Before the
Federal Trade Commission
Washington, DC

In the Matter of	)
	)
Zoom Video Communications, Inc.	)
	)
___________________________________	)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center

I. Introduction

1. This complaint concerns business practices by Zoom Video Communications, Inc. ("Zoom") that placed at risk the privacy and security of the users of its services. As set forth below, 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. As a result, Zoom exposed users to the risk of remote surveillance, unwanted videocalls, and denial-of-service attacks. When informed of the vulnerabilities Zoom did not act until the risks were made public, several months after the matter was brought to the company's attention.

2. Zoom exposed its users to a wide range of harms, many of which are ongoing. These business practices amount to unfair and deceptive practices under Section 5 of the FTC Act, subject to investigation and injunction by the Federal Trade Commission.

3. The Federal Trade Commission should pursue an investigation, enjoin Zoom and other companies that engage in similar practices from such unlawful activities, and provide other remedies as set out in this complaint.

II. Parties

4. The Electronic Privacy Information Center ("EPIC") is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy and has played a leading role in developing the authority of the FTC to safeguard the privacy rights of consumers. [1] EPIC's complaint concerning

[1] See, e.g., Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief),

Google Buzz provided the basis for the Commission's investigation and subsequent settlement concerning the social networking service.[2] Following EPIC's complaint, the FTC successfully petitioned a federal court for a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology allowing individuals to spy on other individuals.[3] In 2008 EPIC filed a consumer complaint with the Commission, alleging that AskEraser falsely represented that search queries would be deleted when in fact they were retained by the company and made available to law enforcement agencies.[4] EPIC also filed a complaint with the Commission alleging that Google's "Store Sales Measurement" consumer profiling technique recorded and stored the majority of consumer credit card purchases in the United States without a meaningful opt-out provision.[5]

5. Zoom Video Communications, Inc. was founded in 2011 and is based in San Jose, California. Zoom's headquarters are located at 55 Almaden Boulevard, 6th Floor, San Jose, CA 95113. At all times material to this complaint, Zoom's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

6. Zoom is one of the largest service-providers in the video conferencing industry, which is expected to grow to $20 billion by 2024.[6] Zoom is used by over 30,000 companies and over 40 million people worldwide.[7]

---

http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief), http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[2] Press Release, *Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network* (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched."). The Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]." The Google Buzz settlement also provided the basis for the subsequent $22.5 m fine for evading security settings. Press Release, Federal Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[3] FTC v. CyberSpy Software, LLC, No. 6:08-cv-1872-Orl-31GJK, 2009 WL 2386137 (M.D. Fla. July 31, 2009) (Order), http://www.ftc.gov/sites/default/files/documents/cases/2010/06/100602cyberspystip.pdf.

[4] EPIC: Does AskEraser Really Erase?, https://epic.org/privacy/ask/.

[5] Davleiid Jones, *EPIC Claims Google Violates Consumer Privacy in FTC Complaint*, TechNewsWorld (Aug. 1, 2017) https://www.technewsworld.com/story/84716.html.

[6] Enlyft, *Companies Using Zoom* (2019), https://enlyft.com/tech/products/zoom.; Peter Cohan, *Can Cisco Respond to Zoom's Challenge in $20B Videoconferencing Market?* Forbes (Mar. 8, 2019), https://www.forbes.com/sites/petercohan/2019/03/08/can-cisco-respond-to-zooms-challenge-in-20b-videoconferencing-market/.

[7] Bailey Lipschultz, *Zoom Video Falls as Mac Webcam Flaw Report Weighs on Shares*, Bloomberg.com (Jul. 9, 2019), https://www.bloomberg.com/news/articles/2019-07-09/zoom-video-falls-as-mac-webcam-flaw-report-drags-red-hot-stock; Marketwired, *Zoom Raises $30M in Series C Funding Led by Emergence Capital*, Globe Newswire (Feb. 4, 2015), https://www.globenewswire.com/news-release/2015/02/04/1130354/0/en/Zoom-Raises-30M-in-Series-C-Funding-Led-by-Emergence-Capital.html.

III. The Importance of Privacy Protection

7. The right of privacy is a personal and fundamental right in the United States.[8] The privacy of an individual is directly implicated by the collection, use, and leaking of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.[9]

8. As the Supreme Court has made clear, "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."[10] The presence of positive law to protect privacy reflects the value of privacy in the American tradition.[11]

9. The Organization for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."[12]

10. The Madrid Privacy Declaration of November 2009 affirms that privacy is a basic human right, notes that "corporations are acquiring vast amounts of personal data without independent oversight," and highlights the critical role played by "Fair Information Practices that place obligations on those who collect and process personal information and gives rights to those whose personal information is collected."[13]

11. Federal legislation has long recognized the importance of communications privacy by implementing restrictions on surveillance of citizens.

12. Since 1968, Title III of the Omnibus Crime Control and Safe Streets Act has acknowledged the necessity to "protect effectively the privacy of wire and oral communications." [14] The Electronic Communications Privacy Act added wireless and

[8] *See Obergefell v. Hodges*, 135 S. Ct. 2584, 2599 (2015) (citing *Zablocki v. Redhail*, 434 U.S. 374, 396 (1978)); Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 763 (1989) ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person"); *Whalen v. Roe*, 429 U.S. 589, 605 (1977); *United States v. Katz*, 389 U.S. 347 (1967); *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[9] Privacy Act of 1974, Pub. L. No. 93-579 § 2, 88 Stat. 1896.

[10] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) (cited by *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)).

[11] *Carpenter v. United States*, 138 S. Ct. 2206, 2270 ("positive law may help provide detailed guidance on evolving technologies without resorting to judicial intuition") (Gorsuch, J., dissenting).

[12] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD (2013).

[13] The Madrid Privacy Declaration: Global Privacy Standards for a Global World, Nov. 3, 2009, http://thepublicvoice.org/madrid-declaration/.

[14] Omnibus Crime Control and Safe Streets Act, 90 P.L. 90-351 § 801, 82 Stat. 197 (1968).

data communications to this legislation, recognizing the privacy interests inherent in internet communications such as teleconferencing.[15]

13. The common-law tort of intrusion upon seclusion recognizes the invasion of privacy that results from unwanted observation.[16]

14. An overwhelming majority of consumers are offended by the prospect of being watched without their permission.[17] Most internet users have taken affirmative steps to avoid observation online.[18]

15. The Federal Trade Commission has routinely investigated companies for violations of privacy when the company has engaged in "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[19]

IV. Factual Background

A. Zoom's Product Design Exposes Users to Foreseeable Harm

16. Zoom states that its service provides "simplified video conferencing and messaging across any device."[20] Zoom further claims that it is "easy to start, join, and collaborate across any device."[21]

17. Over 30,000 companies currently use Zoom for video conferencing and online meetings.[22] According to the company's S–1, Zoom has "thousands of customers of all sizes."[23] The company made $330.5 million in revenue in 2019 and continues to grow.[24]

18. Hospitals, universities, and nonprofits, among others, use Zoom's service.[25] Many companies rely on Zoom's software.

