COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, CENTER FOR DIGITAL DEMOCRACY, CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD, THE PARENT COALITION FOR STUDENT PRIVACY, and CONSUMER FEDERATION OF AMERICA

to the

FEDERAL TRADE COMMISSION

In the Matter of Zoom Video Communications, Inc.

FTC File No. 192 3167

December 14, 2020

By notice published on November 13, 2020, the Federal Trade Commission ("FTC") has proposed a Consent Order with Zoom Video Communications, Inc. ("Zoom") that would settle alleged violations of federal law.[1] The FTC's Agreement Containing Consent Order ("Consent Order")[2] follows the FTC's Complaint ("Complaint"), which alleges that Zoom violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).[3] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC"), the Center for Digital Democracy ("CDD"), the Campaign for a Commercial-Free Childhood ("CCFC"), the Parent Coalition for Student Privacy, and Consumer Federation of America ("CFA") (collectively, "Consumer Privacy Organizations.") submit these

[1] FTC, *Zoom Video Communications, Inc.; Analysis to Aid Public Comment*, 85 FR 72650 (Nov. 13, 2020), https://www.federalregister.gov/documents/2020/11/13/2020-25130/zoom-video-communications-inc-analysis-to-aid-public-comment.
[2] *In the Matter of Zoom Video Communications, Inc.*, (Agreement Containing Consent Order), FTC File No. 192 3167 (Nov. 9, 2020), https://www.ftc.gov/system/files/documents/cases/1923167zoomacco2.pdf [hereinafter "Order"].
[3] *In the Matter of Zoom Video Communications, Inc.*, (Complaint), FTC File No. 192 3167, (Nov. 9, 2020) https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf [hereinafter "FTC Zoom Complaint"].

comments to recommend specific changes to the proposed Consent Order to safeguard the privacy interests of Zoom users.

Last year, EPIC filed a detailed complaint with the FTC about the security flaws with Zoom.[4] EPIC warned the Commission that Zoom had "placed at risk the privacy and security of the users of its services."[5] EPIC also explained that Zoom had "exposed users to the risk of remote surveillance, unwanted videocalls, and denial-of-service attacks."[6] And this was almost a year before the COVID-19 pandemic forced hundreds of millions of Americans onto Zoom for their essential activities including work, school, telehealth appointments, and family gatherings.

The comments of Consumer Privacy Organizations are divided into four sections. Section I sets out the FTC's legal obligations in considering these comments before finalizing the proposed Consent Order. Section II summarizes the FTC Complaint and Consent Order. Section III lays out proposed modifications to the Consent Order and expresses support for Commissioner Rebecca Kelly Slaughter's dissent. Section IV expresses support for the recommendations made by Commissioner Rohit Chopra in his dissent in order to strengthen FTC enforcement efforts.

In short, Consumer Privacy Organizations recommend that the FTC modify the proposed Consent Order and require Zoom to (1) implement a comprehensive privacy program; (2) obtain regular independent privacy assessments and make those assessments available to the public; (3) provide meaningful redress for victims of Zoom's unfair and deceptive trade practices; and (4) ensure the adequate protection and limits on the collection of children's data.

---

[4] EPIC, *Complaint, Request for Investigation, Injunction, and Other Relief* (July 11, 2019), https://epic.org/privacy/zoom/EPIC-FTC-Complaint-In-re-Zoom-7-19.pdf [hereinafter "EPIC Zoom Complaint"]; *See also* EPIC, *In re Zoom: Concerning Zoom's ability to bypass browser security settings and remotely enable a user's web camera without the knowledge or consent of the user,* https://epic.org/privacy/ftc/zoom/.

[5] *Id.* at 1.

[6] *Id.*

I. The FTC Has a Legal Obligation to Consider Public Comments Prior to Finalizing Any Consent Order.

The Administrative Procedure Act requires that the FTC take public comments before finalizing any Consent Order and gives the Commission authority to modify an agreement based on received comments.[7] Consumer Privacy Organizations have previously submitted many comments to the Commission on preliminary consent orders in cases that implicate the privacy interests of consumers.[8] We have set out recommendations that would have established stronger data protection safeguards for consumers, consistent with the purposes of the settlements. In these comments, Consumer Privacy Organizations offer several recommendations that would strengthen protections for Zoom users. We expect that the Commission will provide a "reasoned response."[8] to our comments and modify the Consent Order as appropriate.

