Jason S. Hartley (SBN 192514)
HARTLEY LLP
101 West Broadway, Suite 820
San Diego, California 92101
Telephone: 619-400-5822
hartley@hartleyllp.com

Norman E. Siegel (*pro hac vice* forthcoming)
J. Austin Moore (*pro hac vice* forthcoming)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: 816-714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TESHA KONDRAT, GAVIN WOLFE, and CHANELLE MURPHY, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

ZOOM VIDEO COMMUNICATIONS, INC.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1. **Violation of California's Unfair Competition Law**
2. **Breach of Implied Contract**
3. **Violation of California's Consumer Privacy Act**
4. **Violation of California's Consumer Legal Remedies Act**
5. **Unjust Enrichment/Quasi-Contract**
6. **Declaratory Judgment**
7. **Negligence**
8. **Invasion of Privacy (Public Disclosure of Private Facts)**

Plaintiffs Tesha Kondrat, Gavin Wolfe, and Chanelle Murphy, individually and on behalf of all persons similarly situated, bring this Class Action Complaint against Defendant Zoom Video Communications, Inc. ("Defendant" or "Zoom"), based upon personal knowledge with respect to themselves, and on information and belief derived from investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. "*I really messed up*." That's what Zoom's chief executive officer (CEO) Eric Yuan admitted on April 4, 2020, after dozens of security and privacy flaws had been exposed in his company's wildly popular video-conferencing platform Zoom. But Mr. Yuan's admission comes too late for the millions of individuals who already downloaded and utilized the Zoom platform, unknowingly exposing themselves to sweeping privacy issues that could place them at risk of harm for years to come. As Mr. Yuan soberly acknowledged: "*This kind of thing shouldn't have happened*."

2. Zoom is a video communications provider, offering a cloud platform for video and audio conferencing, collaboration, chat and webinars. Its meteoric rise from a startup with 40 engineers in 2011 to its $20 billion initial public offering in 2019 was celebrated, and its trajectory during the COVID-19 pandemic has exponentially increased as the homebound population uses it as their business and social lifeline. But Zoom's assent came at the expense of consumers' privacy, as it prioritized its breakneck growth above the security of consumers' data and privacy.

3. Zoom's sudden ubiquitous presence in the lives of Americans forced to stay at home and limit face-to-face communications has exposed numerous deficiencies in the technology's data privacy and security, with new problems coming to light as each day passes. Zoom is now playing catch-up to fix each problem as it arises, but it appears to always be one step behind. By using Zoom's rushed-to-market technologies, consumers' private communications and personally-identifying information and data are being exposed to third-parties, both intentionally by Zoom, and maliciously by nefarious actors exploiting flaws in Zoom's data security.

4. As a result of Zoom's intentional and negligent data security failures, Plaintiffs' and Class Members' personal information has been exposed and is at a significant risk of further exposure, and their privacy-rights have been violated. Plaintiffs bring this lawsuit on behalf of themselves and other similarly-situated users of Zoom's technologies to hold Zoom responsible for its deficient privacy and data security, stop Zoom from continuing to profit at the expense of consumers' privacy and security, require that Zoom take all necessary measures to secure the privacy of user accounts and devices, and compensate Plaintiffs and Class Members for the damage that its acts and omissions have caused.

PARTIES

5. Plaintiff Tesha Kondrat is a resident and citizen of Los Angeles, California. She agreed to pay $14.99 per month for Zoom's "Pro" video conferencing plan to communicate with family, friends, and business colleagues in the midst of the pandemic. At the time she began using Zoom's products and services, she was not aware, and did not understand, that they included significant security-deficiencies that would result in the exposure and risk of exposure of her private communications and personally-identifying information. If Ms. Kondrat had known what she now knows about Zoom's data security and privacy deficiencies, she would not have purchased Zoom, or would not have paid as much for it.

6. Plaintiff Gavin Wolfe is a resident and citizen of Sunnyvale, California. He agreed to pay $149.90 annually for Zoom's "Pro" video conferencing plan to host a Bible study group in the midst of the pandemic. At the time he began using Zoom's products and services, he was not aware, and did not understand, that they included significant security-deficiencies that would result in the exposure and risk of exposure of his private communications and personally-identifying information. If Mr. Wolfe had known what he now knows about Zoom's data security and privacy deficiencies, he would not have purchased Zoom, or would not have paid as much for it.

7. Plaintiff Chanelle Murphy is a resident and citizen of Sunnyvale, California. She downloaded and used the Zoom application for iOS. At the time she began using Zoom's products and services, she did not know Zoom was sharing her personally-identifying information to third-parties, like Facebook, and did not consent to this practice. If Ms. Murphy had learned what she knows now about Zoom's practice of sharing personally-identifying information with third-parties, like Facebook, she would not have downloaded and used the Zoom application.

8. Defendant Zoom is a Delaware corporation with its principal place of business in San Jose, California.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332, the Class Action Fairness Act, because: (i) there are 100 or more class members; (ii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and (iii) there is minimal diversity because members of the Class are citizens of different states from Defendant.

10. This Court has personal jurisdiction over Defendant because it maintains its headquarters in this District and operates in this District. Through its business operations in this District, Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because significant events giving risk to this case took place in this District, and because Defendant is authorized to conduct business in this District, has intentionally availed itself of the laws and markets within this District, does substantial business in this District, and is subject to personal jurisdiction in this District.

STATEMENT OF FACTS

12. Zoom is a cloud-based video communications platform that offers companies and consumers the ability to hold video conferences, webinars, conference

calls, and chats. Zoom claims that it can provide "video for every need," allowing users to "join anywhere, on any device."[1]

13. Businesses, healthcare organizations, educational institutions, and individuals use the Zoom platform for a variety of business and social purposes. Zoom's use has exploded recently in response to the novel-coronavirus pandemic's social-distancing requirements that are forcing more people to stay at home. "Where once it enabled client conferences or training webinars, it is now also a venue for virtual cocktail hours, Zumba classes and children's birthday parties."[2] The number of daily meeting participants across Zoom's services has increased from 10 million at the end of 2019 to 200 million now.[3]

14. Zoom's initial public offering last year was one of 2019's most successful public offerings, making Zoom's CEO, Eric Yuan, a billionaire.[4] And while the stock market has seen its first bear market since the 2008 financial crisis,[5] Zoom's share price soared,[6] that is, until recently when investors learned of its major security and privacy flaws.[7]

---

[1] Zoom Meetings & Chat, https://zoom.us/meetings (last visited April 12, 2020).

[2] Aaron Tilley and Robert McMillan, *Zoom CEO: 'I Really Messed Up' on Security as Coronavirus Drove Video Too's Appeal*, The Wall Street Journal (April 4, 2020) ("*I really messed up*"), https://www.wsj.com/articles/zoom-ceo-i-really-messed-up-on-security-as-coronavirus-drove-video-tools-appeal-11586031129?st=jmn0xqiy1ea3c63&mod=openfreereg.

[3] *Id.*

[4] *Id.*

[5] Sergei Klebnikov, *Bear Market, Dow Drops Over 1,400 Points, Ending Longest Bull Market in U.S. History*, Forbes (Mar. 11, 2020), https://www.forbes.com/sites/sergeiklebnikov/2020/03/11/bear-market-dow-drops-over-1400-points-ending-longest-bull-market-in-us-history/#6e75715c6ae4.

[6] Rupert Neate, *Zoom booms as demand for video-conferencing tech grows*, The Guardian (Mar 31, 2020), https://www.theguardian.com/technology/2020/mar/31/zoom-booms-as-demand-for-video-conferencing-tech-grows-in-coronavirus-outbreak.

[7] Wallace Witkowski, *Zoom Video stock slides as much as 15% after analyst joins in backlash on valuation fears*, Market Watch (April 6, 2020), https://www.marketwatch.com/story/zoom-video-stock-slides-as-much-as-15-after-analyst-joins-in-backlash-on-valuation-fears-2020-04-06.

15. Zoom understands that its users want their private meetings to remain private, and their personal information secured, touting its "end-to-end encryption for all meetings, role-based user security, password protection, waiting rooms, and place attendee on hold," as measures to allow users to "meet securely."[8] Zoom promises its customers that "we take security seriously and we are proud to exceed industry standards when it comes to your organizations communications."[9] It further promises that it "is committed to protecting your privacy," and claims it has "designed policies and controls to safeguard the collection, use, and disclosure of your information."[10] According to Zoom, it "places privacy and security as the highest priority in the lifecycle operations of our communications infrastructure."[11]

16. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that do not secure their personal data.[12]

17. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Zoom

---

[8] Zoom Security Guide (April 2020), https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf (last visited April 12, 2020).

[9] Security at Zoom, https://zoom.us/security (last visited April 12, 2020).

[10] *Id.*

[11] *See* Zoom Security Guide, *supra* note 8.

[12] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited April 12, 2020).

would have no reason to tout its data security and privacy efforts to their actual and potential customers.

18. As it turns out, Zoom's promises of privacy and security were false, and Zoom has been forced to walk many of these representations back as the company's meteoric rise has put a spotlight on its technologies' numerous security flaws.

