UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Rohit Chopra

DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA

Regarding Zoom Video Communications, Inc.
Commission File No. 1923167

November 6, 2020

Summary

- When companies deploy deception, this harms customers and honest competitors, and it distorts the marketplace. This is particularly problematic when it comes to the digital economy.
- Zoom's alleged security failures warrant serious action. But the FTC's proposed settlement includes no help for affected parties, no money, and no other meaningful accountability.
- The FTC's status quo approach to privacy, security, and other data protection law violations is ineffective. However, Commissioners can take a series of concrete steps to change this.

Introduction

Sometimes a new product becomes inextricably linked to the brand that made it popular. Kleenex, Band-Aids, and Frisbees are examples where the company became synonymous with the product.[1] This is particularly true in the digital economy where products can improve the use and capability of technology to the point of transforming its role in everyday life. We use "Google" as a verb when referring to use of a search engine. We "Uber" when we need a ride across town. And now, we "Zoom" when referring to videoconferencing. If becoming a verb threatens a trademark, firms fight against it. If it means becoming the default product in a market, they fight for it. But, profiting through unlawful means must come with real consequences.

Zoom (NASDAQ: ZM) did not invent web-based video conferencing. Indeed, there are many other players in the market. But Zoom succeeded in becoming the "default" for many businesses, both large and small, capturing a significant market share despite a crowded field. However, the allegations in the FTC's complaint raise questions whether Zoom's success – and the tens of billions of dollars of wealth created for its shareholders and executives in a short period of time – was advanced through fair play.[2] In my view, the evidence suggests that deception helped to create this windfall.

With businesses, families, schools, and even governments using Zoom to share extremely sensitive information, the alleged security vulnerabilities of this video conferencing platform raise major concerns, including threats to our privacy[3] and national security.[4]

Today, the Federal Trade Commission has voted to propose a settlement with Zoom that follows an unfortunate FTC formula. The settlement provides no help for affected users. It does nothing for small businesses that relied on Zoom's data protection claims. And it does not require Zoom to pay a dime. The Commission must change course.

Deception Distorts Competition

When companies need to act quickly to exploit an opportunity, deploying deception to steal users or sales from competing players is tantalizing. When video conferencing became a necessity for many

---

[1] Mark Abadi, *Taser, Xerox, Popsicle, and 31 more brands-turned-household names*, BUSINESS INSIDER (June 3, 2018), https://www.businessinsider.com/google-taser-xerox-brand-names-generic-words-2018-5.
[2] Richard Waters, *Zoom to cash in on pandemic success with apps and events*, FINANCIAL TIMES (Oct. 14, 2020), https://www.ft.com/content/f1731672-e965-48a1-9362-bab122fc9bf4.
[3] In her voting statement, Commissioner Rebecca Kelly Slaughter details some of the key intersections between privacy and security.
[4] Sonam Sheth, *Foreign intelligence operatives are reportedly using online platforms and video-conferencing apps like Zoom to spy on Americans*, BUSINESS INSIDER (Apr. 9, 2020), https://www.businessinsider.com/foreign-intelligence-agents-china-spying-on-americans-zoom-2020-4.

businesses and families, existing players saw a potential gold mine. Even though we can all technically use multiple videoconferencing platforms as participants, a videoconferencing provider's monetization will largely be driven by how many businesses adopt its offering as their enterprise videoconferencing solution.[5] FTC prohibitions on unfair or deceptive practices are supposed to temper the temptation to deceive customers.

Before the pandemic, Zoom primarily focused on business customers. Small and large businesses alike were looking for ways to connect with clients and business partners through video conferencing. Zoom competed with Microsoft's Skype, Microsoft's Teams, Cisco's WebEx, BlueJeans, and many other products. Comparison guides point out the different strong points of each service – from encryption to price.[6] In the summer of 2019, Zoom had over 600,000 customers that paid fees to use Zoom's services.[7] These customers were overwhelmingly small businesses.[8]

Small businesses often don't have employees dedicated to information security or even to information technology more broadly. That's why they rely on representations made by those they purchase software and services from. Many businesses want to ensure that any software application they use, including any video conferencing solution, comes with meaningful security standards. Zoom had to respond to this critical customer need if it was going to compete. Once the pandemic shut down workplaces across the country, businesses needed to find a reliable solution that was also secure. Many chose Zoom.[9]

Zoom sold its customers on the idea that it was an easy-to-use service that took "security seriously." However, when examining the company's engineering and product decisions, a different reality emerges. For example, as the complaint alleges, Zoom installed a web server onto users' computers, without permission, as an end-run that would circumvent a browser security feature – all to avoid an extra dialogue box.[10] Zoom went further: even if you managed to uninstall Zoom, it would not remove the web server.[11] And that web server could secretly re-install Zoom, even without your permission.[12] This is not just troubling conduct – this is what some have called "malware-like" behavior.[13]