[15] Electronic Communication Privacy Act of 1986, 99 P.L. 508, 100 Stat. 1848.

[16] *See, e.g.*, Restatement (Second) of Torts § 652B (Am. Law Inst. 1977) (the "intrusion itself" makes the defendant liable). *See also Peterson v. Aaron's, Inc.*, 108 F. Supp. 3d 1352 (N. D. Ga. 2015) (plaintiffs prevailed in their intrusion upon seclusion claim against a company that used software to access and monitor their computers without permission).

[17] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, Pew Research Center (May 20, 2015) ("88% [of adults] say it is important that they not have someone watch or listen to them without their permission").

[18] Lee Rainie, et al., *Anonymity, Privacy, and Security Online*, Pew Research Center (Sept. 5, 2013).

[19] 15 U.S.C. § 45 (2006).

[20] Zoom, *Zoom Meetings & Chat* (2019), https://zoom.us/meetings.

[21] *Id.*

[22] Enlyft, *Companies Using Zoom* (2019), https://enlyft.com/tech/products/zoom.

[23] Zoom Video Commc'n, Inc., Registration Statement (Form S–1), at 2 (Mar. 22, 2019), https://www.sec.gov/Archives/edgar/data/1585521/000119312519083351/d642624ds1.htm.

[24] *Id.*

[25] Zoom, *Case Studies* (2019), https://zoom.us/customer/all.

19. According to Zoom, several government agencies, including the Centers for Disease Control and Prevention, the US Department of Homeland Security, the US Department of Energy, as well as several state agencies also use Zoom.[26]

20. Switching to a different video conferencing service, upon learning of faulty security practices, would be costly and difficult for users.

21. Zoom contends that the company is "committed to protecting your privacy and ensuring you have a positive experience on our website."[27] Zoom does not reveal in either its privacy policy or its terms of service that it installs local web servers on its users' devices.[28] Zoom last updated its privacy policy on March 19, 2019 and its terms of service are effective as of May 20, 2019.[29]

B. Zoom Has Previously Jeopardized Users' Privacy

22. In July 2018, Zoom reported to the SEC that the Zoom client for Windows "could result in potential exposure of a Zoom user's password."[30]

23. In October 2018, Tenable, a cyber exposure company, discovered a flaw in Zoom that allowed attendees and remote attackers "to hijack control of presenters' desktops, spoof chat messages, and kick attendees out of Zoom calls."[31] On November 29, 2018, Zoom released an update for Windows and Mac users that fixed the problem.[32] On December 3, 2018, Zoom released an update for Linux users.[33]

24. On March 26, 2019, Jonathan Leitschuh, a security researcher, notified Zoom of three vulnerabilities in Zoom's system, described below. Though primarily affecting Mac users of the Zoom service, the vulnerability has also affected Windows users.[34]

[26] Zoom, *Zoom for Government* (2019), https://zoom.us/government.

[27] Zoom, *Privacy Policy* (2019), https://zoom.us/privacy.

[28] Zoom, *Zoom Terms of Service* (2019), https://zoom.us/terms; Zoom, *Privacy Policy* (2019), https://zoom.us/privacy.

[29] *Id*.

[30] Zoom Video Communications, Inc, SEC Registration No. 333 (2019) (Form S-1 Registration Statement Under The Securities Act of 1933), https://www.sec.gov/Archives/edgar/data/1585521/000119312519083351/d642624ds1.htm.

[31] [R2] Zoom Message Spoofing (CVE-2018-15715), Tenable, https://www.tenable.com/security/research/tra-2018-40; David Wells, *Tenable Research Advisory: Zoom Unauthorized Command Execution (CVE-2018-15715)*, Tenable (Nov. 29, 2018), https://www.tenable.com/blog/tenable-research-advisory-zoom-unauthorized-command-execution-cve-2018-15715.

[32] *Id*.

[33] *Id*.

[34] Nicole Nguyen, *The Zoom Desktop App Lets Any Website Take Over Your Mac's Camera. Here's What To Do About it*, Buzzfeed News (July 9, 2019), https://www.buzzfeednews.com/article/nicolenguyen/zoom-webcam-hacker-watching-you-vulnerability.

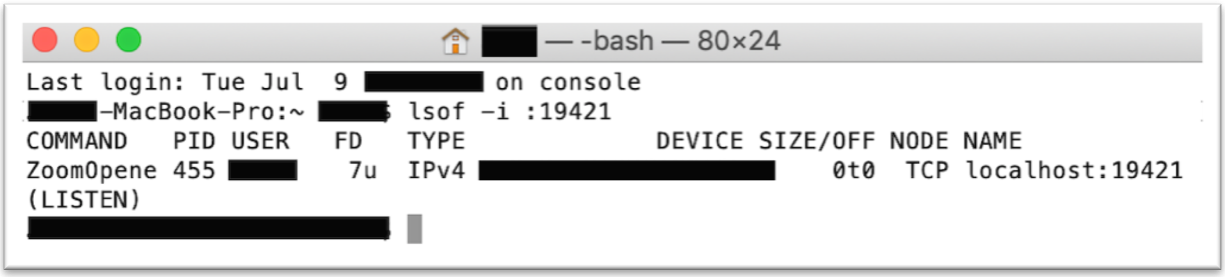
C. Zoom Security Vulnerabilities

Local Web Server Undermines User's Security and Privacy

25. When a Mac-user installs the Zoom client, Zoom also installs a localhost web server on the device without the user's knowledge.[35] The localhost web server allows users to join Zoom meetings without manually launching the Zoom client, but also allows others to join users to Zoom meetings without their knowledge or consent.[36]

26. Zoom developed this technique to bypass a security feature in Safari 12, which required users to affirmatively choose to join a Zoom meeting.[37] Zoom contends that the installation of the Zoom local web server "is a legitimate solution to a poor user experience problem, enabling our users to have faster, one-click-to-join meetings."[38]

27. The Zoom web server runs on port 19421 and can be confirmed by running "lsof -i :19421" in one's terminal.[39]



```
Last login: Tue Jul  9 [redacted] on console
[redacted]-MacBook-Pro:~ [redacted] lsof -i :19421
COMMAND   PID USER      FD   TYPE              DEVICE SIZE/OFF NODE NAME
ZoomOpene 455 [redacted]  7u  IPv4 [redacted]      0t0  TCP localhost:19421
(LISTEN)
[redacted]
```

Figure 1: Confirmation of Existence of Zoom's Local Web Server Even Though Zoom Was Uninstalled (Screen Shot July 10, 2019 at 10:34AM) (personal information of laptop user redacted)

28. Leitschuh discovered that the localhost web server runs with an undocumented Application Programming Interface ("API").[40] An attacker can reverse engineer undocumented APIs, leading to loss of data and a multitude of security issues.[41] In October 2014, for example, a hacker accessed and leaked tens of thousands of Snapchat photos by reverse engineering Snapchat's undocumented APIs.[42]

[35] Richard Farley, *Response to Video-On Concern*, Zoom Blog (July 9, 2019), https://blog.zoom.us/wordpress/2019/07/08/response-to-video-on-concern/. [hereinafter Farley Response].

