Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of	)	
	)	
Zoom Video Communications, Inc.	)	Commission File No. 1923167
	)	
	)	

COMMENTS BY NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE REGARDING ZOOM VIDEO COMMUNICATIONS, INC.

Christine Bannan
Andi Wilson Thompson
New America's Open Technology Institute
740 15th Street NW, Suite 900
Washington, D.C. 20005

December 14, 2020

Introduction

New America's Open Technology Institute (OTI) appreciates the opportunity to submit a statement on the Federal Trade Commission's (FTC) proposed consent agreement with Zoom, Communications Inc.[1] OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technologies that are open and secure, and their benefits. We support and defend the right to privacy and freedom of expression, and press internet platforms to provide greater transparency and accountability around their operations, technologies, and impacts. We urge the Commission to strengthen the proposed consent agreement because the terms do not match the severity of Zoom's misrepresentations about encryption.

Strong Encryption is Crucial to Protecting Privacy

In an April 2020 blog post Zoom CEO Eric Yuan announced that the platform's user base had exploded, reaching 300 million daily meeting participants.[2] This was thirty times the number they had in December 2019, fueled by the need to stay connected now that most of the world was newly working, studying, and socializing from home. The importance of secure and private online communications during the COVID-19 pandemic cannot be overstated.[3] Since it is currently unsafe to share physical spaces with groups of colleagues, friends, and loved ones we are turning to video conference tools to conduct our sensitive and personal conversations.

Appointments with medical or legal professionals are taking place over Zoom now, as are many weddings and funerals. Encryption is crucial to ensuring that these interactions are secure and private.[4] At the beginning of the pandemic, Zoom claimed that users' communications were encrypted both in transit, using end-to-end encryption, and at rest when stored on their servers. It also claimed that it was using AES 256 encryption to encrypt stored data. All of these claims turned out to be misleading. This deception violated user security and privacy, as well as undermining user trust. Users cannot benefit from encrypted communications if they are not confident that the products providing them are trustworthy.

Discussions about the importance of encryption in transit and at rest are often centered around the issue of security. Security from hackers or cyber criminals, security from government or corporate surveillance, or the security encryption provides for vulnerable users are often the

---

[1] "Zoom Video Communications, Inc.; Analysis To Aid Public Comment," Federal Trade Commission, 85 FR 72650, November 13, 2020, https://www.federalregister.gov/documents/2020/11/13/2020-25130/zoom-video-communications-inc-analysis-to-aid-public-comment.

[2] "90-Day Security Plan Progress Report: April 22," Zoom Blog, April 22, 2020, https://blog.zoom.us/90-day-security-plan-progress-report-april-22/.

[3] "Event: Digital Security Needs a Work-From-Home Makeover," New America's Open Technology Institute, April 21, 2020, available at https://www.newamerica.org/oti/events/online-digital-security-needs-work-home-makeover/.

[4] Claire Park and Andi Wilson Thompson, *Privacy's Best Friend: The Importance of Encryption in Protecting Consumer Privacy*, New America's Open Technology Institute, August 24, 2020, available at https://www.newamerica.org/oti/reports/privacys-best-friend/.

pillars of arguments made by encryption activists. These correctly describe specific situations or users to whom encryption is important, but often miss the ways that encryption is important to protect privacy as well.[5] As Commissioner Slaughter noted in her dissent: "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."[6]

Strong encryption can help establish user trust in a product or service, and Zoom has violated that trust by misrepresenting the features provided by their product. If communications are truly encrypted end-to-end, then only a message's sender and recipient can decrypt the content of that message. When implemented correctly, Zoom should not hold the cryptographic keys necessary to review content sent using its tools. The company's misrepresentation that, since at least June 2016, they provided end-to-end encrypted communications not only violated the privacy of its users but also their confidence in Zoom's service.

Although Zoom reports that it has now actually implemented end-to-end encryption, that does not in itself remedy the harms it has caused to users. Until it came to light in the media, the tens of millions of users who had chosen Zoom over its competitors were trusting that their communications were protected in the way the company publicly claimed. Years of private and sensitive communications were transmitted and held insecurely, and the current order does not appropriately hold Zoom to account for this.

The Proposed Consent Agreement Reflects a Flawed Enforcement System

Consent agreements should both provide remedies for the unfair and deceptive practices alleged and seek to prevent future wrongdoing. The FTC's proposed consent agreement with Zoom fails to achieve either of these goals fully.

The FTC should modify the proposed consent agreement to include notice and remedy for affected Zoom users. Zoom is not required to notify users of the security violations even though many users who made calls containing confidential information did so under the belief that their communications would be private. This was not the case and those users who paid for Zoom's falsely advertised service will not be refunded or permitted to end their contracts.

The fact that the order as written requires Zoom to implement a comprehensive security program, but not a privacy program, ignores the fact that poor or deceptive encryption practices aren't just dangerous because of the potential for a security breach. The proposed order's requirements do not take all of the necessary steps to remedy the harms that Zoom has caused. While the majority argues that attempts to include a comprehensive privacy program will likely

[5] "Event: Privacy's Best Friend, How Encryption Protects Consumers, Companies, and Governments Worldwide," New America's Open Technology Institute, February 2, 2020, available at https://www.newamerica.org/oti/events/privacys-best-friend/.
[6] "Dissenting Statement of Commissioner Rebecca Slaughter Regarding Zoom Video Communications, Inc. Commission File No. 1923167," November 6, 2020,

cause protracted litigation, the fact remains that an incomplete order will not appropriately protect Zoom's users from future harm.

However, remedies for harmed users would not be sufficient alone to fix the proposed consent agreement because it also contains flaws that are indicative of the Commission's deficient privacy and security enforcement regime. The status quo of FTC enforcement has had severe consequences for privacy and security. OTI supports Commissioner Chopra's proposed reforms to restore the agency's enforcement credibility, including the recommendation to determine whether third-party assessments are effective.[7]

The FTC should reexamine the major assumption underpinning privacy and security consent orders that third-party assessments effectively detect and prevent future misconduct. The 2019 Facebook case drew attention to the limitations of the FTC's reliance on third-party assessors to track compliance. The 2011 consent order stipulated that the company create a privacy program and submit to biannual third-party compliance assessments. The allegations in the FTC complaint enforcing that order all occurred while Facebook was undergoing regular assessments, and the assessors did not detect the violations. The assessors found that "Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information" during the 2015-2017 reporting period.[8]

This could have been a moment of internal reckoning at the FTC, but instead the Commission continues to rely on similar third-party assessments to enforce the privacy and security program requirements in consent orders. The FTC should not have to rely on investigative journalism and independent researchers to be notified of violations of its consent orders.

Conclusion

OTI recommends that the Commission strengthen the proposed consent agreement by requiring Zoom to implement a comprehensive privacy program and to provide notice and a remedy to affected users. OTI also urges the Commission to reevaluate the method for monitoring compliance through third-party assessments.

---

[7] "Dissenting Statement of Commissioner Rohit Chopra Regarding Zoom Video Communications, Inc. Commission File No. 1923167," November 6, 2020 https://www.ftc.gov/system/files/documents/public_statements/1582914/final_commissioner_chopra_dissenting_statement_on_zoom.pdf.

[8] "Independent Assessor's Report on Facebook's Privacy Program, Biennial Report For the period February 12, 2015 to February 11, 2017, https://epic.org/foia/FTC/facebook/EPIC-18-03-20-FTC-FOIA-20180626-FB-Assessment-2017.pdf