This fervent attention to detail – going to great lengths to avoid a single dialogue box – did not extend to the security features it touted in sales materials.[14] The FTC's complaint details a litany of serious security allegations, from not using what is "the commonly accepted definition" of end-to-end encryption to being a year or more behind in patching software in its commercial environment.[15]

---

[5] Zoom Video Communications, Inc., Oct. 2019 Quarterly Report (Form 10-Q) (Dec. 9, 2019), https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552119000059/zm-20191031.htm.
[6] Kari Paul, *Worried about Zoom's privacy problems? A guide to your video-conferencing options*, THE GUARDIAN (Apr. 9, 2020), https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives.
[7] Compl., *In the Matter of Zoom Video Communications, Inc.*, Comm'n File No. 1923167 (Nov. 9, 2020).
[8] *Id.*
[9] Matt Torman, *5 Reasons Why Zoom Will Benefit Your Small Business*, ZOOM (Jan. 24, 2020), https://blog.zoom.us/zoom-video-communications-small-business-benefits/.
[10] Compl., *supra* note 7.
[11] David Murphy, *Remove Zoom From Your Mac Right Now*, LIFEHACKER (July 9, 2020), https://lifehacker.com/remove-zoom-from-your-mac-right-now-1836209383.
[12] *Id.*
[13] Jacob Kastrenakes, *Zoom saw a huge increase in subscribers — and revenue — thanks to the pandemic*, THE VERGE (June 2, 2020), https://www.theverge.com/2020/6/2/21277006/zoom-q1-2021-earnings-coronavirus-pandemic-work-from-home.
[14] Compl., *supra* note 7.
[15] Michael Lee & Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT (Mar. 31, 2020), https://theintercept.com/2020/03/31/zoom-meeting-encryption/; Compl., *supra* note 7; Oded Gal, *The Facts Around Zoom and Encryption for Meetings/Webinars*, ZOOM (Apr. 1, 2020), https://blog.zoom.us/facts-around-zoom-encryption-for-meetings-webinars/.

Zoom's Windfall

Zoom has "cashed in" on the pandemic.[16] While Zoom doesn't publicly share its total number of users, the company has confirmed that it has nearly four times the number of customers with 10 or more employees than they had at this time a year ago.[17] Their stock value has soared.[18] Zoom's CEO, Eric Yuan, has increased his net worth by almost $16 billion *since March*, and is now one of the wealthiest individuals in America.[19]

Zoom can now use this new market penetration to increase monetization for users who currently do not pay any fees. With the pandemic-driven expansion, Zoom has announced that they're going to make a platform pivot and begin to offer an app marketplace and a paid events platform.[20] Zoom disclosed to its investors how a shift to a "platform and sales model allow[s] us to turn a single non-paying user into a full enterprise deployment."[21]

Zoom stands ready to emerge as a tech titan. But we should all be questioning whether Zoom and other tech titans expanded their empires through deception.[22] Zoom could have taken the time to ensure that its security was up to the right standards. But, in my view, Zoom saw the opportunity for massive growth by quickly leaping into the consumer market, allowing it to rapidly emerge as the new way to virtually celebrate birthdays and weddings and further solidify itself into our lives. But had Zoom followed the law, it might all be different.

Status Quo Approach to Privacy and Security Settlements

In matters like these, investigations should seek to uncover how customers were baited by any deception, how a company gained from any misconduct, and the motivations for this behavior. This approach can help shape an effective remedy. While deciding to resolve a matter through a settlement, regulators and enforcers must seek to help victims, take away gains, and fix underlying business incentives.

Of course, all settlements involve tradeoffs, but like other FTC data protection settlements, the FTC's proposed settlement with Zoom accomplishes none of these objectives. This is particularly troubling given the nature of the alleged deception. Key features of the FTC's proposed settlement include:

No help. Small businesses that purchased Zoom services or signed long-term contracts based on false representations are not even addressed in the Commission's order. They will not have the ability to be released from any contracts, seek refunds, or get credit toward future service. Similarly, Zoom's law-