19. On April 1, 2020, Zoom's Chief Executive Officer, Eric Yuan, admitted that the company had "fallen short of the community's – and our own – privacy and security expectations,"[13] acknowledging that Zoom "did not design the product with the foresight" to accommodate the number of people using and the variety of reasons it was being used. This, he said, "present[ed] us with challenges we did not anticipate when the platform was conceived."[14] On April 4, 2020, after more and more security and privacy flaws were exposed, Yuan admitted that he had "really messed up as CEO, and we need to win [users'] trust back," stating "[t]his kind of thing shouldn't have happened."[15]

A. Zoom prioritizes rapid growth over consumers' security.

20. Compared to other video-conferencing platforms, Zoom is easy to set up and use, and this ease-of-use has caused Zoom to take off while other platforms have not.[16] "But there's a downside." Zoom's ease-of-use comes at the expense of data security, as numerous security and privacy problems have been exposed in a matter of

---

[13] Eric S. Yuan, *A Message to Our Users*, Zoom Blog (April 1, 2020) ("*April 1, 2020 Zoom Blog*"), https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/.

[14] *Id.*

[15] *See I Really Messed Up*, *supra* note 2.

[16] Paul Wagenseil, *Zoom privacy and security issues: Here's everything that's wrong (so far)*, Tom's Guide (last updated April 10, 2020) ("*Tom's Guide*"), https://www.tomsguide.com/news/zoom-security-privacy-woes.

weeks.[17] The backlash against Zoom has already begun, with school districts,[18] governments,[19] and major companies like SpaceX and Google[20] banning the use of Zoom due to privacy and security concerns.

21. As detailed below, as of the filing of this Complaint, more than a dozen security and privacy problems with Zoom's technologies have come to light, exposing the company's overall lax view of data security as it rushed to get its technology to market and to the front-of-the-line. Each of these problems shows that consumers' information and privacy is at risk and that Zoom's representations of data security were false and misleading.

1. Zoom blatantly misrepresents its encryption capabilities.

22. Prior to April 2020, Zoom's website and its security white paper claimed its meetings use "end-to-end encryption"—a method of secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. "End-to-end encryption" is well known in the technology field to designate data that can be sent from one user endpoint (like a desktop, laptop, smartphone or tablet) to another endpoint where the server delivering the information

---

[17] *Id.*

[18] Sean Keane, *School districts reportedly ban Zoom over security issues*, CNET (April 6, 2020), https://www.cnet.com/news/school-districts-reportedly-ban-zoom-over-security-issues/; John Geddie, *Singapore stops teachers using Zoom app after 'very serious incidents'*, Reuters (April 9, 2020), https://www.reuters.com/article/us-zoom-video-comm-privacy-singapore-idUSKCN21S0AH.

[19] Mary Hui, *Taiwan is taking cybersecurity seriously by banning the use of Zoom in government* (April 7, 2020), https://qz.com/1834151/taiwan-government-bans-official-use-of-zoom/; Ben Lovejoy, *Governments restrict or ban the use of Zoom, as company faces lawsuit*, 9to5mac (April 8, 2020), https://9to5mac.com/2020/04/08/ban-the-use-of-zoom/; Kiran Stacey and Hannah Murphy, *US Senate tells members not to use Zoom*, ars technical (April 9, 2020), https://arstechnica.com/tech-policy/2020/04/us-senate-tells-members-not-to-use-zoom/.

[20] Munsif Vengattil, Joey Roulette, *Elon Musk's SpaceX bans Zoom over privacy concerns – memo*, Reuters (April 1, 2020), https://www.reuters.com/article/us-spacex-zoom-video-commn/elon-musks-spacex-bans-zoom-over-privacy-concerns-memo-idUSKBN21J71H?il=0; Pranav Dixit, *Google Has Banned Zoom Software From Employees' Computers, Citing Security Vulnerabilities*, BuzzFeed News (April 8, 2020), https://www.buzzfeednews.com/article/pranavdixit/google-bans-zoom?bftwnews&utm_term=4ldqpgc#4ldqpgc.

cannot decrypt the message. For example, when a user sends an Apple message from an iPhone to another iPhone user, Apple's servers help the message get from one place to another, but they can't read the content. So end-to-end encryption means that only the parties to the communication can access it, and not any middlemen that relay the communication through its servers. This is not the case with Zoom.

23. Under pressure from investigative journalists at *The Intercept*, a Zoom representative admitted that Zoom's definitions of "end-to-end" and "endpoint" are not the same as that commonly used in the technology industry.[21] The Zoom spokesperson admitted "When we use the phrase 'End to End,' in our literature, it is in reference to the connection being encrypted from Zoom end point to Zoom end point."[22] Because it holds the encryption keys, Zoom can view users' communications, and could share that information with others, for example, if presented with a warrant from law enforcement.[23]

24. Notably, Apple's FaceTime, which allows group videoconferencing, offers actual end-to-end encryption, so the technology is available and used by Zoom's competitors.[24] Of course that's what Zoom users thought they were getting based on Zoom's false representations that it too provided "end-to-end" encryption.

25. In a blog post dated April 1, 2020, Zoom's chief product officer Oded Gal admitted the company had misrepresented its level of encryption writing "we want to start by apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption."[25] He further

[21] Micah Lee, Yael Grauer, *Zoom Meeting Aren't End-To-End Encrypted, Despite Misleading Marketing*, The Intercept (Mar. 31, 2020), https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

[22] *Id.*

[23] *See Tom's Guide*, *supra* note 16.

[24] *Id.*

[25] Oded Gal, *The Facts Around Zoom and Encryption for Meetings/Webinars*, Zoom Blog (April 1, 2020), https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/.

acknowledged: "We recognize that there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it."[26]

26. Not only was Zoom misleading consumers about its "end-to-end encryption" capabilities, but it also falsely represented the quality of its encryption algorithm. Zoom says it uses AES-256 encryption to encode video and audio data traveling between Zoom servers and Zoom users, but researchers at The Citizen Lab at the University of Toronto reported on April 3, 2020, that Zoom actually uses a weaker single AES-128 key in a home-grown "ECB mode", which is not as secure as promised.[27] "Even worse, Zoom uses an in-house implementation of encryption algorithm that preserves patterns from the original file. It's as if someone drew a red circle on a gray wall, and then a censor painted over the red circle with a whi[t]e circle. You're not seeing the original message, but the shape is still there."[28]

27. In a blog post on April 3, 2020, Zoom's CEO Eric Yuan acknowledged the encryption issue but said only that "we recognize that we can do better with our encryption design" and "we expect to have more to share on this front in the coming days."[29]

2. The Chinese Government may have access to private information.

28. The Citizen Lab report also revealed that several Zoom servers in China were issuing encryption keys to Zoom users even when all participants in the meeting were in North America.[30]

---

[26] *Id.*

[27] Bill Marczak and John Scott-Railton, *Move Fast and Roll Your Own Crypto, A Quick Look at the Confidentiality of Zoom Meetings*, The Citizen Lab (April 3, 2020) ("*The Citizen Lab*"), https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/.

[28] *See Tom's Guide*, *supra* note 16.

[29] Eric S. Yuan, *Response to Research From University of Toronto's Citizen Lab Zoom Blog* (April 3, 2020) ("*April 3, 2020 Zoom Blog*"), https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/.

[30] *The Citizen Lab*, *supra* note 27.

29. While Zoom is a Silicon Valley-based company, it owns three companies in China through which at least 700 employees are paid to develop Zoom's software. According to the Citizen Lab: "This arrangement is ostensibly an effort at labor arbitrage: Zoom can avoid paying US wages while selling to US customers, thus increasing their profit margin. However, this arrangement may make Zoom responsive to pressure from Chinese authorities."[31]

30. Since Zoom servers can decrypt Zoom meetings while falsely claiming "end-to-end encryption", and Chinese authorities can compel operators of Chinese servers to hand over data, "the Chinese government might be able to see your Zoom meetings."[32]

31. In his April 3, 2020 blog post, Zoom's CEO Eric Yuan admitted this was a problem: "In our urgency to come to the aid of people around the world during this unprecedented pandemic, we added server capacity and deployed it quickly — starting in China, where the outbreak began. In that process, we failed to fully implement our usual geo-fencing best practices. As a result, it is possible certain meetings were allowed to connect to systems in China, where they should not have been able to connect."[33] Zoom claims to have fixed this problem.[34]

3. Zoom meeting recordings can be found online.

32. Zoom meeting recordings saved to the meeting host's computer are automatically assigned a certain type of default file name. Patrick Jackson, the technology chief of the privacy-software company Disconnect and a former researcher for the National Security Agency, searched unprotected cloud servers to see if anyone

[31] *Id.*

[32] *See Tom's Guide*, *supra* note 16.

[33] *April 3, 2020 Zoom Blog*, *supra* note 29.