II. Zoom's Deceptive Trade Practices Threatened the Privacy and Security of Millions of Americans.

The FTC Complaint details numerous, significant failure's in Zoom's development and maintenance of its video conferencing software that exposed users to potential malicious software execution, privacy invasions, and loss of control of their sensitive data.[9] Ultimately, Zoom's business practices did not live up to their promises. They did not provide secure video communications services and they did not protect the privacy of their users. Instead, they lured small businesses and other users in for lucrative subscription contracts with promises of security that they never delivered. Specifically, Zoom made false and misleading statements since at least June 2016 regarding the company's offering of end-to-end encryption for Zoom meetings; the company did not actually

[7] Commission Rules of Practice, 16 C.F.R. § 2.34.
[8] *See Interstate Nat'l Gas Ass'n of Am. v. F.E.R.C.*, 494 F.3d 1092, (D.C.C. 2007); *see e.g.,* Response of FTC Secretary Donald S. Clark to EPIC, *In the Matter of Google, Inc.*, File No. 102 3136, Docket No. C-4336 (Oct. 13, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzepic.pdf.
[9] *In the Matter of Zoom Video Communications, Inc.*, (Complaint), FTC File No. 192 3167, (Nov. 9, 2020) https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf [hereinafter "Complaint"].

provide end-to-end encrypted communications until this year.[10] Zoom also made deceptive claims regarding the security of recorded meetings.[11] And, as detailed in EPIC's July 2019 complaint to the FTC, Zoom intentionally designed their web conferencing service to bypass browser security settings and remotely enable a user's web camera without the consent of the user.[12] As a result, Zoom exposed users to the risk of remote surveillance, unwanted videocalls, denial-of-service attacks, and other potentially malicious code execution.[13] Zoom did not fix these vulnerabilities until they were publicly exposed (several months after they were brought to the company's attention).[14]

These are not isolated incidents. There have been myriad reported problems with Zoom's security and privacy practices this year, including:

- Vice reported that "iOS version of the Zoom app is sending some analytics data to Facebook, even if Zoom users don't have a Facebook account."[15]
- Vice also reported that "Zoom is leaking personal information of at least thousands of users, including their email address and photo, and giving strangers the ability to attempt to start a video call with them through Zoom."[16]
- The *New York Times* reported "data-mining feature on Zoom allowed some participants to surreptitiously have access to LinkedIn profile data about other users — without Zoom asking for their permission during the meeting or even notifying them that someone else was snooping on them." This included the full names and e-mail addresses of students.[17]
- The *Washington Post* reported "Thousands of personal Zoom videos have been left viewable on the open Web, highlighting the privacy risks to millions of Americans as

[10] FTC Zoom Complaint, *supra*, at ¶¶ 15–30.
[11] *Id.* at ¶¶ 31–33.
[12] *Id.* at ¶¶ 34–53; EPIC Zoom Complaint, *supra* note 6 at 6–11.
[13] *Id.*
[14] EPIC Zoom Complaint, *supra*, at 11.
[15] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account* (Mar. 26, 2020), https://www.vice.com/en/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.
[16] Joseph Cox, *Zoom is Leaking Peoples' Email Addresses and Photos to Strangers,* Vice (Apr. 1, 2020), https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos.
[17] 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.

they shift many of their personal interactions to video calls in an age of social distancing."[18]

- CitizenLab reported that "the mainline Zoom app appears to be developed by three companies in China." There is a long and unfortunate history of US tech firms diminishing privacy safeguards in response to the Chinese government.[19]

- School districts nationwide, including New York City Public Schools, banned the use of Zoom in the spring over data security concerns.[20]

As EPIC's Complaint and the FTC's Complaint make clear, Zoom's unlawful business practices created substantial privacy and security risks for consumers and gave the company an unfair advantage at a time when millions of companies, institutions, and individual users were forced to communicate and interact with their teachers, coworkers, friends, family, and others through videoconferencing services. In response to these violations, the FTC filed its Complaint against Zoom and has entered into a proposed Consent Order that focuses primarily on Zoom's internal security controls.

The Commission's Consent Order imposes the following requirements:

- Zoom is prohibited from making misrepresentations about its privacy and security practices, including about how it collects, uses, maintains, or discloses personal information; its security features; and the extent to which users can control the privacy or security of their personal information;

- Zoom is required to implement and maintain a comprehensive information security program;

- Zoom must obtain biennial assessments of its security program by an independent third

[18] Drew Harwell, *Thousands of Zoom Video Calls Left Exposed on Open Web,* Wash. Post (Apr. 3, 2020) ("Many of the videos include personally identifiable information and deeply intimate conversations, recorded in people's homes."), https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