---

[16] Richard Waters, *Zoom to cash in on pandemic success with apps and events*, FINANCIAL TIMES (Oct. 14, 2020), https://www.ft.com/content/f1731672-e965-48a1-9362-bab122fc9bf4.
[17] *Id*.
[18] *Id*.
[19] Taylor Nicole Rogers, *Meet Eric Yuan, the founder and CEO of Zoom, who has made over $12 billion since March and now ranks among the 400 richest people in America*, BUSINESS INSIDER (Sep. 9, 2020), https://www.businessinsider.com/meet-zoom-billionaire-eric-yuan-career-net-worth-life; Kerry A. Dolan et al., *The Forbes 400: The Definitive Ranking of the Wealthiest Americans in 2020*, FORBES (Sep. 8, 2020), https://www.forbes.com/profile/eric-yuan/?list=forbes-400&sh=474b78c761bf.
[20] *Supra* note 16.
[21] Zoom Video Communications, Inc., Quarterly Report (Form S-1) (Dec. 21, 2018), https://www.sec.gov/Archives/edgar/data/1585521/000095012318012479/filename1.htm.
[22] Decision and Order, *In the Matter of Google Inc.*, Comm'n File No. 1023136 (Oct. 24, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf; Decision and Order, *In the Matter of Facebook, Inc.*, Comm'n File No. 0923184 (July 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

abiding competitors and other consumers affected by the alleged misconduct will not get anything to address how they were harmed.

No notice. The targets of deception deserve the dignity of knowing that the product they were using did not use the security features that were advertised. Notice also provides information on whether or not users need to take any specific further actions to protect themselves or their place of business. This is especially critical in cases where individuals may not know if they are affected. In this matter, Zoom's technology was integrated into white label products that may not use Zoom's brand. Notice is also helpful when victims receive no restitution.

No money. In my view, the evidence is clear that Zoom obtained substantial benefits through its alleged conduct. However, the resolution includes no monetary relief at all, despite existing FTC authority to seek it in settlements when conduct is dishonest or fraudulent. If the FTC was concerned about its ability to seek adequate monetary relief, it could have partnered with state law enforcers, many of whom can seek civil penalties for this same conduct.

No fault. The Commission's order includes no findings of fact or liability. In other words, Zoom admits nothing and the Commission's investigation makes no significant conclusions. This will make it more difficult for affected parties to exercise any contractual rights or seek help through private actions.

Earlier this year, after a number of security concerns emerged, the Attorney General of New York quickly took action, and Zoom signed a voluntary compliance agreement, which requires certain third-party reports and compliance with additional standards.[23] The FTC's proposed settlement terms add some requirements to what Zoom has already agreed to with New York, largely involving additional independent monitoring and paperwork submissions. It is not clear to me that these new obligations are actually changing the way Zoom does business. In fact, Zoom may already be retaining third parties to assist with compliance as part of its contractual obligations with its largest customers.

Recommendations to Restore Credibility

To protect the public and promote fair markets, the FTC must be a credible law enforcement agency, especially when it comes to large players in digital markets. Our recent law enforcement actions raise questions that warrant careful attention if we aspire to be an effective enforcer. Below are some of the tangible steps the Commission should pursue:

1. Strengthen orders to emphasize more help for individual consumers and small businesses, rather than more paperwork.

When consumers and small businesses are the targets of unlawful data protection practices, the FTC's status quo approach often involves requiring the company engaged in misconduct to follow the law in the future and submit periodic paperwork. In certain orders, the Commission requires the retention of a third-party assessor, which the company might already be doing.

[23] Press Release, N.Y. Att'y Gen., Attorney General James Secures New Protections, Security Safeguards for All Zoom Users (May 7, 2020), https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users.

The FTC should focus its efforts on ensuring resolutions lead to meaningful help and assistance to affected consumers and small businesses. For example, the Commission could seek requirements that defendants respond to formal complaints and inquiries. This assists consumers while also allowing the Commission to track emerging harms and how the company is remediating them.

Another way to help affected consumers and businesses is to order releases from any long-term contractual arrangements. When customers are baited with deceptive claims, it would be appropriate to allow them to be released from any contract lock-in or otherwise amend contractual terms to make customers whole. This would also help honest competitors regain some of the market share improperly diverted by deceptive conduct.

The Commission should seek notices to affected parties, so that these individuals and businesses can determine whether they need to take any action and whether they want to continue to do business with a company that engaged in any wrongdoing.

2. Investigate firms comprehensively across the FTC's mission.

The FTC is a unique institution with legal authorities related to data protection, consumer protection, and competition, all under one roof, rather than divided up across multiple agencies. It is critical that the agency use its authority to deter unfair or deceptive conduct in conjunction with our authority to deter unfair methods of competition. The agency can do more to comprehensively use its authorities across its mission, particularly when unfair or deceptive practices can advance dominance in digital markets. When we do not, investigations may result in ineffective resolutions that fail to fix the underlying problems and may increase the likelihood of recidivism. The Commission may need to reorganize its offices and divisions to ensure investigations are comprehensive.