[36] *Id*.

[37] *Id*.

[38] *Id*.

[39] Jonathan Leitschuh, *Zoom Zero Day: 4+ Million Webcams & Maybe an RCE? Just Get Them to Visit Your Website!*, Medium (July 8, 2019), https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5. [hereinafter Leitschuh, *Zoom Zero Day*].

[40] *Id*.

[41] *See* Perry Eising, *What Exactly Is an API*, Medium (Dec. 7, 2017), https://medium.com/@perrysetgo/what-exactly-is-an-api-69f36968a41f; *Undocumented APIs*, Microsoft (May 30, 2018), https://docs.microsoft.com/en-us/windows/win32/w8cookbook/undocumented-apis.

[42] *See* Ben Popper and Russell Brandom, *Is Snapchat's Unofficial API Just Too Easy To Hack?*, The Verge (Oct. 13, 2014), https://www.theverge.com/2014/10/13/6958745/is-snapchats-api-too-easy-to-hack; Andy Thurai, *What Are Your "Undocumented" APIs Up To?*, IBM Developer (Oct. 23, 2014),

29. Leitschuh also notes that Zoom encoded the localhost "in the dimensions of an image file . . . to bypass Cross-Origin Resource Sharing (CORS)."[43] CORS is a security policy that requires servers "to specify not just who can access its assets, but also *how* the assets can be accessed."[44] It controls "which resources a web page can request from outside domains."[45]

30. *Forbes* reported that Zoom's localhost web server "essentially bypasses user browser safeguards in the interests of user experience. Safeguards which are clearly there for good reason."[46] Leitschuh argues that Zoom's use of this web server "paint[s] a huge target on its back."[47]

31. The secret localhost web server interacts with every website a Zoom user visits.[48] If Zoom users visit a website with an iframe embed, the Zoom localhost web server will automatically launch the Zoom app—even if a user has not clicked a Zoom meeting URL.[49] Attackers can then deliberately place iframe embeds in their websites to enable Zoom users' cameras.[50]

32. Zoom's Chief Information Security Officer Richard Farley acknowledges this design choice—"[w]e consciously enabled the ability to have meeting joins initiated from within an iframe on a webpage"—but claims that it is "not a security concern."[51]

33. Zoom refuses to block the Zoom client auto-launch ability "because too many of its large enterprise customers actually use iframes in their implementation of Zoom's software."[52]

https://developer.ibm.com/apiconnect/2014/10/23/undocumented-apis/. [See also EPIC complaint to FTC regarding Snapchat]

[43]Leitschuh, *Zoom Zero Day*.

[44] CodeAcademy, *What is CORS?*, https://www.codecademy.com/articles/what-is-cors. *See also* Mozilla, *Cross-Origin Resource Sharing (CORS)*, https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS.

[45] Dennis Fisher, *Zoom Bug Allowed Access to Mac Webcam*, Decipher (July 9, 2019), https://duo.com/decipher/zoom-patches-bug-that-allowed-access-to-mac-webcam. *See also* Chris Duckett, *Zoom Defends Use of Local Web Server on Macs After Security Report*, ZDNet (July 9, 2019), https://www.zdnet.com/article/zoom-defends-use-of-local-web-server-on-macs-after-security-report/.

[46] Zak Doffman, *Confirmed: Zoom Security Flaw Exposes Webcam Hijack Risk, Change Settings Now*, Forbes (July 9, 2019), https://www.forbes.com/sites/zakdoffman/2019/07/09/warning-as-millions-of-zoom-users-risk-webcam-hijack-change-your-settings-now/#187d764f42d9.

[47] Leitschuh*, Zoom Zero Day*, *supra* note 40.

[48] *Id*.

[49] *Id*.; Nguyen, *supra* note 35.

[50] Leitschuh*, Zoom Zero Day*, *supra* note 40.

[51] Nguyen, *supra* note 35.

[52] Nick Statt, *Zoom Fixes Major Mac Webcam Security Flaw With Emergency Patch*, The Verge (July 9, 2019), https://www.theverge.com/2019/7/9/20688113/zoom-apple-mac-patch-vulnerability-emergency-fix-web-server-remove.

34. Even once the Zoom client has been uninstalled, the Zoom localhost web server remains.[53] Zoom's localhost web server allows Zoom to update and secretly reinstall the app after a user clicks on a meeting URL.[54]

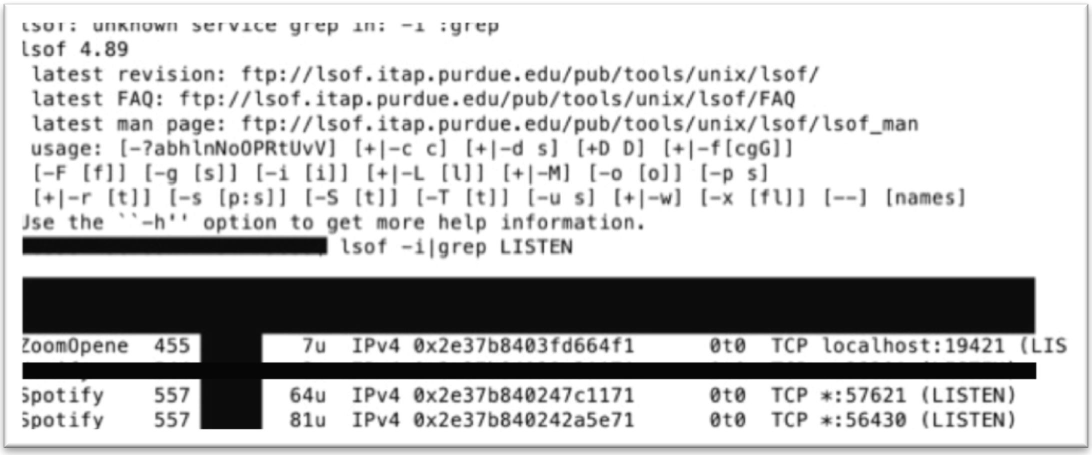
35. In a statement released on July 8, 2019, Zoom stated that there is no "easy" way to delete the Zoom web server: "The user needs to manually locate and delete those two apps for now. This was an honest oversight."[55]

36. Leitschub explains: "To shut down the web server, [a Zoom user must] run lsof -i :19421 to get the PID of the process, then do kill -9 [process number]. Then you can delete the ~/.zoomus directory to remove the web server application files."[56]

37. In the July 9 revision of their July 8 statement, Zoom announced the release of a patch that would "[r]emove the local web server entirely, once the Zoom client has been updated."[57]

38. Farley, however, still maintains that the web server was "stripped down to its bare functionality" and was secure.[58]

