e-Competitions
Antitrust Case Laws e-Bulletin

Concurrences
Antitrust Publications & Events

Competition Law & Covid-19

The US FTC settles allegations that a real-time communications platform offering a videoconferencing software has engaged in a series of unfair practices and requires it to enhance its security procedures *(Zoom)*

UNILATERAL PRACTICES, INVESTIGATIONS / INQUIRIES, AUDIOVISUAL , TELECOMMUNICATIONS, SETTLEMENT, INFORMATION TECHNOLOGY, UNITED STATES OF AMERICA, CONSUMER PROTECTION, ONLINE PLATFORMS, PRIVACY, COVID-19

US FTC, *Zoom*, File No. 192 3167, Agreement containing Consent Order, 9 November 2020

Lale Tuzmen Aktas | Macmillan Keck (New York)

e-Competitions Special Issue Competition Law & Covid-19

During the Covid-19 pandemic, Zoom Video Communications, Inc. (Zoom) gained enough popularity to attract the FTC's attention, including to its security practices. The FTC-Zoom *settlement* announced on November 9, 2020, which requires Zoom to implement a robust information security program, marked its entry to the ranks of big tech companies.

Background

Zoom is a real-time communications platform offering a videoconferencing software as a service, plus certain add-ons such as the option to save meetings on the cloud. Zoom was founded in 2011 and, until the Covid-19 pandemic made it the videoconferencing tool of choice, most of its customers were small businesses. Zoom's daily user base grew from 10 million in December 2019 to 300 million in April 2020. In addition to Zoom's traditional business customers, individuals, doctors, mental health professionals, and schools started using Zoom's videoconferencing services during the pandemic. However, a growing number of "zoom-bombing" incidents and other customer complaints brought Zoom's security practices under the regulator's spotlight. [*1*] [*2*] The FTC *complaint* in question alleges that the videoconferencing provider engaged in a series of deceptive and unfair practices that undermined the security of its users in violation of Section 5 of the US Federal Trade Commission Act.

Allegations

- *Misrepresentations about the strength of Zoom's security features*. The complaint alleges violations of the FTC Act on five separate counts. The first three counts of alleged violations concern false or misleading

representations about Zoom's encryption. Zoom has allegedly misrepresented over the years that it uses end-to-end 256-bit Advanced Encryption Standard (AES) on various platforms, including its app, website, Security Guides, HIPAA compliance Guide, blog posts, and direct communications with customers. End-to-end encryption means no one other than the communicating parties – not even Zoom itself – has access to encrypted communications. The first allegation is that Zoom kept copies of encryption keys on its servers, which would allow Zoom to access the content of its users' Zoom meetings. Second, Zoom's encryption key was allegedly not 256-bit as advertised, but instead 128-bit, which is a shorter key, easier to hack, and provides less confidentiality protection compared to 256-bit encryption. Third, this protection allegedly did not apply to customers who saved their meetings on the server (for example, doctors who want to keep a copy of their communications with a patient for future reference). The FTC alleged that even though recorded meetings were encrypted once they were transferred to the cloud, they were held in Zoom's servers for up to 60 days, unencrypted, until they were transferred to the cloud.

- *Implementation of a software update that circumvented a browser security feature*. The remaining two counts relate to the way Zoom handled Apple computer users. The FTC's complaint alleged that Zoom secretly installed software called ZoomOpener, which allowed Apple computers to launch the app in a way that circumvented Safari's new browser privacy protection. The Zoom meeting would launch directly with one click from the Safari browser. The ZoomOpener web server also allegedly exposed users to other vulnerabilities and made them easier targets for hackers. Even if a user deleted Zoom from the Mac computer, the ZoomOpener web server would remain on the computer, continuing to expose the user to the same security vulnerabilities. Finally, on count five, the FTC alleged that the ZoomOpener web server was disguised as a software update to fix minor bugs; Zoom failed to make adequate disclosures to its users about what the new update entailed.

Consent Order and Settlement

FTC consent decrees and settlements typically require organizations to implement and maintain a security compliance program. Similarly, in this case, the FTC Commission voted 3-2 along party lines to accept the consent agreement with the company. Zoom did not admit or deny the allegations in the settlement but agreed to implement a new mandated information security program within 60 days. Zoom also agreed to use more secure safeguards like multi-factor authentication and data deletion, document potential risks annually and find ways to mitigate these risks and implement a vulnerability management program. Also, Zoom will be required to undergo independent security audits every other year. Finally, Zoom agreed not to make misrepresentations about privacy, security and data usage.

The consent decree sharpens the FTC's enforcement teeth. Under Section 5 of the FTC Act, the FTC can seek monetary penalties when an organization violates a consent decree. For example, in 2012 Google paid $22.5 million to settle FTC allegations that it violated a prior consent order by placing tracking cookies on certain users' computers despite its representations to the contrary. [*3*] Similarly, in 2019, Facebook settled with the FTC for a record-setting $5 billion over claims that it violated a 2012 privacy-related order. [*4*]

Dissenting Statements and Critique

FTC Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson, all Republicans, defended the settlement in a *majority statement*, stating that the deal provided 'immediate and important relief to consumers' while ensuring that Zoom would 'prioritize consumers' privacy and security' moving forward. However,

Commissioners *Rohit Chopra* and *Rebecca Kelly Slaughter*, the FTC's two Democrats, issued separate dissenting statements expressing their views that the proposed settlement fell short in providing redress to users allegedly misled by Zoom's practices and imposing meaningful accountability on the company.