[19] Bill Marczak and John Scott-Railton, *Move Fast & Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings,* CitizenLab (Apr. 3, 2020), https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/; *See also* Schneier on Security, *Security and Privacy Implications of Zoom* (Apr. 3, 2020) ("In general, Zoom's problems fall into three broad buckets: (1) bad privacy practices, (2) bad security practices, and (3) bad user configurations."), https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html

[20] Valerie Strauss, *School districts, including New York City's, start banning Zoom because of online security issues*, Wash. Post (Apr. 4, 2020), https://www.washingtonpost.com/education/2020/04/04/school-districts-including-new-york-citys-start-banning-zoom-because-online-security-issues/.

party, which must be submitted to the FTC;

- Zoom officials must annually certify that the company is complying with the Consent Order; and
- Zoom must notify the FTC of covered incidents such as data breaches.

III. The Consent Order Should Be Modified to Ensure That Zoom Protects the Privacy of Its Users.

As Commissioner Slaughter makes clear in her dissenting opinion, the FTC's proposed Consent Order with Zoom does not adequately address or remedy Zoom's failure to protect the privacy of its users. The FTC Complaint fails to even mention the word "privacy."[21] Instead, the Commission focuses solely on data security practices and provides only limited remedies for those violations.[22] It is clear from the FTC Complaint that Zoom engaged in unfair and deceptive trade practices with respect to its handling of user data, including private and sensitive communications. Therefore, the Commission should include new privacy safeguard requirements in its Consent Order with Zoom. A failure to do so now would only create the opportunity for Zoom to avoid monetary penalties in the future if it fails to protect users' privacy. That is simply unacceptable.

Recommendation 1: The FTC should amend their proposed order to require Zoom to implement a comprehensive privacy program based on the Code of Fair Information Practices, OECD Privacy Guidelines, or NIST Privacy Framework.

The FTC has previously required many companies that have committed similar violations to implement a comprehensive privacy program.[23] That should be a bare minimum requirement for all FTC Consent Orders involving privacy and data security violations, and the Commission should

[21] Dissenting Statement of Comm'r Rebecca Kelly Slaughter, *In the Matter of Zoom Video Communications, Inc.*, FTC File No. 192 3167 (Nov. 9, 2020).
[22] *Id.*
[23] Decision and Order, *In re: Uber Technologies, Inc.*, FTC No. 1523054 (Oct. 25, 2018); Decision and Order, *In the Matter of PayPal, Inc.,* FTC, File No. 162-3102 (March 5, 2018); Decision and Order, *In the Matter of Facebook, Inc.,* FTC, File No. 092 3184 (Aug. 10, 2012); Decision and Order, *In the Matter of Myspace LLC.,* FTC, File No. 102 3058 (May 8, 2012); Decision and Order, *In the Matter of Google, Inc.,* FTC, File No. 102 3136 (Oct. 24, 2011).

have required the same of Zoom. As Commissioner Slaughter noted:

> 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.[24]

The Commission should also take this opportunity to strengthen its comprehensive privacy program requirements. As a starting point, Consumer Privacy Organizations recommend that the FTC require Zoom to adopt and implement a familiar privacy framework, such as the original U.S. Code of Fair Information Practices ("FIPs"), the OECD Privacy Guidelines, or NIST Privacy Framework. These frameworks create obligations for companies that collect personal data and rights for individuals. Core principles include:

- Transparency about business practices
- Data collection and use limitations
- Data minimization and deletion
- Purpose specification
- Access and correction rights
- Accountability
- Data accuracy
- Confidentiality/security

The FTC should require Zoom to comply with these principles for all uses of personal data and compliance should be ensured through independent audits, public reporting, and routine inspection by the FTC.

As Commissioner Slaughter noted, the Commission must ensure that its orders address not only security, but also privacy.[25] A failure to do so is a failure to understand how consumers understand data security as being inextricably intertwined with privacy and would be a dereliction of the FTC's duties to protect consumers.[26]

Recommendation 2: The FTC should amend their proposed order to require Zoom to obtain biennial privacy assessments from a qualified, objective, independent third-party professional, and make those assessments available to the public.

The FTC now routinely requires that companies under consent order for privacy violations be

[24] Dissenting Statement of Comm'r Slaughter, *supra*, 3.
[25] Dissenting Statement of Comm'r Slaughter, *supra*.
[26] *Id.*

subject to periodic privacy assessments as a condition of their Consent Order.[27] The same should be true for Zoom. But, unlike in earlier cases, the FTC should not allow Zoom to keep those assessments secret. The FTC should modify the order to require Zoom to obtain biennial privacy assessments from a qualified, objective, independent third-party professional. The FTC should require that the assessments include impact assessments and compliance metrics so that policy changes can be tracked over time. And the assessments should be made public so they can be closely scrutinized.