39. Farley also notes, "We are not alone among video conferencing providers" in installing web server processes.[59] The existence of a localhost web server can be confirmed by running the search: "lsof -i :grep LISTEN."



```
lsof: unknown service grep in: -i :grep
lsof 4.89
 latest revision: ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/
 latest FAQ: ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/FAQ
 latest man page: ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/lsof_man
 usage: [-?abhlnNoOPRtUvV] [+|-c c] [+|-d s] [+D D] [+|-f[cgG]]
 [-F [f]] [-g [s]] [-i [i]] [+|-L [l]] [+|-M] [-o [o]] [-p s]
 [+|-r [t]] [-s [p:s]] [-S [t]] [-T [t]] [-u s] [+|-w] [-x [fl]] [--] [names]
Jse the ``-h'' option to get more help information.
[redacted] lsof -i|grep LISTEN

[redacted]
ZoomOpene   455 [redacted]     7u  IPv4 0x2e37b8403fd664f1      0t0  TCP localhost:19421 (LIS
[redacted]
Spotify     557 [redacted]    64u  IPv4 0x2e37b840247c1171      0t0  TCP *:57621 (LISTEN)
Spotify     557 [redacted]    81u  IPv4 0x2e37b840242a5e71      0t0  TCP *:56430 (LISTEN)
```

Figure 2: Examples of Additional Apps With localhost Web Servers (Screen Shot July 10, 2019 at 3:55PM) (personal information of laptop user redacted)

[53] Leitschuh, *Zoom Zero Day*, *supra* note 40.

[54] *Id*.

[55] Farley Response, *supra* note 36. Zoom's statement was released on July 8, 2019 and was revised on July 9, 2019. Apple subsequently address the security vulnerability and removed the Zoom web server in an update released July 10, 2019. Zach Whittaker, *Apple has pushed a silent Mac update to remove hidden Zoom web server*, TechCrunch (July 10, 2019) https://techcrunch.com/2019/07/10/apple-silent-update-zoom-app/.

[56] Leitschuh, *Zoom Zero Day*, *supra* note 40.

[57] Farley Response, *supra* note 36.

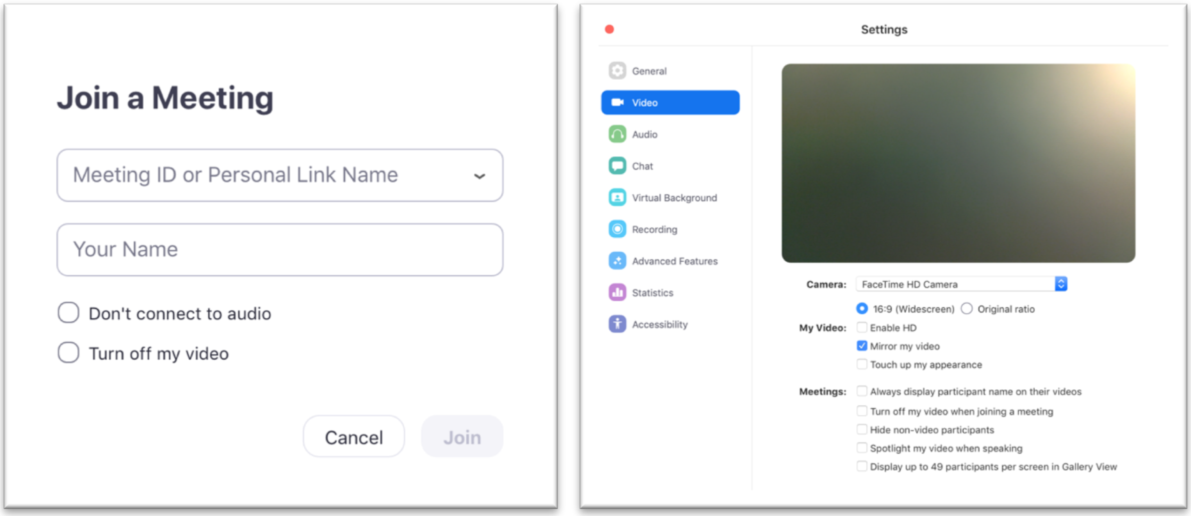
[58] Statt, *supra* note 53.

[59] Farley Response, *supra* note 36.

Remote Access to Zoom Users' Webcams Without Consent

40. If a Zoom user does not opt-out of video, Zoom may enable the user's webcam and subject the user to remote surveillance.

41. By default, when a user joins a Zoom call, her camera is turned on. Users can choose to opt-out in one of two ways: (1) by clicking "Turn off my video" when joining the meeting, or (2) by manually changing their default settings by clicking "Turn off my video when joining a meeting" under the "Video" tab (see Figure 3).



Join a Meeting

Meeting ID or Personal Link Name

Your Name

○ Don't connect to audio

○ Turn off my video

Cancel | Join

Settings

Camera: FaceTime HD Camera

● 16:9 (Widescreen) ○ Original ratio

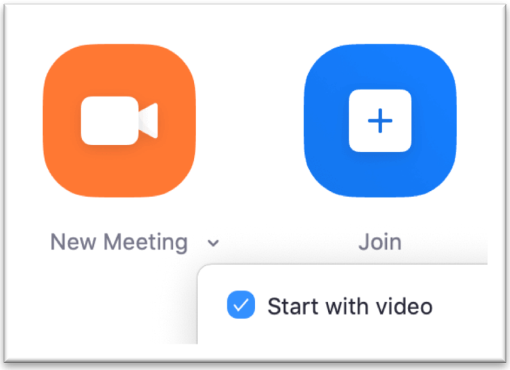
My Video:
□ Enable HD
☑ Mirror my video
□ Touch up my appearance

Meetings:
□ Always display participant name on their videos
□ Turn off my video when joining a meeting
□ Hide non-video participants
□ Spotlight my video when speaking
□ Display up to 49 participants per screen in Gallery View

Figure 3*: Joining a Zoom Meeting (Screen Shot July 10, 2019 at 1:00PM) (left); (Screen Shot July 10, 2019 at 1:03PM) (right)*

42. If a user does not opt out of video, the meeting host can choose whether a user's camera is turned on or off. If the host merely clicks on "New Meeting" or on the image of the video camera (see Figure 4), the web cams of all meeting participants are turned on.

43. For a meeting host to start a meeting without video, she has to click on the dropdown arrow and manually uncheck the box "Start with Video" (see Figure 4).



☑ Start with video

Figure 4*: Host Starting a Zoom Meeting (Screen Shot July 10, 2019 at 1:09PM)*

44. According to Leitschuh, an attacker can gain full access to an unsuspecting Zoom user's video feed by tricking the user into clicking the attacker's meeting URL.[60] To demonstrate, Leitschuh was able to "[get] a user into a call without their permission."[61]

45. In response, Farley claimed that there is "no indication that this has ever happened." [62] But Farley did not deny that Leitschuh's phishing attack was a possibility.[63]

46. Farley later admitted to BuzzFeed that "[m]eeting joins happen all the time. Millions a day. There isn't really a way for us to look at the logs to determine whether that was an intentional join by the user or the user was phished into joining."[64]

47. Zoom announced that the video-on default would be changed in a future July update such that "1. First-time users who select the 'Always turn off my video' box will automatically have their video preferences saved. . . 2. Returning users can update their video preferences and make video OFF by default at any time through the Zoom client settings."[65]

48. The July update still would not fix the security vulnerability, but instead would merely tweak Zoom's software so that users who already know about the security flaws can manually adjust their account settings.[66] Many Zoom users would remain vulnerable to surveillance.

