In either case, the dissenting commissioners would have sought to strengthen the consent order and the relief sought because of the way that the company's security practices fostered or reflected other issues.

Third, the consent order highlights how companies can face increasing scrutiny as their business expands rapidly, emphasizing the potential value of security and privacy by design for younger, smaller, or quickly growing companies. In Zoom's case, the coronavirus pandemic expanded the company's user base significantly – from 10 million in December 2019 to 300 million in April 2020 – magnifying security and privacy harms its practices and vulnerabilities created.

You can subscribe to future ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Kathleen Benway
202.239.3034
kathleen.benway@alston.com

Alexander G. Brown
404.881.7943
alex.brown@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

James A. Harvey
404.881.7328
jim.harvey@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Joseph H. Hunt
202.239.3278
404.881.7811
jody.hunt@alston.com

Amy S. Mushahwar
202.239.3791
amy.mushahwar@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Nameir Abbas
202.239.3004
nameir.abbas@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor, Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333