It is crucial that the public can access these assessments both as an added incentive for Zoom to comply and to further the goals of transparency and open government. Privacy program assessments are meaningless without vigorous enforcement by the FTC and other public and privacy oversight bodies.[28] As the Facebook case has shown, third party assessments can and have failed to identify critical failures when they are not subject to public oversight.[29]

In the past, the Commission has represented that privacy assessments would be available to the public, subject to applicable laws.[30] Releasing the privacy assessments to the public is necessary so that consumer organizations can ensure that the FTC is doing its job and that user privacy is protected. Public release is also necessary to allow the public to determine whether they can safely and securely continue to use Zoom's services, and to restore public trust in the company.

---

[27] *See e.g.* Fed. Trade Comm'n., *In the Matter of Uber Technologies, Inc.*, Decision and Order, FTC File No. 1523054 (Oct. 26, 2018) https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_agreement.pdf; Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Aug. 10, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[28] Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Opposition to the Motion to Approve Consent Judgment at 17, *United States v. Facebook Inc.*, 456 F.Supp.3d 105 (D.D.C. 2020).

[29] *Id.*

[30] Letter from Federal Trade Comm'n, Office of Secretary, to EPIC (Oct. 13, 2011), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzepic.pdf.

Recommendation 3: The FTC should modify the proposed Order to provide redress to Zoom's affected customers.

The FTC Complaint details egregious misrepresentations by Zoom of its security and privacy practices.[31] It also notes that of Zoom's approximately 600,000 paying customers in July 2019, 88% were small businesses.[32] Yet the FTC's proposed Order contains no redress, no refunds, no requirement that Zoom must notify its customers about the company's misleading statements.

The FTC should modify the proposed Order to give relief to Zoom's paying customers who were led to believe that their videoconferences and recordings were encrypted and their private recordings secured. This would not be unprecedented – in 2014, the Commission required Google to provide full refunds (with a minimum payment of $19 million) to consumers who were charged for children's unauthorized in-app purchases.[33] The FTC reached a similar settlement with Apple[34] and sued Amazon[35] to require refunds be provided to parents for children's unauthorized purchases. The Commission can now do the same for Zoom customers who were duped into paying for a secure encrypted videoconferencing service that they never received.

The FTC should provide this relief for two reasons: 1) customers deserve redress when they were intentionally mislead about the security of a product and 2) the Commission must disgorge the company's unlawfully earned profits as a deterrent effect to prevent such conduct in the future.

The FTC should also require Zoom to delete any data the company impermissibly collected, especially from children and teens.

---

[31] FTC Zoom Complaint, *supra* note 3.
[32] *Id.* at ¶ 9.
[33] Decision and Order, *In the Matter of Google Inc.*, Docket No. C-4499 (Dec. 5, 2014).
[34] Agreement Containing Consent Order, *In the Matter of Apple Inc.*, (Jan. 15, 2014).
[35] Press Release, Fed. Trade Comm'n: *Federal Court Finds Amazon Liable for Billing Parents for Children's Unauthorized In-App Charges* (Apr. 27, 2016), https://www.ftc.gov/news-events/press-releases/2016/04/federal-court-finds-amazon-liable-billing-parents-childrens.

Recommendation 4: The FTC should modify the proposed Order to ensure adequate protection and limits on the collection of children's data

In light of Zoom's usage for online learning, it is crucial that the FTC modify the proposed Order to ensure the adequate protection of and limits on the collection of the data of children and teens. The FTC must ensure that Zoom is compliant with both the Children's Online Privacy Protection Act (COPPA) and the Federal Educational Rights and Privacy Act (FERPA). Additionally, the FTC should require that Zoom:

- Do not use marketing or non-functional cookies or tracking technologies for children and teens;
- Do not monetize or sell children's data and do not use children's data for targeted or non-targeted advertising;
- Provide an accounting of third parties who have access to children's data and for what purpose;
- Delete and destroy children's data upon a verified request from a parent.

Colorado has a state law that requires contracted school service providers to be transparent about the data elements they collect, how data is used, and to list every third-party who has access to the data.[36] The Parent Coalition for Student Privacy has reported that Zoom has refused to comply with the law, arguing that Zoom is not a "school service."[37] The Colorado State Board of Education has asked the Colorado Attorney General to "review Zoom's compliance with state and federal privacy laws."[38] That review is pending. But the FTC, by modifying its proposed Zoom Order to require the above, has an opportunity to provide clarity on Zoom's security and privacy protections to school districts nationwide. It is crucial that school districts and parents can assess Zoom's business model with regard to the collection, use, and disclosure of student data.