In his dissent, Commissioner Chopra criticized the consent agreement for not providing for meaningful accountability for Zoom; it provided no help for affected users, did nothing for small businesses that relied on Zoom's data protection claims, and did not require Zoom to pay a fine. He added that Zoom's misrepresentation of its security practices allowed it to steal users from competing players in the video conferencing market, and to "cash in" on the pandemic.

Commissioner Chopra pondered the risk that all tech titans expand their empires through deception. Growth-stage companies, in the interest of acting and growing quickly, may engage in deceptive practices, which he believes harms consumers and competition. It is a fact that privacy is not a priority for companies until they are big enough to be brought under scrutiny by regulators. As Professor Daniel J. Solove and Professor Woodrow Hartzog noted, "[i]n a weird sense, for tech companies, being enforced against by the FTC for a privacy or security violation has become an initiation ritual to being recognized in the pantheon of the tech company big leagues." [*5*] FTC scrutiny is almost a pat on the shoulder letting tech companies know that they made it.

As Commissioner Chopra noted in his dissent, Zoom's lack of disclosure to its investors (it is a publicly traded company) about the FTC's law enforcement inquiry suggests that the company did not think it would have a material impact on the business. Chris Hoofnagle has *suggested* that the "FTC's catch and release policy appears to have lost its deterrent effect." The concern is that the FTC's current approach allows companies to capitalize on a product by breaking the law first, entrenching themselves in the market, and paying a modest regulatory price later.

In Commissioner Slaughter's dissent, she expressed concern that the Commission's action did not sufficiently address the associated privacy issues connected to Zoom's actions. The Zoom case is a privacy case as much as it is a data security case. She criticized the consent order for its lack of consumer privacy protections. She noted that Zoom should have been ordered 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."

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.

- **Debate on privacy and competition.** To put this case into perspective, the FTC-Zoom settlement was announced only three days after Congress unveiled the nearly 450-page big tech antitrust report finding that Amazon, Apple, Facebook and Google each hold monopoly power. The report calls for revising the antitrust laws to address what it considers to be big tech's monopoly problem. At the same time, there are extensive efforts to develop federal privacy legislation while individual US States introduce such laws as the State level. Policy makers, legislators and regulators will have to consider whether regulation is needed not only for large tech companies but also for those that are still growing. The Zoom case offers insights into market failures and privacy. The FTC clearly values third party providers' enhanced privacy and security safeguards, such as Apple's Safari browser safeguards, as we have seen in the Zoom case as well as the Google case. [*6*] However, it is not clear whether consumers value Safari's additional layers of protection as much as the FTC

does. The Covid-19 pandemic showed that consumers continued to use Zoom despite news of Zoom-bombings and the notorious ZoomOpener because it had a very simple user interface compared to its competitors. Consumers apparently chose convenience over privacy. Time will show whether competition leads to greater privacy and whether consumers will shift towards products that have the highest levels of privacy and security protection.

- **Privacy by design.** 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. Going forward, growth-stage companies may show more interest in integrating privacy principles into their product early-on. Also, observing that Zoom's blog posts and communications with customers from its early days were brought under scrutiny, small companies may pay more attention to making accurate statements across all platforms.

- **A more holistic approach to privacy and security**. The dissenting statements could signal an interest in addressing privacy and security concerns in a more holistic fashion. Commissioner Slaughter's dissent emphasizes the inter-connected risks to security and privacy posed by Zoom's practices, remarking that "when we solve only for one we fail to secure either."

- **Interest in Stronger Enforcement.** Commissioner Chopra criticized the agency's overall approach to oversight of companies operating in the digital market and created a roadmap for conducting more proactive and comprehensive investigations. He suggested using interdisciplinary teams and technologists, and increasing collaboration with other international, federal, and state partners where appropriate. He also laid out how the FTC could expand its authority under the current laws to enable the FTC to seek monetary relief for violations. If the FTC acts on one or more of Commissioner Chopra's suggestions, we would see increasing enforcement action in the near future.

[1] Allyn, B. (2020, May 07). Zoom to Crack Down on Zoombombing, In Deal with NY Attorney General. *https://www.npr.org/2020/05/07/852186312/zoom-to-crack-down-on-zoombombing-in-deal-with-ny-attorney-general*

[2] Tilley, Aaron. *Zoom to Get Closer Scrutiny Under FTC Settlement*. 9 Nov. 2020, *www.wsj.com/articles/zoom-to-get-closer-scrutiny-under-ftc-settlement-11604940184*.

[3] "Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser." Federal Trade Commission, 28 Feb. 2019, *www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented*.

[4] "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook." Federal Trade Commission, 28 Apr. 2020, *www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions*.

[5] Solove, Daniel, and Woodrow Hartzog . *The FTC Zoom Case: Does the FTC Need a New Approach?* 17 Nov. 2020, teachprivacy.com/the-ftc-zoom-case-does-the-ftc-need-a-new-approach/?utm_source=Opt-in+Newsletter.

[6] Federal Trade Commission, see note 3.