[34] *Id.*

had uploaded Zoom recordings and found more than 15,000 unprotected examples, according to The Washington Post.[35]

33. Videos viewed by The Washington Post included "one-on-one therapy sessions; a training orientation for workers doing telehealth calls that included people's names and phone numbers; small-business meetings that included private company financial statements; and elementary school classes, in which children's faces, voices and personal details were exposed. Many of the videos include personally identifiable information and deeply intimate conversations, recorded in people's homes. Other videos include nudity, such as one in which an aesthetician teaches students how to give a Brazilian wax."[36]

34. As explained by The Post, "because Zoom names every video recording in an identical way, a simple online search can reveal a long stream of videos elsewhere that anyone can download and watch."[37]

35. Jackson said Zoom could do a better job at cautioning people to protect their videos. Zoom could also help by implementing design tweaks, such as naming videos in an unpredictable way to make them harder to find.[38] In designing their service, Zoom's engineers bypassed these common security features. "That style of operating simplicity has powered Zoom to become the most popular video-chat application in the United States, but it has also frustrated some security researchers who believe such shortcuts can leave users more vulnerable to hacks or abuse."[39]

---

[35] Drew Harwell, *Thousands of Zoom video calls left exposed on open Web*, The Washington Post (April 3, 2020), https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/.

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

4. Zoom meetings can be accessed by malicious, uninvited participants.

36. Due to Zoom's lax privacy controls, anyone can join a public Zoom meeting if they know the meeting number, and then use the file-share photo to post shocking images, or make disruptive sounds in the audio—a phenomenon dubbed "Zoombombing". The uses of Zoombombing by nefarious actors are as varied as the imaginations of the hackers themselves. The incidents started as pranks or trolling, and have risen to the level of hate speech and harassment. The host of the Zoom meeting can mute or even kick out troublemakers, but they can come right back with new user IDs. Zoom made such so-called "Zoombombs" easy because its default settings did not require users to have a password to join.[40]

37. An analysis by *The New York Times* found "153 Instagram accounts, dozens of Twitter accounts and private chats, and several active message boards on Reddit and 4Chan where thousands of people had gathered to organize Zoom harassment campaigns, sharing meeting passwords and plans for sowing chaos in public and private meetings."[41]

38. For example, on April 6, 2020, the first day the San Diego school district started its distance learning program, a high school biology class was Zoombombed. A person with the username "Dee Znuts" wore a red ski mask and a red sweatshirt during the meeting and made several hand signs in front of his computer's camera, screenshots of the Zoom meeting show. Another unknown person displayed a photo of a bearded man on their camera and displayed a caption that claimed the biology teacher "Hates BlackPeople." And a third unknown person typed the n-word in the group chat.[42]

---

[40] Taylor Lorenz and Davey Alba, *'Zoombombing' Becomes a Dangerous Organized Effort*, The New York Times (April 3, 2020), https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html.

[41] *Id.*

[42] Kristen Taketa, *San Diego 'Zoombombing' incident highlights need for schools to use safety controls*, The San Diego Union-Tribune (April 8, 2020), https://www.sandiegouniontribune.com/news/education/story/2020-04-08/san-diego-zoombombing-incident-highlights-need-for-schools-to-use-safety-controls.

39. On March 29, 2020, during a call among members of the Concordia Forum, a global network of Muslim leaders, about maintaining spirituality and wellness during the coronavirus crisis, a cursor began to draw a racial slur across one of the slides. The infiltrator then began to screen-share a pornographic video while repeating the racial epithet verbally.[43]

40. Harassers have begun to use every feature of Zoom's platform for abuse, including using the app's custom background feature to project a GIF of a person drinking to participants in an Alcoholics Anonymous meeting, and its annotation feature to write racist messages in a meeting of the American Jewish Committee in Paris.[44]

41. The frequency and reach of the incidents on Zoom prompted the F.B.I. to issue a warning on March 30, 2020, singling out Zoom and stating that it had "received multiple reports of conferences being disrupted by pornographic or hate images and threatening language" nationwide.[45]

42. To avoid Zoombombing, Zoom advises meeting hosts to set up "waiting rooms." A waiting room keeps participants on hold until a host lets them in, either all at once or one at a time. However, The Citizen Lab said it found a serious security issue with Zoom waiting rooms, and advised hosts and participants to not use them for now. The Citizen Lab is not disclosing the details of the waiting room flaw because the issue presents a risk to users, and it did not want the issue to be abused before Zoom could fix it, but has told Zoom of the flaw.[46]

43. Moreover, nefarious actors can easily find open meetings to harass users by rapidly cycling through possible Zoom meeting IDs, a security researcher told

---

[43] *Id.*

[44] *Id.*

[45] Kristen Setera, *FBI Wans of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*, FBI Boston (March 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[46] *The Citizen Lab*, *supra* note 27.

security blogger Brian Krebs.[47] The researcher got past Zoom's meeting-scan blocker by running queries through Tor, which randomized his IP address. It's a variation on "war driving" by randomly dialing telephone numbers to find open modems in the dial-up days. The researcher told Krebs that he could find about 100 open Zoom meetings every hour with the tool, and that "having a password enabled on the [Zoom] meeting," which is not the default, "is the only thing that defeats it."

5. Zoom meeting chats don't stay private and are not secure.

44. During meetings, Zoom ostensibly allows users to message privately amongst each other through a private window in the meeting's chat app. But unbeknownst to those users, their conversations are not private and will be visible in the end-of-meeting transcript the host receives, thus allowing the host to see the discussion had during the supposedly private side-meeting.[48]

45. In addition, during side chats, participants can send text-based messages and post web links. But until recently, Zoom made no distinction between regular web addresses and a different kind of remote networking link called a Universal Naming Convention (UNC) path. That left Zoom chats vulnerable to attack.[49]

46. If a malicious Zoombomber slipped a UNC path to a remote server that he controlled into a Zoom meeting chat, an unwitting participant could click on it. The participant's Windows computer would then try to reach out to the hacker's remote server specified in the path and automatically try to log into it using the user's Windows username and password. The hacker could capture the password "hash" and decrypt it, giving him access to the Zoom user's Windows account.[50] The security firm Seekurity,

---

[47] Brian Krebs, *'War Dialing' Tool Exposes Zoom's Password Problems*, Krebs on Security (April 2, 2020), https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/.

[48] *See* https://twitter.com/MoriartyCR/status/1245875244302204936 (last visited April 12, 2020).

[49] *See Tom's Guide*, *supra* note 16.

[50] *Id.*

discovered this same flaw would let a hacker inject malware onto a Windows user's computer.[51] Zoom claims to have fixed this problem.[52]

6. Zoom leaks users' email addresses and profile photos.

47. As one tech writer put it, Zoom "seems to be leaking data like a colander draining pasta."[53] A report from Vice Media's *Motherboard* exposed that a default Zoom setting, the "Company Directory" setting, "automatically adds other people to a user's lists of contacts if they signed up with an email address that shares the same domain. This can make it easier to find a specific colleague to call when the domain belongs to an individual company. But multiple Zoom users say they signed up with personal email addresses, and Zoom pooled them together with thousands of other people as if they all worked for the same company, exposing their personal information to one another."[54]

48. One Zoom user, Barend Gehrels, provided *Motherboard* with a redacted screenshot of him logged into Zoom with nearly 1000 different accounts listed in the "Company Directory" section, all people he did not know. "If you subscribe to Zoom with a non-standard provider (I mean, not Gmail or Hotmail or Yahoo etc.), then you get insight to ALL subscribed users of that provider: their full names, their mail addresses, their profile picture (if they have any) and their status. And you can video call them," Gehrels said.

49. "I just had a look at the free for private use version of Zoom and registered with my private email. I now got 1000 names, email addresses and even pictures of

---

[51] *Id.*

[52] *See April 1, 2020 Zoom Blog*, *supra* note 13.

[53] Henry T. Casey, *Zoom may be leaking your email address: What to do now*, Tom's Guide (April 1, 2020), https://www.tomsguide.com/news/zoom-may-be-leaking-your-email-address-what-to-do-now.

[54] Joseph Cox, *Zoom is Leaking Peoples' Email Addresses and Photos to Strangers*, Motherboard Tech by Vice (April 1, 2020) ("*Zoom is leaking*"), https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos.

people in the company Directory. Is this intentional?," one user recently tweeted along with a screenshot.[55]

50. A Zoom user affected by this issue must contact Zoom to request their domain be removed from the Company Directory feature.[56]

7. Zoom's accounts can be hijacked.

51. On April 10, 2020, *Tom's Guide* reported that Zoom paid a Kurdish security researcher a "bug bounty"—a reward for finding a serious flaw—after he discovered and privately reported a way for anyone to easily hijack any existing Zoom account if the account email address was known or successfully guessed.[57] The researcher described how if he tried to log into the Zoom website with a Facebook account, Zoom would ask for the email address associated with that Facebook account. Then Zoom would open a new webpage notifying him that a confirmation email message had been sent to that email address.[58]

52. The URL of the notification webpage would have a unique identification tag in the address bar, for example, "zoom.com/signup/123456XYZ". When the researcher received and opened the confirmation email message sent by Zoom, he clicked on the confirmation button in the body of the message. This took him to yet another webpage that confirmed his email address was now associated with a new account. But then, the researcher noticed that the unique identification tag in the Zoom confirmation webpage's URL was identical to the first ID tag, in the example above, "zoom.com/confirmation/123456XYZ".[59]

53. The matching ID tags, one used before confirmation and the other after confirmation, meant that the researcher could have avoided receiving the confirmation

---

[55] *See* https://twitter.com/JJVLebon/status/1242175850306580486 (last visited April 12, 2020).