Zoom Leaves Users Vulnerable to Denial of Service (DoS) Attacks

49. The video-on default vulnerability additionally allows hackers to launch DoS attacks against Zoom users.[67] A DoS attack "occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor."[68]

50. Zoom concedes that because of the vulnerability, a hacker could target a Zoom user "with an endless loop of meeting join requests, effectively causing the targeted machine to lock up."[69]

[60] A prior version Zoom enabled the attacker to bypass a Zoom user's settings. *See* Leitschuh*, Zoom Zero Day*. Though an attacker now cannot now bypass a Zoom user's settings if she has manually opted-out of video, Zoom "did not disable the ability for an attacker to forcibly join a call anyone visiting a malicious site." *Id*.

[61] *Id*.

[62] Farley Response, *supra* note 36.

[63] *Id.*

[64] Nguyen, *supra* note 35.

[65] Farley Response, *supra* note 36.

[66] Lily Hay Newman, *A Zoom Flaw Gives Hackers Easy Access to Your Webcam*, Wired (July 9, 2019), https://www.wired.com/story/zoom-bug-webcam-hackers/.

[67] Leitschuh*, Zoom Zero Day*, *supra* note 40.

[68] Cybersecurity and Infrastructure Security Agency (CISA), *Security Tip (ST04-015)*, https://www.us-cert.gov/ncas/tips/ST04-015.

[69] Farley Response, *supra* note 36.

51. Zoom contends the company fixed this problem in May 2019.[70] However, in the update records there is no indication of this particular fix.[71]

52. Because Zoom determined that the DoS vulnerability was "empirically a low-risk vulnerability," it did not require users to update their Zoom applications.[72]

D. Zoom Is Still Failing to Protect Consumer Privacy

53. Zoom's flaws were first uncovered by Jonathan Leitschuh, a security researcher, who contacted Zoom on March 26, 2019.[73] Zoom initially responded that the technique was a "legitimate solution to a poor user experience, enabling our users to have seamless, one-click-to-join meetings, which is our key product differentiator."[74] Ninety days after contacting Zoom, Leitschuh expressed strong concerns about the company's security practices in his first published article:

> First off, let me start off by saying having an installed app that is running a web server on my local machine with a totally undocumented API feels incredibly sketchy to me. Secondly, the fact that any website that I visit can interact with this web server running on my machine is a huge red flag for me as a Security Researcher.[75]

54. Leitschuh noted that "[a]ll of the vulnerabilities described in this report can be exploited be exploited via 'drive-by attack' methodologies."[76] A "drive-by" attack is "when an adversary gains access to a system through a user visiting a website over the normal course of browsing."[77]

55. Zoom only publicly recognized serious security concerns with its product upon "hearing the outcry from . . . users and the security community."[78] The company acknowledged that it "[i]nitially . . . did not see the web server or video-on posture as significant risks to our customers and, in fact, felt that these were essential to our seamless join process."[79]

[70] *Id*.
[71] Zoom keeps a record of its updates in the Zoom Help Center. Two updates were made in May 2019. The May 12, 2019 update (Version 4.4.52600.0508) fixed the problem of "Jabra 510 devices . . . intermittently disconnecting." The May 19, 2019 update (Version 4.4.53582.0519) made "minor bug fixes." Neither explicitly claims that the vulnerability in question here has been fixed. *See* Zoom Help Center, *New Updates for Mac OS*, https://support.zoom.us/hc/en-us/articles/201361963-New-Updates-for-Mac-OS. Leitschuh noted that "[t]his DOS vulnerability was patched in version 4.4.2 of the Zoom client." *Supra* note 40. However, according to the Zoom Help Center, there is no version 4.4.2 of Zoom client**.**
[72] Farley Response, *supra* note 36.
[73] Leitschuh*, Zoom Zero Day*, *supra* note 40.
[74] Chris Duckett, *Zoom Defends use of Local Web Server on Macs After Security Report*, ZDNet (July 9, 2019), https://www.zdnet.com/article/zoom-defends-use-of-local-web-server-on-macs-after-security-report/.
[75] Leitschuh*, Zoom Zero Day*, *supra* note 40.
[76] Leitschuh*, Zoom Zero Day*, *supra* note 40.
[77] Mitre Attack, *Drive-By Compromise*, https://attack.mitre.org/techniques/T1189/.
[78] Farley Response, *supra* note 36.
[79] *Id.*

Zoom's "patch" solutions are incomplete and were only offered several months after Zoom was first informed of security issues with its service.[80]

E. Consumers Oppose Zoom's Failure to Protect Users' Privacy and Security

56. Following the release of Leitschuh's article, Zoom users immediately expressed strong concern about Zoom's services. Many prominent news organizations also criticized the company. Many experts recommended removing the app.[81] One technology writer advised readers to "[s]tay away from downloading Zoom or clicking on any Zoom links for the foreseeable future."[82]

57. Jason Snell, director of Mac Publishing, wrote about Zoom's decision to circumvent Apple security features: "what gives me pause is what this says about Zoom's priorities as a company. They are acting like they know better than Apple how to keep their users secure—and the evidence strongly suggests they don't."[83]

58. Matt Haughey, a programmer and web designer, wrote: "This Zoom vulnerability is bananas. I tried one of the proof of concept links and got connected to three other randos also freaking out about it in real time."[84]

59. Security Consultant Eleanor Saitta criticized Zoom for its failure to consider surveillance issues and user choices.[85] She explained:

> Per their own statement, Zoom made a set of product decisions that intentionally prioritized use of their system over user choice . . . Zoom clearly had not considered malicious uses—or, worse, had disregarded them—when they decided to remove this choice from the user, and appear to consider Zoom use, and presumably their revenue growth, more important than surveillance of users.[86]

60. Thomas Reed, an Apple security expert, said: "The web server is concerning because of the possibility that someone could find a way to use it remotely to trigger remote code execution."[87]

[80] *See* Tom McKay, *Serious Security Flaw with Teleconferencing App Could Allow Websites to Hijack Mac Webcams*, Gizmodo (July 9, 2019), https://gizmodo.com/serious-security-flaw-with-teleconferencing-app-allowed-1836202438.

[81] *See, e.g.*, Nguyen, *supra* note 35; Zak Doffman, *Confirmed: Zoom Security Flaw Exposes Webcam Hijack Risk, Change Settings Now*, Forbes (July 9, 2019), https://www.forbes.com/sites/zakdoffman/2019/07/09/warning-as-millions-of-zoom-users-risk-webcam-hijack-change-your-settings-now/#4eb415f642d9.