[36] 2016 Colo. Sess. Laws 1457.
[37] Parent Coalition for Student Privacy, What You Need to Know About Zoom for Education (Aug. 11, 2020), https://www.studentprivacymatters.org/tag/zoom-colorado/.
[38] Press Release, Colo. Dept. of Ed., *State Board of Education approves statewide waivers* (May 13, 2020), https://www.cde.state.co.us/communications/20200513sbemeeting.

IV. The FTC Needs to Take Bolder and Swifter Action to Ensure Privacy Protections Going Forward, and Should Seek More Substantial Remedies.

Consumer Privacy Organizations agree with Commissioner Chopra that the FTC's approach to oversight of the digital economy has left the commission with a "credibility deficit."[39] Our groups have long argued that the FTC has not done enough to address the growing threats to consumer privacy.[40] And the proposed Consent Order with Zoom is just one more example of how the FTC's old strategy does not serve the interests of consumers and does not deter unlawful business practices.

Consumer Privacy Organizations support Commissioner Chopra's calls for the FTC to: (1) strengthen orders to emphasize more help for individual consumers and small businesses, rather than more paperwork; (2) investigate firms comprehensively across the FTC's mission; (3) diversify the FTC's investigative teams to increase technical rigor; (4) restate existing legal precedent into clear rules of the road and trigger monetary remedies for violations; (5) demonstrate greater willingness to pursue administrative and federal court litigation; (6) increase cooperation with international, federal, and state partners; (7) determine whether third-party assessments are effective.

The FTC plays an important role in safeguarding consumers from fraud and reviewing potentially anticompetitive business practices, but the Commission is an effective data protection agency. Over the last twenty years, the FTC has attempted to address privacy violations primarily through its Section 5 deceptive trade practices authority without establishing clear data protection rules or broad remedial authority. The result has been a quasi-self-regulatory approach that embraces a notice and choice theory of privacy regulation—companies are not punished unless they explicitly

[39] Dissenting Statement of Comm'r Rebecca Kelly Slaughter, *In the Matter of Zoom Video Communications, Inc.*, FTC File No. 192 3167 (Nov. 9, 2020).
[40] *See e.g.* Letter from Center for Digital Democracy and Campaign for a Commercial-Free Childhood to Fed. Trade Comm'n (July 3, 2019), https://www.democraticmedia.org/sites/default/files/field/public-files/2019/ftc_letter_july_3_2019_final.pdf; *Oversight of the Federal Trade Comm'n,* S. Comm. on the Commerce, Sci., and Trans. (Aug. 4, 2020) (Statement of EPIC) https://epic.org/testimony/congress/EPIC-SCOM-FTCOversight-Aug2020.pdf.

lie about their privacy practices, and even then they are not fined unless they deceive their users a second (or third) time. American consumers are left with a sense that companies are free from consequence when they collect, disclose, mishandle, or outright abuse their access to user data. Meanwhile consumers suffer from some of the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber-attack by criminals and foreign adversaries. U.S. companies continue to collect vast amounts of personal data about American's without their knowledge and without any meaningful data protection standards. The Cambridge Analytica case is just one example of how that vulnerability threatens not only U.S. citizens, but also our democratic institutions. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security. The FTC should follow Commissioner Chopra's recommendations if the agency wants to demonstrate that it is up to the task of protecting American consumers.

V. Conclusion

EPIC, CDD, CCFC, the Parent Coalition for Student Privacy, and CFA support the Order set out by the FTC regarding Zoom's past practices of issuing false and misleading statements on its security practices. But the Commission's failure to address the privacy concerns arising from Zoom's business practices in this settlement is unacceptable. These comments detail how the proposed Order with Zoom can be strengthened to help protect the privacy of American consumers. Specifically, Consumer Privacy Organizations urge the Commission to require Zoom to (1) implement a comprehensive privacy program; (2) obtain regular independent privacy assessments, which must be made publicly accessible; (3) provide meaningful redress for victims of unfair and deceptive trade practices; and (4) ensure the adequate protection and limits on the collection of children's data.

We remind the FTC that the Commission is required by statute to meaningfully consider comments submitted by the public before finalizing consent orders. Most importantly, it is the responsibility of the FTC to protect consumer privacy and to prosecute companies that engage in unfair and deceptive trade practices.

Respectfully submitted,

Electronic Privacy Information Center
Center for Digital Democracy
Campaign for a Commercial-Free Childhood
Parent Coalition for Student Privacy
Consumer Federation of America