[56] *See Zoom is leaking*, *supra* note 54.

[57] *See Tom's Guide*, *supra* note 16.

[58] *Id.*

[59] *Id.*

email, and clicking on the confirmation button, altogether. In fact, he could have entered *any* email address into the original signup form. Then he could have copied the ID tag from the resulting Zoom notification page and pasted the ID tag into an already existing Zoom account-confirmation page, giving him access to any Zoom account created using the targeted email address. Even if the user already linked their account with a Facebook account, Zoom automatically unlinked it and linked it with the attacker Facebook account.[60]

54. And, as explained above, because Zoom lets anyone using a company email address view all other users signed up with the same email domain, *e.g.* "company.com", a criminal hacker could use this method to steal *all* of a given company's Zoom accounts. Zoom purportedly fixed this flaw after the researcher relayed it to Zoom.[61]

8. Zoom's software mimics malware to gain access to Apple Macintosh operating systems (OS).

55. For users accessing Zoom on an Apple device, Zoom uses hacker-like methods to bypass normal macOS security precautions. As security researcher Felix Seele explains: the Zoom "application installs itself on Macs by working around Apple's regular security, demonstrating behavior commonly associated with malware."[62] Zoom's Mac app installer uses pre-installation scripts and displays a password dialog pretending to be an OS prompt. Seele explained: "While this practice is nice from Zoom's perspective and for usability, it violates Mac user expectations. If a Mac user opens a pkg file, they expect to click through it and give their consent before installation. Instead, Zoom performs this operation instantly without another

[60] *Id.*

[61] *Id.*

[62] Felix Seele, *Good Apps Behaving Badly, Dissecting Zoom's macOS Installer Workaround*, VMray Blog (April 1, 2020), https://www.vmray.com/cyber-security-blog/zoom-macos-installer-analysis-good-apps-behaving-badly/.

confirmation. An analogy would be like putting car keys into the ignition, but instead of only the radio and the engine starting up, the car starts driving on its own."[63]

56. Seele stated further, "[t]he second and more severe problem is the password prompt. There is no need to fake this message, rather than explicitly state what operations Zoom is performing. Instead, Zoom impersonates the system and attempts to 'social-engineer' the user into entering his password." Seele noted "[t]his is not strictly malicious but very shady and definitely leaves a bitter aftertaste. The application is installed without the user giving his final consent and a highly misleading prompt is used to gain root privileges. The same tricks that are being used by macOS malware."[64] After Zoom received complaints about these practices, Zoom released a new version of Zoom client for macOS that purportedly removes the challenged techniques.[65]

9. Zoom software can be easily corrupted.

57. Secure software typically has built-in anti-tampering mechanisms to make sure that applications do not run code that has been altered by a third party. Zoom has such anti-tampering mechanisms in place, however, Zoom's anti-tampering mechanisms themselves are not protected from tampering.[66]

58. A British computer student who calls himself "Lloyd," showed how Zoom's anti-tampering mechanism can easily be disabled, or even replaced with a malicious version that hijacks the application, allowing malware already present on a computer to use Zoom's own anti-tampering mechanism to tamper with Zoom.

---

[63] *Id.*

[64] *Id.*

[65] *See Tom's Guide*, *supra* note 16.

[66] *Tampering with Zoom's Anti-Tampering Library*, lloydlabs (April 3, 2020), https://blog.syscall.party/post/tampering-with-zooms-anti-tampering-library/.

Criminals could also create fully working versions of Zoom that have been altered to perform malicious acts.[67]

10. Hackers are finding and selling vulnerabilities in Zoom's software and hardware.

59. Information-security researchers have discovered several Zoom "zero-day" exploits. "Zero-days" are exploits for software vulnerabilities that the software maker does not know about, and hence has "zero days" to prepare before the exploits appear.[68]

60. Hackers around the world are researching Zoom to uncover its most severe security vulnerabilities, and finding plenty, which they can then sell to the highest bidder, be it to a government or private hackers. "Depending on what software they're in, they can be sold for thousands or even millions of dollars."[69] For example, as explained in more detail below, *Motherboard* found that the Zoom's iOS app shares information with Facebook, and leaks people's email addresses and photos.

61. In addition, another security researcher found two new bugs that can be used to take over a Zoom user's computer.[70] Patrick Wardle, a former NSA hacker publicly disclosed these bugs to warn users. "The two bugs, Wardle said, can be launched by a local attacker—that's where someone has physical control of a vulnerable computer. Once exploited, the attacker can gain and maintain persistent access to the innards of a victim's computer, allowing them to install malware or spyware."[71] As described above, Zoom uses a "shady" technique—one that is also used by Mac

---

[67] *See Tom's Guide*, *supra* note 16.

[68] *Id.*

[69] Lorenzo Fransceschi-Bicchierai, *Interest in Zoom Zero-Day Hacks is 'Sky High' as Meeting Move Online*, Vice (April 8, 2020), https://www.vice.com/en_us/article/akwpxp/zoom-hacks-zero-day-exploits.

[70] Zack Whittaker, *Ex-NSA hacker drops new zero-day doom for Zoom*, TechCrunch (April 1, 2020), https://techcrunch.com/2020/04/01/zoom-doom/.

[71] *Id.*

malware—to install the Mac app without user interaction. Wardle found that a local attacker with low-level user privileges can inject the Zoom installer with malicious code to obtain the highest level of user privileges, known as "root." Those root-level user privileges mean the attacker can access the underlying macOS operating system, which are typically off-limits to most users, making it easier to run malware or spyware without the user noticing.[72]

62. The second bug exploits a flaw in how Zoom handles the webcam and microphone on Macs. Zoom, like any app that needs the webcam and microphone, first requires consent from the user. But Wardle said an attacker can inject malicious code into Zoom to trick it into giving the attacker the same access to the webcam and microphone that Zoom already has. Once Wardle tricked Zoom into loading his malicious code, the code will "automatically inherit" any or all of Zoom's access rights, he said—and that includes Zoom's access to the webcam and microphone. "No additional prompts will be displayed, and the injected code was able to arbitrarily record audio and video," wrote Wardle. Wardle said, "if you care about your security and privacy, perhaps stop using Zoom."[73]

11. The Zoom installer is bundled with malware.

63. Researchers at Trend Micro discovered a version of the Zoom installer that has been bundled with cryptocurrency-mining malware, *i.e.* a coin-miner. The coin-miner will ramp up users' computers' central processor unit, and its graphics card if there is one, to solve mathematical problems in order to generate new units of cryptocurrency.

64. Consumers can get infected with this malware if they click on links in emails, social media posts, or pop-up messages that offer to install Zoom on their computers.

[72] *Id.*

[73] *Id.*

B. Zoom discloses consumers' personally-identifying information to third-parties like Facebook without authorization.

65. In addition to Zoom's recklessness in rushing its product to market with easily exploitable security flaws as detailed above, Zoom also engaged in the unauthorized disclosure of users' personally-identifying information ("PII") in violation of their privacy rights.

66. On March 26, 2020, *Motherboard* reported that the iOS version of the Zoom mobile app was sending customer PII to Facebook without customer authorization or customer consent—even if the customer did not have a Facebook account.[74]

67. Upon downloading and opening the app, Zoom would connect to Facebook's Graph API. The Graph API is the main way that app developers get data in or out of Facebook.[75]

68. The Zoom app would notify Facebook when the user opened the app, details on the user's device—such as the model, time zone and city from which they were connecting, which phone carrier they were using—and a unique advertiser identifier created by the user's device which companies can use to target a user with advertisements.[76]

69. The disclosure of the unique advertiser identifier (also known as an "IDFA," or, "Identifier for Advertisers") is particularly invasive because each device is assigned a unique one, and thus they are tied to each individual user. IDFAs are unique, alphanumeric strings that are used to identify an individual device—and the individual who uses that device—to track and profile the user.

---

[74] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Accoun*t, Motherboard Tech by Vice (Mar. 26, 2020), https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.

[75] *Id.*

[76] *Id.*

70. Advertisers use the IDFA to track data so that they can deliver customized advertising. The IDFA is used for tracking and identifying a user, allowing whoever is tracking it to identify when users interact with mobile advertising and whether specific users click advertisements.[77] An IDFA is similar to a cookie in that it allows advertisers to know that a specific iPhone user is looking at a specific publication so that it can serve an ad targeting that user.[78] Key digital privacy and consumer groups have described why and how an identifier like an IDFA facilitates targeted advertising and is not "anonymous" at all, even though the IDFA itself does not contain the user's name:

> With the increasing use of new tracking and targeting techniques, any meaningful distinctions between personal and so-called non-personal information have disappeared. This is particularly the case with the proliferation of personal digital devices such as smart phones and Internet-enabled game consoles, which are increasingly identified with individual users, rather than families. This means that marketers do not need to know the name, address, or email of a user in order to identify, target and contact that particular user.[79]

71. The other information shared by Zoom can also allow individual users to be identified individually. Details about the type of device (*e.g.*, iPhone or iPad), details about its software (iOS), its network carrier (*e.g.*, Spring, T-Mobile, AT&T), and the location of the user, when taken together, provide a high level of detail about the user. In combination with the IDFA, the information shared is extremely detailed and can be used to identify the user personally.