3. Diversify the FTC's investigative teams to increase technical rigor.

Engineers, designers, and other technical experts can offer major contributions to our investigative teams. Many of the cases previously pursued by the FTC were the result of press coverage from technical experts, especially security researchers. In fact, an independent researcher working in his private capacity was one of the first to discover a serious vulnerability in Zoom's product.[24]

Many of our peer agencies around the world approach investigations with diverse, interdisciplinary teams. Unfortunately, the Commission has deprived our litigators and enforcement attorneys of this needed expertise. The Commission should restore the role of the Chief Technologist and make a concerted effort to increase the proportion of technologists and others with technical knowledge in our investigative teams. If these individuals play meaningful leadership roles in our investigations, the agency can be much more effective.

With these technical skills and leadership in place, the Commission could proactively review the dominant digital products and services rather than primarily following up on concerning media reports after sensitive information or access has been at risk.

[24] The independent research solicited readers for contributions to assist with his work and pay off his student loans. Jonathan Leitschuh, *Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!*, INFOSEC WRITE-UPS (July 8, 2019), https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5.

4. Restate existing legal precedent into clear rules of the road and trigger monetary remedies for violations.

Markets benefit when there are simple, clear rules of the road. This allows honest businesses to know what is and is not permissible. This especially helps small businesses and startups. On the other hand, ambiguity helps large incumbents who can hire lawyers and lobbyists to sidestep their obligations. The FTC can promote fair markets by restating accepted legal precedent and past Commission experience through an agency rulemaking. These would create no new substantive obligations on market participants. But once restated and enforced, violations trigger significant monetary relief.

Under the FTC Act, the Commission has a number of authorities to seek monetary relief. While one of these authorities, Section 13(b), is under considerable scrutiny in the courts, the Commission can also seek money by restating existing legal precedent through a rulemaking. When the Commission has issued prior orders for past misconduct in the market or there is other information indicating a widespread pattern of unfair or deceptive conduct, Section 18 of the FTC Act authorizes the Commission to define what constitutes an unfair or deceptive practice by rule. Violations of these rules can trigger liability for redress, damages, penalties, and more.

Over the years, the Commission has finalized a substantial number of orders related to data protection, including privacy and data security. There have also been developments in case law in the courts. The Commission should consider restating this past precedent into a rule under Section 18 or other appropriate statutes to provide clear guidance and systematically deter unlawful data protection practices.[25]

5. Demonstrate greater willingness to pursue administrative and federal court litigation.

Congress intended for the FTC to serve as an expert agency that analyzes emerging business practices and determines whether they might be unfair or deceptive. Administrative litigation and final Commission orders can provide important guidance to the marketplace on the agency's analytical approach. It can also serve as the basis for triggering financial liability for other market actors, pursuant to the Commission's Penalty Offense Authority.[26]

Federal court litigation pursued by our staff has contributed to strong outcomes and important development of the law. For example, in 2012, the FTC took action against Wyndham Hotels, a major hospitality chain the Commission charged with employing unfair data practices. Wyndham Hotels waged an aggressive defense, challenging the FTC's theories before the District Court and the Third Circuit Court of Appeals. The court's ruling cemented the Commission's ability to target lax data security practices under existing law.

The public benefits from the work of the FTC's talented investigators and litigators across the agency, and as Commissioners, we should have confidence that they can hold accountable even the largest players in the economy. But recently, when it comes to data protection, FTC Commissioners

[25] Statement of Commissioner Rohit Chopra Regarding the Report to Congress on Protecting Older Consumers, Comm'n File No. P144400 (Oct. 19, 2020), https://www.ftc.gov/system/files/documents/public_statements/1581862/p144400choprastatementolderamericansrpt.pdf.
[26] *See* Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority* (Oct. 29, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721256.

have rarely voted to authorize agency staff to sue national players for misconduct. We must do more to safeguard against any perception about the agency's unwillingness to litigate.

6. Increase cooperation with international, federal, and state partners.

When it comes to data protection abuses and other harmful practices by large technology firms, these concerns are increasingly global. The FTC can use its resources more effectively and obtain superior outcomes when it cooperates with other law enforcement partners.

In the Ashley Madison matter, the FTC partnered with the Office of the Privacy Commissioner of Canada, Office of the Australian Information Commissioner, and many state attorneys general. This action was the result of significant cooperation and ultimately led to a joint resolution.[27] Unfortunately, this is too rare.

The FTC can rely on key provisions of the U.S. SAFE WEB Act that allow the FTC to share information with foreign counterparts to combat deceptive or unfair practices that cross national borders. Domestically, agencies can form multistate working groups to combine resources and leverage a diverse set of legal authorities.