[82] Charlie Warzel, *Your Inbox is Spying on You*, New York Times (July 9, 2019), https://www.nytimes.com/2019/07/09/opinion/email-tracking.html.

[83] Jason Snell (@jsnell), Twitter (July 9, 2019), https://twitter.com/jsnell/status/1148672054188638209.

[84] Matt Haughey (@mathowie), Twitter (July 8, 2019), https://twitter.com/mathowie/status/1148391109824921600.

[85] Nicole Nguyen, *The Zoom Desktop*, *supra* note 7.

[86] *Id.*

[87] Newman, *supra* note 67.

61. Lily Hay Newman, a writer "focused on information security, digital privacy, and hacking,"[88] wrote: "[G]iven the choice between protecting security and privacy or prioritizing convenience, Zoom unabashedly chose convenience. And will continue to do so."[89]

62. Noting that he was deleting Zoom from his devices, writer and activist Cory Doctorow wrote in his blog:

> I am a regular Zoom user and I'm aghast at this behavior. From . . . the incredibly poor choice to install a secret webserver on its customers' computers, to the even worse form in creating an uninstaller that leaves that webserver in place and running in the background after their software is removed, this entire episode inspires great distrust for the company.[90]

63. Users condemned Zoom in comments to Leitschuh's article. In the first 24 hours following publishing on Medium, the article received 37,000 "claps" by readers.[91] Several commenters remained frustrated even after Zoom's response.

64. Commenter "Keir Thomas" said: "This is 100% unacceptable for corporate IT policies."[92]

65. Commenter "msbrandymorgan" said: "This scared the pants off me! I have been using Zoom for years and was just raving about it on a Youtube video. I really appreciate you taking the time to tell us how to take care of some of these issues ourselves."[93]

66. Commenter "Ivan Jansch" noted:

> The problem with tools such as this is that they are often installed under social pressure. You're joining an online meeting and at the last moment you see they are using zoom/skype/meet/whatever to do the meeting. While the other participants text you that they're waiting for you you hastily install the software, click through all the dialogs without reading them just to be in your meeting in time.[94]

67. In response to the article, a ycombinator commenter said:

> I think they need to be made aware that this isn't acceptable. My reply to their support team: I do not believe this is a fair trade-off - allowing any arbitrary web site local control of privileged software installed on my

[88] Wired, Lily Hay Newman (2019), https://www.wired.com/author/lily-hay-newman/.
[89] Newman, *supra* note 67.
[90] Cory Doctorow, *Zoom Has Slow-Walked a Fix For a Bug That Allows Randos To Take Over Your Mac's Camera*, Boingboing (July 9, 2019), https://boingboing.net/2019/07/09/wontfix.html.
[91] Leitschuh*, Zoom Zero Day*, *supra* note 40.
[92] Keir Thomas, Comment to Jonathan Leitschuh, *Zoom Zero Day*, *supra* note 40.
[93] Msbrandymorgan, Comment to Jonathan Leitschuh, *Zoom Zero Day*, *supra* note 40.
[94] Ivan Jansch, Comment to Jonathan Leitschuh, *Zoom Zero Day*, *supra* note 40.

> machine - because Safari offers a security prompt (specifically so that any arbitrary web site does not gain control of privileged software on my machine). I will be switching ~/.zoomus/ZoomOpener.app off, and considering other options until it has been fixed.[95]

68. Another commenter said, "I liked Zoom when I used it a couple of times, but the reinstall 'feature' is a huge violation of my trust. Software from the company behind it will not touch my system anymore."[96]

69. Following recent news reports, Zoom's shares have fallen 1.1%, reflecting widespread decrease in consumer trust.[97]

V. Legal Analysis

The FTC's Section 5 Authority

70. Zoom is engaging in unfair and deceptive acts and practices.[98] Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act's prohibitions.[99] These powers are described in FTC Policy Statements on Deception[100] and Unfairness.[101]

71. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[102] The FTC has identified two primary factors that support a finding of unfairness: whether the practice injures consumers and whether it violates established public policy.[103]

[95] Rahoulb, *Comment to Vulnerability in the Mac Zoom Client Allows Malicious Websites to Enable Camera*, YCombinator (July 9, 2019), https://news.ycombinator.com/item?id=20389668.

[96] Thijsvandien, *Comment to Vulnerability in the Mac Zoom Client Allows Malicious Websites to Enable Camera*, YCombinator (July 9, 2019), https://news.ycombinator.com/item?id=20388111.

[97] Bailey Lipschultz, *Zoom Video Falls as Mac Webcam Flaw Report Weighs on Shares*, Bloomberg (July 9, 2019), https://www.bloomberg.com/news/articles/2019-07-09/zoom-video-falls-as-mac-webcam-flaw-report-drags-red-hot-stock.

[98] *See* 15 U.S.C. § 45.

[99] *Id.*

[100] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), http://www.ftc.gov/bcp/policystmt/ad-decept.htm [hereinafter FTC Deception Policy].

[101] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [hereinafter FTC Unfairness Policy].

[102] 15 U.S.C. § 45(n); *see, e.g.*, *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 04-CV-00377, WL 2403124, at *3 (D.N.H. 2004) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").

[103] FTC Unfairness Policy, *supra* note 103.

72. The injury must be "substantial."[104] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[105] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[106]

73. Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces."[107] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[108]

74. Finally, "the injury must be one which consumers could not reasonably have avoided."[109] This factor enables the FTC to act in situations where seller behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision making," while leaving consumer choice to govern the market in most instances.[110] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[111]

75. The FTC will also look at "whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise."[112] Public policy is used to "test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present."[113] The Commission typically uses public policy as a "means of providing additional evidence on the degree of consumer injury caused by specific practices."[114]

76. An act or practice is deceptive if there has been a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[115]

77. There are three elements to a deception claim. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[116] The relevant inquiry for

[104] *Id.*
[105] *Id.*; *see, e.g.*, Complaint for Injunctive and Other Equitable Relief, *Fed. Trade Comm'n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099, at *5 (D. Md. May 1, 2006) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").
[106] FTC Unfairness Policy, *supra* note 103.
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] FTC Deception Policy, *supra* note 102.
[116] *Id.*; *see, e.g., Fed Trade Comm'n v. Pantron I Corp.*, 33 F.3d 1088, 1101 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).

this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.[117]

78. Second, the act or practice must be considered from the perspective of a reasonable consumer.[118] "The test is whether the consumer's interpretation or reaction is reasonable."[119] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[120]

79. Finally, the representation, omission, or practice must be material.[121] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[122] Express claims will be presumed material.[123] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[124]

80. The harms of Zoom's practices are within the scope of the FTC's authority to enforce Section 5 of the FTC Act, and Zoom should face FTC action for these violations.