---

[77] *See, e.g.*, Adjust Mobile Measurement Glossary, https://www.adjust.com/glossary/idfa/.

[78] Jim Edwards, *Apple Wants More Advertisers to Use its iPhone Tracking System*, Business Insider (June 13, 2013), https://www.businessinsider.com/apples-idfa-and-ifatracking-system-2013-6.

[79] Comments of The Center for Digital Democracy, *et al*., FTC, In the Matter of Children's Online Privacy Protection Rule at 13-14 (Dec. 23, 2011), https://www.democraticmedia.org/sites/default/files/COPPA%20Rule%20Comments%20of%20Children%27s%20Privacy%20Advocates.pdf (last visited April 12, 2020).

72. Advertisers use this information to learn more about users, including when and how they use the Zoom platform, along with their behaviors, demographics, and preferences, so that they can serve them with tailored and targeted advertising. Thereafter, anyone with access to the IDFA can track the effectiveness of those advertisements after the user sees them.

73. This information has tremendous economic value. Moreover, the disclosure of this identifying information makes people more vulnerable to voter fraud, medical fraud, phishing, and other identity-based harms. But most importantly, the ability to de-anonymize and analyze user data allows parties to personally and psychologically target Zoom's customers with great precision.

74. The information shared by Zoom allows Facebook and any other recipient to spy on Zoom's customers and deliver targeted advertisements to them as they browse the Internet, as well as to determine the effectiveness of the advertisements.

75. Zoom's data-sharing activity was not visible to the user, who simply saw the Zoom app interface. Thus, Zoom users had no opportunity to express or withhold consent to Zoom's misconduct.

76. Since they could not detect this activity from the app itself, and Zoom does not allow them to monitor whether it is sharing their PII, users of Zoom have no reasonable way of knowing whether, when they open the Zoom app, their PII will be safeguarded or disclosed without their consent.

77. Zoom users had no reason to expect that Zoom would transmit their PII to Facebook, a completely unrelated social networking company, or any other undisclosed third party, to be used to track and target them for advertising.

1. Zoom failed to obtain customer authorization before sharing PII.

78. Zoom completely failed to inform its users that, as they opened the iOS version of the Zoom app, Zoom was surreptitiously disclosing their PII to Facebook (and, upon information and belief, other third parties) for use for targeted advertising.

79. Zoom's Privacy Policy claims that Zoom is "committed to protecting your privacy and ensuring you have a positive experience on our websites and when you use our products and services."[80]

80. Prior to March 29, 2020, Zoom's Privacy Policy disclosed that it collected certain categories of personal data about users, including "[i]nformation commonly used to identify you, such as your name, user name, physical address, email address, phone numbers, and other similar identifiers"; "information about your job, such as your title and employer"; "credit/debit card or other payment information"; "Facebook profile information (when you use Facebook to log-in to our Products or to create an account for our Products)"; "General information about your product and service preferences"; "Information about your device, network, and internet connection, such as your IP address(es), MAC address, other device ID (UDID), device type, operating system type and version, and client version"; "Information about your usage of or other interaction with our Products"; and "[o]ther information you upload, provide, or create while using the service[.]"[81] Zoom claimed that it collected this information "to provide you with the best experience with our products."[82]

81. This was the only reference to Facebook in its Privacy Policy, and Zoom did not disclose that it was not only itself collecting information from Facebook, but it was also disclosing information about its users *to* Facebook.

82. While Zoom told users that its "advertising partners (*e.g.*, Google Ads and Google Analytics) automatically collect some information" about users, Zoom omitted that Facebook (or any other third party) was collecting that information and did not explain the level of detail that Zoom shared:

---

[80] *See* Zoom March 29, 2020 Privacy Policy, https://zoom.us/privacy (last visited April 12, 2020); *see also* Zoom March 18, 2020 Privacy Policy, available at: https://web.archive.org/web/20200325143843/https://zoom.us/privacy (last visited April 12, 2020).

[81] *See id*. Zoom March 18, 2020 Privacy Policy.

[82] *Id.*

> Zoom, our third-party service providers, and advertising parties (e.g., Google Ads and Google Analytics) automatically collect some information about you when you use our Products, using methods such as cookies and tracking technologies (further described below). Information automatically collected includes Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referrer URL, exit pages, the files viewed on our site (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data. We use this information to offer and improve our services, trouble shoot, and to improve our marketing efforts.

83. Thus, Zoom never disclosed that it was providing third parties like Facebook, which are not "advertising parties" like Google Ads and Google Analytics, with sufficient PII to actually identify users and track their engagement with online advertising.

84. In fact, Zoom specifically promised users that "we do not allow any third parties access to any Personal Data we collect in the course of providing services to users. We do not allow third parties to use any Personal Data obtained from us for their own purposes, unless it is with your consent (e.g., when you download an app from the Marketplace). So in our humble opinion, we don't think most of our users would see us as selling their information, as that practice is commonly understood."[83]

85. Zoom violated its promises to its customers when it shared their PII without their authorization or consent. And by disclosing Plaintiffs' and the Class Members' PII with third parties like Facebook to assist in profiling them and tracking them across multiple online platforms, particularly after failing to obtain their permission to do so, Zoom breached their expectations of privacy.

2. Zoom's conduct violated its users' privacy by sharing their PII.

86. Zoom's conduct violated its users' privacy. The ability to serve targeted advertisements to (or otherwise profile) a specific user does not turn on the ability to obtain the kinds of PII with which most consumers are familiar—name, email address,

[83] *Id.*

etc. Instead, it is accomplished through the surreptitious collection and disclosure of identifiers like the IDFA and device information shared by Zoom, which are used to build robust online profiles. But consumers do not want companies like Zoom to share their PII with third parties for advertising purposes without first obtaining their express consent.

87. A 2014 report by the Senate Committee on Homeland Security and Governmental Affairs entitled "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy" also highlights this concern in light of ordinary consumers' lack of awareness of these invasive practices and their inability to prevent them:

> Although consumers are becoming increasingly vigilant about safeguarding the information they share on the Internet, many are less informed about the plethora of information created about them by online companies as they travel the internet. A consumer may be aware, for example, that a search engine provider may use the search terms the consumer enters in order to select an advertisement targeted to his interests. Consumers are less aware, however, of the true scale of the data being collected about their online activity. A visit to an online news site may trigger interactions with hundreds of other parties that may be collecting information on the consumer as he travels the web. . . . The sheer volume of such activity makes it difficult for even the most vigilant consumer to control the data being collected or protect against its malicious use.

88. Consumers prefer to keep their private information private: in a Pew Research Center study, nearly 800 Internet and smartphone users were asked the question, "How much do you care that only you and those you authorize should have access to information about where you are located when you use the internet?" 54% of adult Internet users responded "very important," 16% responded "somewhat important," and 26% responded "not too important."[84]

[84] Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden, *Anonymity, Privacy, and Security Online, Pew Research Center 7* (Sept. 5, 2013), https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/.

89. The same study reported that 86% of Internet users have tried to be anonymous online and have taken at least one step to try to mask their behavior or avoid being tracked.

90. Smartphone owners are especially careful when it comes to these behaviors. Approximately half of smartphone owners have cleared their phone's browsing or search history, while a third have turned off the location tracking feature on their phone due to concerns over who might access that information.[85]

91. Another study by the Pew Research Center found that 68% of adults were "not ok with" being targeted with online ads "because I don't like having my online behavior tracked and analyzed." Less than a third responded that they were "okay with it."[86]

92. Yet another study suggested that "if Americans could vote on behavioral targeting today, they would shut it down," finding that 66% of 1000 polled individuals over the age of 18 did not want to receive targeted advertising—and when they were told that such advertising was "based on following them on other websites they have visited," the percentage of respondents rejecting targeted advertising increased to 84%.[87]

93. The upshot is that "there's something unnatural about the kind of targeting that's become routine in the ad world . . . something taboo, a violation of norms we consider inviolable. . . . [T]he revulsion we feel when we learn how we've been

---

[85] Jan Lauren Boyles, Aaron Smith and Mary Madden, *Privacy and Data Management on Mobile Devices, Pew Research Center*, (Sept. 5, 2012), https://www.pewresearch.org/internet/2012/09/05/privacy-and-data-management-on-mobile-devices/.

[86] Kristen Purcell, Joanna Brenner and Lee Rainie, *Search Engine Use*, Pew Research Center (March 9, 2012), https://www.pewresearch.org/internet/2012/03/09/search-engine-use-2012/.