In the matter before the Commission today, the conduct at issue might have also violated state laws. Additional liability triggered by these laws could have led to a resolution with a far superior outcome. Instead, other law enforcement agencies both at home and abroad will likely need to continue to scrutinize Zoom's practices, given the FTC's proposed resolution.

In addition, the Commission needs to rethink its approach to enforcing privacy promises by large technology firms related to their participation in international agreements, such as the EU-U.S. Privacy Shield Framework. Zoom's conduct may have violated key aspects of the framework, and I believe the Commission should have taken action accordingly. The Commission should now fully cooperate with our international partners to ensure that they can proceed with appropriate sanctions.

7. Determine whether third-party assessments are effective.

A common provision in FTC orders requires the defendant to retain a third party to monitor compliance and the company's data protection protocols. However, it is unclear whether those assessments are truly effective when it comes to deterring or uncovering misconduct. For example, in the FTC's investigation of Facebook for compliance with its privacy obligations under a 2012 Commission order, the FTC alleged major violations of the order even though an independent third party, PriceWaterhouseCoopers (PwC), was supposedly watching over the company's compliance.[28]

[27] Press Release, Fed. Trade Comm'n, Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting.

[28] *See* Nitasha Tiku, *Facebook's 2017 Privacy Audit Didn't Catch Cambridge Analytica*, WIRED (Apr. 19, 2018), https://www.wired.com/story/facebooks-2017-privacy-audit-didnt-catch-cambridge-analytica/; S*ee also* Dissenting Statement of Commissioner Rohit Chopra In re Facebook, Inc., Comm'n File No. 1823109 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

Additionally, the Commission's decision to not proactively make certain information about these third party reports public limits our ability to determine their effectiveness.[29] If independent researchers and journalists – often the ones who originally discovered data protection failures in the first place – had access to these reports, companies and third-party monitors might take them more seriously, which would help to fulfill the intended purpose of their efforts.

Conclusion

This year families have said their final goodbyes to loved ones over Zoom.[30] Desperate parents have propped their children in front of screens for school and hoped that they won't fall too far behind.[31] Small businesses have been turned upside down by our new way of life and have fought for a chance at survival by switching to doing business virtually.[32] But when tech companies cheat, rather than compete, and then face no meaningful accountability, all of us suffer.

I am concerned that Zoom simply thought that the FTC's law enforcement inquiry wasn't serious. That's probably why the company didn't even bother to disclose the agency's inquiry to its investors.[33] The company seemed to guess that the FTC wouldn't do anything to materially impact their business. Sadly, for the public, they guessed right. Given the company's approach, efforts to hold Zoom accountable by regulators and enforcers in the U.S. and abroad will clearly need to continue.

Finally, the Federal Trade Commission has requested greater authority from Congress to protect Americans from abuse and misuse of personal data. But, actions like today's proposed settlement undermine these efforts. The agency must demonstrate that it is willing to use all of its existing tools to protect consumers and the market. Only then will the Commission be entrusted to take on more responsibilities.

It is critical that we restore the agency's credibility deficit when it comes to oversight of the digital economy. This does not stem from a lack of authority or resources or capabilities from our staff – it stems from the policy and enforcement approach of the Commission, and this needs to change.

For these reasons, I respectfully dissent.

---

[29] Statement of Commissioner Rohit Chopra In the Matter of Uber Technologies, Inc., Comm'n File No. 1523054 (Oct. 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1418195/152_3054_c-4662_uber_technologies_chopra_statement.pdf.

[30] Sarah Zhang, *The Pandemic Broke End-of-Life Care*, THE ATLANTIC (June 16, 2020), https://www.theatlantic.com/health/archive/2020/06/palliative-care-covid-19-icu/613072/.

[31] Heather Kelly, *Kids used to love screen time. Then schools made Zoom mandatory all day long.*, WASH. POST (Sep. 4, 2020), https://www.washingtonpost.com/technology/2020/09/04/screentime-school-distance/.

[32] Justin Lahart, *Covid Is Crushing Small Businesses. That's Bad News for American Innovation.*, WALL STREET J. https://www.wsj.com/articles/covid-is-crushing-small-businesses-thats-bad-news-for-american-innovation-11602235804.

[33] Zoom Video Communications, Inc., July 2020 Quarterly Report (Form 10-Q) (Sep. 3, 2020), https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552120000238/zm-20200731.htm. When publicly traded firms do not disclose to their investors that they are facing a federal law enforcement inquiry, this suggests that they do not believe the inquiry is material to their financial or operational performance.