Zoom's Actions Constitute an Unfair Trade Practice

81. Zoom's security vulnerabilities constitute an unfair business practice because they are likely to cause substantial injury to customers, which is not reasonably avoidable by customers and not outweighed by countervailing benefits to consumers or to competition. Zoom provided conferencing services to thousands of consumers, surreptitiously forcing users to download its remote web server and turning on their video in conferences as a default, rather than with user consent. Zoom's actions placed users at risk of severe privacy violations, including remote surveillance or distribution of illicit photographs or location information obtained through users' Mac cameras. These consequences constitute "unwarranted health and safety risks" similar to those resulting from obtaining and selling confidential customer phone records.[125]

82. This injury was not reasonably avoidable by consumers themselves. Consumers were not made aware of Zoom's vulnerabilities. Users were also unable to use Zoom Client without the web server and thus would have been forced to choose between forgoing their privacy interest or forgoing Zoom's services had they been aware of the vulnerabilities.

[117] FTC Deception Policy, *supra* note 102.
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] FTC Unfairness Policy, *supra* note 103; *see Fed. Trade Comm'n v. Information Search, supra* note 107.

83. This substantial and unavoidable injury is not offset by any countervailing benefits. There is no evidence that Zoom's use of a secret web server benefited either unknowing consumers or competition.

84. No statute or other source of public policy authorizes Zoom's unethical conduct. The harm caused was reasonably avoidable, yet Zoom affirmatively chose to deviate from industry standard systems to run its product through a secret web server.

Zoom Made Deceptive Representations About the Privacy and Security of Zoom Client

85. Zoom made material misrepresentations that misled reasonable consumers regarding the security of the Zoom Client application.[126] In addition to presenting Zoom Client as secure, Zoom did not make clear to consumers that the company would install a local web server that would bypass browser security settings and allow Zoom to reinstall the software without the user's consent. These misrepresentations were both likely to mislead and actually did mislead consumers.

86. Users reasonably relied on Zoom's promises when choosing to use and purchase Zoom's services. 40 million individuals participated in Zoom meetings in 2015,[127] and Zoom had 450,000 business customers by 2017.[128]

87. Zoom's misrepresentations were material. Zoom customers – including EPIC, technology companies, investment banks, healthcare providers, and universities[129] – are sensitive to online privacy and security. Many would have chosen a different product if the deception had not occurred, but purchased Zoom's product in reasonable reliance on its misrepresentations of adequate security.

88. Zoom's material representations were deceptive. Zoom was aware of this vulnerability and chose to do nothing about it until July 2019.[130] Zoom continues to prefer non-disclosure of security vulnerabilities and recommends that future security concerns be addressed through its private bug bounty program, which includes non-disclosure terms.[131]

[126] Zoom, Zoom Terms of Service, https://zoom.us/terms (effective May 30, 2019) ("Zoom will maintain reasonable physical and technical safeguards to prevent unauthorized disclosure of or access to Content, in accordance with industry standards."); Zoom, Privacy Policy, https://zoom.us/privacy (updated Mar. 19, 2019) ("Zoom Video Communications, Inc. ("Zoom") is committed to protecting your privacy and ensuring you have a positive experience on our website and in using our products and services (collectively, "Products")").

[127] Zoom, *Zoom Raises $30M in Series C Funding Led by Emergence Capital*, GlobeNewswire (Feb. 4, 2015), https://www.globenewswire.com/news-release/2015/02/04/1130354/0/en/Zoom-Raises-30M-in-Series-C-Funding-Led-by-Emergence-Capital.html.

[128] Alex Konrad, *How Zoom CEO Eric Yuan Turned Frustration Into A $1B Valuation In Six Years*, Forbes (Jan. 17, 2017), https://www.forbes.com/sites/alexkonrad/2017/01/17/how-zoom-ceo-eric-yuan-turned-frustration-into-a-1-billion-valuation-in-six-years/#12ad82cf7dcc.

[129] Zoom, *Our Customers Love Us*, https://zoom.us/customer/all.

[130] Farley Response, *supra* note 36.

[131] Farley Response, *supra* note 36.

Unfair and Deceptive Privacy Practices and Policies Constitute Consumer Harm

89. Zoom's actions—including its decision to install a hidden web server on users' Macs and require consumers to manually change their default camera settings—placed users at risk of severe violations of their privacy. Zoom customers risked consequences including: remote surveillance through hackers viewing a video stream from users' computers without their knowledge, an attacker implementing a Denial of Service (DOS) attack through sending repeated HTTP GET requests, or users being launched into a video call with an advertiser without his or her consent.[132] These privacy intrusions can have severe results, from illicit photographs or video being taken for sale to distribution of information for the purposes of physical harm.

90. The widespread alarm from Zoom users after the exposure of the vulnerability in the Mac Zoom Client illustrates that the vulnerabilities substantially injure Zoom users and harm the public interest.[133]

91. Furthermore, Zoom's inadequate privacy policy failed to notify users of these substantial risks.[134] Zoom's practices thus allowed access to consumer information in ways and for purposes other than those consented to or relied on by users, causing them to believe falsely that Zoom Client was secure and undermining users' ability to avail themselves of the privacy protections promised by the company.

92. The FTC Act empowers and directs the FTC to investigate business practices, including poor online security practices and inadequate privacy policies, that constitute consumer harm.[135]

93. The FTC has previously barred companies from circumventing privacy settings without user consent. In 2012, the FTC fined Google $22.5 million for circumventing privacy settings on Safari browsers in order to place cookies without user consent.[136] Google assured users that the Safari default settings would block ad-tracking software, but then secretly collected cookies.[137] In addition to the civil penalty, Google was required to maintain systems that delete Google cookies from Safari browser users and submit to FTC monitoring of its compliance.[138]

94. Like Google, Zoom circumvented the privacy settings of browsers for its own advantage and without user consent. Even more so than Google, Zoom's conduct created additional risk to consumers by enabling video surveillance.

[132] Leitschuh, *Zoom Zero Day*.

[133] Newman, *supra* note 67.

[134] Zoom, Privacy Policy, https://zoom.us/privacy (updated Mar. 19, 2019).

[135] 15 U.S.C. § 45.

[136] United States v. Google, Inc., No. CV 12-04177, 2012 WL 5833994, at *2-3 (N.D. Cal Nov. 16, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf.

[137] *Id.*

[138] *Id.*

95. In 2017, the FTC found that computer manufacturer Lenovo engaged in unfair and deceptive business practices when the company preloaded a software program that interfered with users' browser functionality and created serious security vulnerabilities.[139] Lenovo laptops came with a preinstalled software program which interfered with how a user's browser interacted with websites, acting as a "man-in-the-middle" between consumers' browsers and the websites they visited.[140] The software also replaced websites' digital certificates with its own certificates, overriding browsers' ability to confirm the privacy of encrypted websites.[141]

96. As Acting FTC Chairman Maureen K. Ohlhausen's summarized: "Lenovo compromised consumers' privacy when it preloaded software that could access consumers' sensitive information without adequate notice or consent to its use. This conduct is even more serious because the software compromised online security protections that consumers rely on."[142]

97. The consent order obtained by the FTC prohibited Lenovo from making misleading representations and preinstalling similar software without consent in the future.[143] The Lenovo consent order also required Lenovo to establish a comprehensive software security program and submit to third-party software security assessments.[144]

98. Like Lenovo, Zoom surreptitiously installed software that interfered with overrode users' browser functionality and security processes without consent. Both companies created serious security vulnerabilities by doing so.