[87] Joseph Turow, *et al.*, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 2009), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers.

algorithmically targeted, the research suggests, is much the same as what we feel when our trust is betrayed in the analog world."[88]

94. The sharing of PII for advertising purposes with Facebook, in particular, is especially egregious given the serious defects in Facebook's handling of consumer information. Facebook's entire business model is premised on sharing personal information and content with third parties for advertising purposes. And Facebook has acknowledged that it shares personal information of Facebook users with app developers and advertisers, who make billions of dollars from monetizing data.[89]

95. Numerous lawsuits are currently pending against Facebook regarding its disclosure of significant quantities of user information to third parties without their consent, and Facebook has faced enforcement action from the Federal Trade Commission and Congressional investigation regarding its misuse of user data.[90]

96. But even Facebook required Zoom to share the fact that it was disclosing users' PII with Facebook. Facebook's Business Tools terms of use state that if a company like Zoom is using Facebook's software development kit, "you further represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the customer data collection, sharing, and usage."[91]

97. Facebook further states that apps must explain that "third parties, including Facebook, may collect or receive information from [the app] and other apps that use that information to provide measurement services and targeted ads," and include links showing "how and where users can opt-out."[92] Zoom did not make these disclosures,

---

[88] Sam Biddle, *You Can't Handle the Truth about Facebook Ads, New Harvard Study Shows*, The Intercept (May 9, 2018), https://theintercept.com/2018/05/09/facebook-ads-tracking-algorithm/.

[89] *See, e.g.*, Josh Constine, *Facebook now has 2 billion monthly users … and responsibility*, TechCrunch (June 27, 2017), https://techcrunch.com/2017/06/27/facebook-2-billion-users/.

[90] *See, e.g., In re: Facebook*, F.T.C. No. 092-3184, Case No. 19-cv-2184 (D.D.C.); *In re: Facebook, Inc. Consumer Privacy User Profile Litig.*, Case No. 18-md-02843-VC (N.D. Cal.).

[91] Facebook Business Tools Terms, https://www.facebook.com/legal/technology_terms (last visited April 12, 2020).

[92] *Id.*

provide a link to Facebook's data collecting activity, or give users the opportunity to opt out.

98. Thus, Zoom's conduct in sharing customers' PII with unauthorized third parties like Facebook in order to assist in the tracking and profiling of them across multiple platforms was an egregious breach of their privacy, trust and of social norms.

99. Had consumers including Plaintiffs known the truth about Zoom's information sharing practices—that Zoom would share their PII without their consent—they would not have entrusted their PII to Zoom and would not have been willing to download and use, pay for, or pay as much for, the Zoom mobile application. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with Zoom because they paid for services, either through PII or a combination of their PII and money, they expected but did not receive.

C. Zoom suffered a data breach.

100. In addition to the numerous privacy issues described above, Zoom has also apparently suffered a data breach exposing users' personal information. On April 1, 2020, "an actor in a popular dark web forum posted a link to a collection of 352 compromised Zoom accounts," a spokesperson for the Israeli cybersecurity firm Sixgill, which specializes in monitoring underground criminal activity, wrote in an email. "In comments on this post, several actors thanked him for the post, and one revealed intentions to troll the meetings."[93]

101. Sixgill said these links included email addresses, passwords, meeting IDs, host keys and names, and the type of Zoom account. According to Sixgill, "one belonged to a major U.S. healthcare provider, seven more to various educational institutions, and one to a small business." However, most of the compromised accounts

[93] Ethan Wolff-Mann, *Hackers are posting verified Zoom accounts on the dark web*, Yahoo Finance (April 6, 2020), https://finance.yahoo.com/news/hackers-are-posting-verified-zoom-accounts-on-the-dark-web-161442319.html.

were for personal use.[94] The full extent of the number of accounts and types of information compromised is still unknown.

102. This type of breach can have a host of negative consequences, including setting up Zoom users as targets for extortion. For example, in April 2020 there were reports of a recent surge of "sextortion" emails whereby "where cybercriminals email you out of the blue to claim that they've implanted malware on your computer, and have therefore been able to keep tabs on your online activity. The crooks go on to claim that they've taken screenshots of you looking at a porn site – along with video recorded from your webcam. They say they've put the screenshots and the webcam footage side-by-side to create an embarrassing video that they're going to send to your friends and family…unless you pay them blackmail money, usually somewhere from $1,500 to $4,000". [95] Many individuals fall for the scam because the extortion email contains the user's actual email address and password, which lends a degree of legitimacy to the extortion attempt.[96] Zoom's breach is especially conducive to these types of scams because it involves software that requires the use of a webcam.

103. Additionally, security researchers recently uncovered another database on a "dark web" forum containing more than 2,300 compromised Zoom credentials, including "usernames and passwords for Zoom accounts – including corporate accounts belonging to banks, consultancy companies, educational facilities, healthcare providers

---

[94] *Id.*

[95] Paul Ducklin, *Sextortion emails and porn scams are back – don't let them scare you!*, naked security by SOPHOS (April 10, 2020), https://nakedsecurity.sophos.com/2020/04/10/sextortion-emails-and-porn-scams-are-back-dont-let-them-scare-you/; *see also* Brian Krebs, *Sextortion Scam Uses Recipient's Hacked Passwords*, Krebs on Security (July 12, 2018), https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/.

[96] *See id.*

and software vendors. Some of the accounts included meeting IDs, names and host keys in addition to credentials."[97]

104. The researches note that these types of compromised accounts "could give cybercriminals access to web conference calls, where sensitive files, intellectual property data and financial information are shared. Cybercriminals can also use these credentials for social-engineering purposes, ultimately leading to attacks like business email compromise efforts." [98] It is currently unclear whether these stolen credentials were obtained from a breach of Zoom's systems or another third-party attack.

105. As the result of the wide variety of injuries that can be traced to Zoom's unlawful conduct, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, purchasing services they would not have otherwise paid for and/or paying more for services than they otherwise would have paid, had they known the truth about Zoom's sub-standard data security and privacy practices; losing the value of the explicit and implicit promises of data security and privacy; loss of the right to privacy; and costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the loss of privacy and data security stemming from Zoom's inadequate privacy and data security.

106. Further, Zoom continues to hold Plaintiffs' and Class Members' PII, and, therefore, they have an interest in ensuring that their PII is secured and not subject to risk of theft, exposure, and disclosure.

[97] Lindsey O'Donnell, *Compromised Zoom Credentials Swapped in Underground Forums* (April 10, 2020), threatpost.com, https://threatpost.com/compromised-zoom-credentials-underground-forums/154616/.

[98] *Id.*

CLASS ALLEGATIONS

107. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiffs seek certification of two nationwide classes defined as follows:

Nationwide Class A: All persons in the United States who purchased Zoom.

Nationwide Class B: All persons in the United States who used the Zoom app for iOS.

108. Pursuant to Rule 23, and in the alternative to the Nationwide Classes, Plaintiffs assert claims under the law of California on behalf of two separate statewide subclasses defined as follows:

California Subclass A: All persons in the state of California who purchased Zoom.

California Subclass B: All persons in the state of California who used the Zoom app for iOS.

109. Excluded from each of the above Classes is Zoom, any entity in which Zoom has a controlling interest, and Zoom's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded from the Classes and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

110. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

111. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

112. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Classes are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, the proposed Classes includes potentially hundreds of

thousands of individuals. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

113. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The predominating common questions include:

a. Whether Zoom had a duty to use reasonable data security and privacy measures;
b. Whether Zoom's security and privacy measures were reasonable in light of known legal requirements;
c. Whether Zoom's security and privacy measures were reasonable in light of known industry standards;
d. Whether Zoom owed duties to Plaintiff Murphy and Class Members to disclose that it was sharing their PII with third parties, including Facebook;
e. Whether Zoom owed duties to Plaintiffs and Class Members to disclose that its products and services did not maintain adequate data and privacy security;
f. Whether Zoom's acts and practices complained of herein amount to egregious breaches of social norms;
g. Whether Zoom violated Plaintiffs' and Class Members' privacy rights;
h. Whether Plaintiffs and the Class Members were harmed;
i. Whether Zoom formed implied contracts with Plaintiffs and Class Members;
j. Whether Zoom breached implied contracts with Plaintiffs and the Class Members;
k. Whether Zoom's conduct was unfair;

l. Whether Zoom's conduct was fraudulent;

m. Whether Zoom's conduct was unlawful;

n. Whether Zoom omitted or misrepresented material facts regarding the PII of Plaintiff Murphy and Class Members it shared with third parties, including Facebook;

o. Whether Zoom omitted or misrepresented material facts regarding the level or quality of the security of its products and services;

p. Whether Zoom's conduct constituted unfair or deceptive trade practices;

q. Whether Plaintiffs and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and

r. Whether Plaintiffs and the Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

114. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of the members of the Classes as all members of the Classes are similarly affected by Zoom's actionable conduct. Zoom's conduct that gave rise to the claims of Plaintiffs and members of the Classes is the same for all members of the Classes.

115. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Classes because they are each a member of their respective Classes and are committed to pursuing this matter against Zoom to obtain relief for the Classes. Plaintiffs have no conflicts of interest with the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions and have extensive experience litigating data breach and privacy class actions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Classes' interests.

116. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient

adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Classes are relatively small compared to the burden and expense required to individually litigate their claims against Zoom, and thus, individual litigation to redress Zoom's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

117. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Zoom, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole.

118. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, those common issues identified above.

119. Finally, all members of the proposed Classes are readily ascertainable. Zoom has access to information regarding which individuals purchased or used its products and services. Using this information, the members of the Classes can be identified and their contact information ascertained for purposes of providing notice to the Classes.

APPLICABLE LAW

120. California law applies to the claims of all Class Members.

121. The State of California has sufficient contacts to Zoom's relevant conduct for California law to be uniformly applied to the claims of the Classes. Application of California law to all relevant Class Member transactions comports with the Due Process Clause given the significant aggregation of contacts between Defendant's conduct and California.

122. Zoom is headquartered and does substantial business in California.

123. A significant percentage of the Class Members are located in, and Zoom aimed a significant portion of its unlawful conduct at, California.

124. The conduct that forms the basis for each Class Member's claims against Zoom emanated from Zoom's headquarters in San Jose, California, including Zoom's misrepresentations and omissions regarding data privacy and security. Zoom instructs users with questions about privacy and security to contact Zoom at an address in San Jose.

125. California has a greater interest than any other state in applying its law to the claims at issue in this case. California has a very strong interest in preventing its resident corporations from engaging in unfair and deceptive conduct and in ensuring that harm inflicted on resident consumers is redressed. California's interest in preventing unlawful corporate behavior occurring in California substantially outweighs any interest of any other state in denying recovery to its residents injured by an out-of-state defendant or in applying its laws to conduct occurring outside its borders. If other states' laws were applied to Class Members' claims, California's interest in deterring resident corporations from committing unfair and deceptive practices would be impaired.

CAUSES OF ACTION

COUNT I
Violation of California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code. § 17200, et seq.
(On behalf of Plaintiffs and the Nationwide Classes or, Alternatively, Plaintiffs and the California Subclasses)

126. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

127. Plaintiffs have standing to pursue this cause of action because Plaintiffs suffered injury in fact as a result of Zoom's misconduct described herein.

128. As described herein, Zoom advertised their products and services as having strong data privacy and security included.

129. Plaintiffs and the Class Members would continue using Zoom's products and services if they could be assured that Defendant would take adequate security measures to protect their privacy and PII going forward.

130. The UCL defines unfair business competition to include any "unlawful, unfair or fraudulent" act or practice, as well as any "unfair, deceptive, untrue or misleading" advertising. Cal. Bus. & Prof. Code § 17200. Zoom has engaged in business acts and practices that, as alleged above, constitute unfair competition in violation of Business and Professions Code section 17200.

131. Zoom's acts, as described herein, are "fraudulent" because they are likely to deceive the general public.

132. Zoom's business practices, as alleged herein, violate the "unfair" prong of the UCL because they offend an established public policy and are immoral, unethical, and unscrupulous or substantially injurious to consumers.

133. The reasons, justifications, or motives that Zoom may offer for the acts and omissions described herein are outweighed by the gravity of harm to the victims. The injuries suffered by Plaintiffs and the Class Members are substantial, and are not outweighed by any countervailing benefits to consumers or competition.

134. Zoom's business practices described herein also violate the UCL because Zoom falsely represented that goods or services have characteristics they do not have, namely, reasonable security and privacy protections; falsely represented that its goods or services are of a particular standard when they are of another; advertised its goods and services with intent not to sell them as advertised; represented that the subject of a transaction was supplied in accordance with a previous representation when it was not; and/or made material omissions regarding its safeguarding of customer PII and privacy.

135. As a result of Zoom's unfair business practices, Plaintiffs and the Class Members suffered injury.

136. If Zoom is permitted to continue to engage in the unfair and fraudulent business practices described above, its conduct will engender further injury, expanding the number of injured members of the public beyond its already large size, and will tend to render any judgment at law, by itself, ineffectual. Under such circumstances, Plaintiffs and the Classes have no adequate remedy at law in that Zoom will continue to engage in the wrongful conduct alleged herein, thus engendering a multiplicity of judicial proceedings. Plaintiffs and the Classes request and are entitled to injunctive relief, enjoining Defendant from engaging in the unfair and fraudulent acts described herein.

137. Had consumers including Plaintiffs known the truth that Zoom's products and services included inadequate data security and privacy protections, and that Zoom would share their PII without their consent, they would not have entrusted their PII to Zoom and would not have been willing to use, pay for, or pay as much for, the Zoom's products and services. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with Zoom because they paid for a value of services, either through PII or a combination of their PII and money, they expected but did not receive.

138. The basis for Plaintiffs' claims emanated from California, where the primary decisions regarding Zoom's security and privacy practices were made.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Classes or, Alternatively, Plaintiffs and the California Subclasses)

139. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

140. Zoom offered its videoconferencing capabilities to Plaintiffs and the Class Members. In exchange, Zoom received benefits in the form of monetary payments and access to Plaintiffs' and Class Members' valuable personal information.

141. Zoom has acknowledged these benefits and accepted or retained them.

142. Implicit in the exchange of the products and services for the benefits provided by Plaintiffs and the Class Members is an agreement that Zoom would safeguard their personal information and privacy.

143. Without such implied contracts, Plaintiffs and the Class Members would not have paid for and conferred benefits on Zoom, but rather would have chosen an alternative videoconference platform that did not maintain inadequate data security and privacy measures and share their PII with undisclosed and unauthorized third parties.

144. Plaintiffs and the Class Members fully performed their obligations under their implied contracts with Zoom, but Zoom did not.

145. Zoom breached its implied contracts with Plaintiffs Kondrat and Wolfe and the Members of Class A when it failed to provide them products and services with adequate data privacy and security protections.

146. Zoom breached its implied contracts with Plaintiff Murphy and the Members of Class B when it disclosed their PII to unauthorized third parties like Facebook.

147. As a direct and proximate result of Zoom's breach of its implied contracts with Plaintiffs and the Class Members, Plaintiffs and the Class Members have suffered and will suffer injury.

148. Had consumers including Plaintiffs known the truth that Zoom's products and services included inadequate data security and privacy protections, and that Zoom would share their PII without their consent, they would not have entrusted their PII to Zoom and would not have been willing to use, pay for, or pay as much for, the Zoom mobile application. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with Zoom because they paid value for Zoom's products and services, either through PII or a combination of their PII and money, and expected to receive a more valuable product and service than they in fact received.

COUNT III
Violation of California's Consumer Privacy Act
Cal. Civ. Code § 1798.100, et seq.
(On behalf of Plaintiffs Kondrat and Wolfe and California Subclass A)

149. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

150. California's Consumer Privacy Act ("CCPA") went into effect on January 1, 2020. This comprehensive privacy law was enacted to protect consumers' personal information from collection and use by businesses without appropriate notice and consent.

151. Zoom is a corporation that is organized and operated for the profit or financial benefit of its owners with a reported total third-quarter revenue for fiscal year 2020 of $166.6 million. Zoom collects users' personal information as defined in Civil Code § 1798.140.

152. Through the above-detailed conduct, Zoom violated the CCPA by, among other things, collecting and using personal information without providing consumers with adequate notice consistent with the CCPA, in violation of Civil Code § 1798.100(b).

153. Zoom further violated Civil Code § 1798.150(a) of the CCPA by failing to prevent Plaintiffs' and the Class Members' nonencrypted and nonredacted personal

information, the full extent of which is currently unknown and should be subject to discovery, from unauthorized disclosure as a result of Zoom's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and Class Members.

154. As a direct and proximate result of the Zoom's conduct, Plaintiffs' and the Class Members' personal information was subjected to unauthorized disclosure as a result of Zoom's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and Class Members. Plaintiffs' and Class Members' personal information was accessed and exfiltrated, stolen, and/or disclosed through a data breach of Defendant's data systems as set forth above.

155. As a direct and proximate result of Zoom's conduct, Plaintiffs and the Class Members were injured and lost money or property, including but not limited to the price received by Zoom for its services, the loss of the Class Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses as described above.

156. Zoom knew or should have known that its security practices were inadequate to safeguard the Class Members' personal information and that the risk of unauthorized access and exfiltration, theft, and disclosure was highly likely. Zoom failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and the Class members.

157. In accordance with Civil Code section 1798.150(b), Plaintiffs have served Defendant with notice of these CCPA violations and a demand for relief by certified mail, return receipt requested, as well as via electronic mail on Zoom's counsel.

158. On behalf of Class Members, Plaintiffs seek injunctive relief in the form of an order enjoining Defendant from continuing to violate the CCPA. If Zoom fails to

properly respond to Plaintiffs' notice letter or agree to timely and adequately rectify the violations detailed above, Plaintiffs also will seek actual, punitive, and statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, whichever is greater; restitution; attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5); and any other relief the Court deems proper as a result of Zoom's CCPA violations.