99. The FTC has previously barred companies from propagating deceptive claims about privacy and security. In 2018, the FTC obtained a settlement with mobile phone-maker BLU Products Inc. for including deceptive representations in its privacy policy.[145] BLU Products failed to implement appropriate security procedures, but represented to consumers that the company used "appropriate" physical, electronic, and managerial procedures to protect consumers' personal information.[146] The terms of the order prohibit BLU from misrepresenting the extent to which it protects the privacy and security of

[139] Lenovo, No. 1523134, 7-8 (2017) (complaint), https://www.ftc.gov/system/files/documents/cases/1523134_lenovo_united_states_complaint.pdf.

[140] Federal Trade Commission, *Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security* (Sept. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

[141] *Id.*

[142] *Id.*

[143] Lenovo, No. 1523134, 8-9 (2017) (decision and order), https://www.ftc.gov/system/files/documents/cases/1523134_lenovo_united_states_agreement_and_do.pdf.

[144] *Id.* at 9-10.

[145] Blu Products, Inc., No. C-4657 (2018) (decision and order), https://www.ftc.gov/system/files/documents/cases/1723025_blu_decision_and_order_4-30-18.pdf; *see also* Federal Trade Commission, *FTC Gives Final Approval to Settlement with Phone Maker BLU* (Sept. 10, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/ftc-gives-final-approval-settlement-phone-maker-blu.

[146] Blu Products, Inc., No. C-4657, 3-4 (complaint), https://www.ftc.gov/system/files/documents/cases/172_3025_c4657_blu_complaint_9-10-18.pdf.

personal information and require it to implement and maintain a new comprehensive security program.[147]

100. The FTC also recently prohibited PayPal, Inc. and its subsidiary Venmo from misrepresenting Venmo's level of security and the extent of control provided by its privacy settings.[148] Venmo's public statements on its mobile app and website misled consumers about the extent to which they could control the privacy of their transactions, as well as the application's protection of consumer financial accounts.[149] The FTC's consent order also requires Paypal to make affirmative disclosures about its privacy practices.[150]

101. In addition, the FTC barred Life is Good, Inc. from "misrepresent[ing] in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected from or about consumers."[151] The company had represented to its customers, "we are committed to maintaining our customers' privacy," when, in fact, it did not have secure or adequate measures of protecting personal information.[152] The Commission further ordered the company to establish comprehensive privacy protection measures in relation to its customers' sensitive information.[153]

102. The FTC has also enjoined companies from maintaining inadequate privacy policies. The FTC obtained a consent order from Sears Holding Management Corporation which forced the company to disclose more information about the privacy of customers' data, replacing its misleading privacy policy that did not "adequately [inform consumers as to] the full extent of the information the software tracked."[154]

103. In addition, the Commission obtained a consent order against an online company, Gateway Learning Corporation, for changing its privacy policy without obtaining user consent.[155] The settlement bars Gateway Learning from, among other things,

[147] Blu Products, Inc., No. C-4657, 4 (2018) (decision and order).
[148] PayPal, Inc., No. 162-3102, 7-8 (2018) (decision and order), https://www.ftc.gov/system/files/documents/cases/venmo_agreement_with_decision.pdf; *see also* Federal Trade Commission, *PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act* (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.
[149] PayPal, Inc., No. 162-3102, 4-10 (2018) (complaint), https://www.ftc.gov/system/files/documents/cases/venmo_complaint.pdf.
[150] PayPal, Inc., No. 162-3102, 9 (2018) (decision and order).
[151] Life is Good, No. C-4218, 2-3 (2008) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2008/04/080418do.pdf.
[152] Life is Good, No. C-4218, 2 (2008) (complaint), https://www.ftc.gov/sites/default/files/documents/cases/2008/04/080418complaint.pdf.
[153] Life is Good, No. C-4218, 3 (2008) (decision and order).
[154] Sears Holdings Mgmt. Corp., No. C-4264 (2009) (complaint), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf; *see also* In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.
[155] Gateway Learning Corp., No. C-4120 (2004) (decision and order), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.

"misrepresent[ing] in any manner, expressly or by implication . . . the manner in which Respondent will collect, use, or disclose personal information."[156]

104. Like BLU Products, PayPal, and Life is Good, Zoom misrepresented its commitment to privacy and propagated deceptive claims about privacy, security, and user control. Zoom assured users of their privacy on the platform even while knowing the vulnerabilities of the Zoom Client system.[157] The company also propagated deceptive claims about privacy, security, and user control. Zoom's privacy practices and policy were fundamentally inadequate like those of Sears Holding Management Corporation and changed without user consent like the privacy policy of Gateway Learning Corporation.

The FTC Must Prevent Ongoing Harm to Consumers

105. Zoom Client's vulnerabilities jeopardize consumer privacy and safety.

106. Zoom's misrepresentations of its privacy settings and associated policies are misleading and fail to provide users clear and necessary privacy protections.

107. Absent injunctive relief by the Commission, Zoom is likely to continue its unfair and deceptive business practices and harm the public interest.

108. Absent injunctive relief by the Commission, the privacy safeguards for consumers engaging in online conferencing and communication will be diminished.

VI. Prayer for Investigation and Relief

109. EPIC requests that the Commission investigate Zoom, enjoin its unfair and deceptive business practices, and require Zoom to protect the privacy of Zoom users. Specifically, EPIC requests the Commission to:

a. Initiate an investigation into Zoom's security vulnerabilities, including: Zoom Client's use of a remote web server, including its automatic installation of Zoom Client without consent, and Zoom Client's default video settings;

b. Compel Zoom to notify by email all current and previous users of the Zoom client vulnerabilities, the currently available patches, and the remaining system vulnerabilities;

c. Compel Zoom to remove the Zoom remote web server from the computers of all current and previous Zoom users;

d. Compel Zoom to change its default video setting to off and give Zoom users more control over their privacy settings;

[156] *Id.*

[157] *See* Zoom, Privacy Policy, https://zoom.us/privacy (updated Mar. 19, 2019).

e. Compel Zoom to make its security practices clearer and more comprehensible;

f. Investigate other companies engaged in similar practices;

g. Provide such other relief as the Commission finds necessary and appropriate.

110. EPIC reserves the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully Submitted,
/s/
Marc Rotenberg, EPIC Executive Director
Christine Bannan, EPIC Consumer Protection Counsel
Jessica Hui, EPIC IPIOP Clerk
Lauren O'Brien, EPIC IPIOP Clerk
Sarah Parker, EPIC IPIOP Clerk
Sonali Seth, EPIC IPIOP Clerk
Jacob Wiener, EPIC IPIOP Clerk

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

July 11, 2019