COUNT IV
Violation of California's Consumer Legal Remedies Act ("CLRA")
Civ. Code §§ 1750 et seq.
(On behalf of Plaintiffs and the Nationwide Classes, or, alternatively, Plaintiffs and the California Subclasses)

159. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

160. Plaintiffs and each Class Member are "consumers" under Cal. Civ. Code § 1761(d).

161. Defendant is a "person" as defined by Cal. Civ. Code § 1761(a).

162. Defendant's sale of its app was the sale of a good to consumers under Cal. Civ. Code §§ 1761(e) and 1770(a).

163. The CLRA protects consumers against unfair and deceptive practices, and is intended to provide an efficient means of securing such protection.

164. Defendant violated the CLRA by engaging in unfair and deceptive practices and by causing harm to Plaintiffs and the Classes.

165. As to Class A, Zoom misrepresented and failed to maintain adequate data privacy and security as to its products and services. But Zoom did not disclose these inadequacies to consumers.

166. As to Class B, Zoom disclosed Plaintiff Murphy's and the Class Members' sensitive PII to unauthorized third parties like Facebook for advertising purposes. But Zoom did not disclose this practice to consumers or obtain their consent to sell or disclose their data.

167. Zoom's failures to disclose its inadequate data privacy and security and unauthorized disclosures of Class Members' sensitive PII violated the CLRA in multiple ways:

a. Zoom represented that its products and services had characteristics they did not have, Cal. Civ. Code § 1770(a)(5);

b. Zoom represented its products and services were of a particular standard, grade, or quality when they were of another, *id.* § 1770(a)(7);

c. Zoom advertised its products with intent not to sell them as advertised, *id.* § 1770(a)(9);

d. Zoom knowingly and intentionally withheld material information from Plaintiffs and the Class Members, *id.* § 1770(a)(14).

168. Zoom's unfair or deceptive acts or practices were capable of deceiving a substantial portion of the public. It did not disclose the facts of its inadequate data privacy and security or its disclosure of PII because it knew that consumers would not use its products, and instead would use other products, if they knew the truth.

169. Zoom had a duty to disclose the truth about its security and privacy practices because it is in a superior position to know the quality and level of its data security and privacy measures and whether, when, and how it discloses sensitive PII to third parties; Plaintiffs and the Class Members could not reasonably have been expected to learn or discover Zoom's privacy and security inadequacies or the disclosure of their PII to unauthorized parties like Facebook; and Zoom knew that Plaintiffs and the Class Members would not use its products if they knew the truth.

170. The facts concealed and not disclosed by Zoom are material in that a reasonable consumer would have considered them to be important in deciding whether to use Zoom's products and services.

171. Plaintiffs and the Class Members reasonably expected that Zoom would use adequate data security and privacy measures and safeguard their PII and not disclose it without their consent.

172. Due to Zoom's violations of the CLRA, Plaintiffs and the Class Members suffered injury.

173. Had consumers including Plaintiffs known the truth that Zoom's products and services included inadequate data security and privacy protections, and that Zoom would share their PII without their consent, they would not have entrusted their PII to Zoom and would not have been willing to use, pay for, or pay as much for, the Zoom's products and services. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with Zoom because they paid value for Zoom's products and services, either through PII or a combination of their PII and money, and expected to receive a more valuable product and service than they in fact received.

174. Plaintiffs Kondrat and Wolfe and the members of Class A seek an injunction requiring Zoom to implement adequate data security and privacy measures, and Plaintiff Murphy and the members of Class B seek an injunction barring Zoom from disclosing their PII without their consent.

COUNT V
Unjust Enrichment/Quasi-Contract
(On behalf of Plaintiffs and the Nationwide Classes, or, Alternatively Plaintiffs and the California Subclasses)

175. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein, and to the extent necessary, assert this count in the alternative to the breach of implied contract claim.

176. Zoom has profited and benefited from the use of its videoconferencing services by Plaintiffs and the Classes in exchange for monetary benefits and access to PII.

177. Zoom has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiffs and the Class Members did not receive products of the quality, nature, fitness or value represented by Zoom and that reasonable consumers expected.

178. Zoom has been unjustly enriched by its withholding of and retention of these benefits, at the expense of Plaintiffs and the Class Members.

179. Equity and justice militate against permitting Zoom to retain these profits and benefits.

180. Plaintiffs and the Class Members suffered injury as a direct and proximate result of Zoom's unjust enrichment and seek an order directing Zoom to disgorge these benefits and pay restitution to Plaintiffs and the Class Members.

COUNT VI
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Classes, or, Alternatively, Plaintiffs and the California Subclasses)

181. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

182. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

183. An actual controversy has arisen related to the revelations regarding Zoom's inadequate data and privacy security and disclosures of Plaintiff Murphy's and the members of Class B's PII regarding whether Zoom has violated its duties to provide adequate data and privacy security and to maintain the privacy of users' PII. Plaintiffs allege that Zoom's data security and privacy measures remain inadequate. Zoom presumably will disagree. Furthermore, Zoom continues to possess Plaintiffs' information and, therefore, they remain at continued risk that Zoom's inadequate data and privacy security and unauthorized disclosures of users' PII will result in further compromises of their privacy and security in the future.

184. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Zoom continues to owe legal duties to maintain the privacy of users' PII and to maintain adequate data privacy and security measures under the common law and various state statutes;

b. Zoom continues to breach these duties by failing to maintain the privacy of users' PII and failing to employ adequate data security and privacy measures.

185. The Court also should issue corresponding prospective injunctive relief requiring Zoom to maintain the privacy of users' PII and adequate data privacy and security measures consistent with law and industry standards.

186. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of further unauthorized disclosures and compromises of users' privacy and PII. The risk of further compromise is real, immediate, and substantial. If further compromises and disclosures occur, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable and they will be forced to bring multiple lawsuits to rectify the same conduct.

187. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Zoom if an injunction is issued. Among other things, if compromise and disclosure of users' privacy and PII occurs due to Zoom's failures identified herein, Plaintiffs and Class Members will likely be subjected to fraud, identify theft, invasions of privacy, and other harms described herein. On the other hand, the cost to Zoom of complying with an injunction by employing reasonable prospective data security and privacy measures is relatively minimal, and Zoom has a pre-existing legal obligation to employ such measures.

188. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing further compromises of users' privacy and unauthorized disclosures of PII, thus eliminating the

additional injuries that would result to Plaintiffs and the millions of consumers whose privacy and security would be further compromised.

COUNT VII
NEGLIGENCE
(On Behalf of Plaintiff Murphy and Nationwide Class B, or, Alternatively, Plaintiff Murphy and the California Subclass B)

189. Plaintiff Murphy restates and re-alleges the preceding paragraphs as if fully set forth herein.

190. Zoom provided services to Plaintiff Murphy and the Class Members, including the ability to participate in allegedly secure videoconferences. The transactions between Defendant and the Class Members are intended to benefit the Plaintiff Murphy and the Class Members by providing them the ability to use Zoom's videoconference services for all of the purposes they expected and which were intended by Zoom.

191. Zoom owed a duty to Plaintiff Murphy and the Class Members to exercise reasonable care in the obtaining, using, and protecting of their personal information, arising from the sensitivity of the information shared via Zoom and their reasonable expectation that their information would not be shared with third parties without their consent. This duty included Zoom ensuring that no unauthorized third parties, including Facebook, were improperly given Plaintiff Murphy's and the Class Members' PII.

192. The use of Zoom by Plaintiff Murphy and Class Members was predicated on the understanding that Zoom would take appropriate measures to protect their information. Zoom had a special relationship with Plaintiff Murphy and the Class Members as a result of being entrusted with their content and information, which provided an independent duty of care.

193. It was entirely foreseeable to Zoom that Plaintiff Murphy and the Class Members would be harmed if Zoom disclosed their PII to third parties for advertising purposes without their consent.

194. There is a close connection between Defendant's failure to adequately safeguard Class Member privacy and the injuries suffered by them. But for Zoom's acts and omissions in maintaining inadequate security, Plaintiff Murphy's and the Class Members' PII would not have been shared with Facebook and other unauthorized third parties.

195. Zoom's conduct also involves moral blame. Aware of the privacy expectations of its customers, and the sensitive nature of the information shared during videoconferences intended to be private, Zoom has not taken sufficient actions to prevent the unauthorized disclosure of PII.

196. Zoom breached its duty to Plaintiff Murphy and the Class Members when it disclosed their PII to unauthorized third parties like Facebook.

197. Plaintiff Murphy and the Class Members were harmed by Zoom's failure to exercise reasonable care in safeguarding their PII, and that harm was reasonably foreseeable.

COUNT VIII
Invasion of Privacy (Public Disclosure of Private Facts)
(On behalf of Plaintiff Murphy and the Nationwide Class B, or alternatively, Plaintiff Murphy and the California Subclass B)

198. Plaintiff Murphy restates and re-alleges the preceding paragraphs as if fully set forth herein.

199. Plaintiff Murphy and the Class Members have a reasonable expectation of privacy in their PII, their mobile devices and their online behavior generally. Their private affairs include their behavior on their mobile devices, including their use of Zoom's products and services, and any other behavior that may be monitored by the data gathered by Zoom and disclosed to unauthorized parties such as Facebook.

200. The reasonableness of such expectations of privacy is supported by Zoom's unique position to monitor Plaintiff Murphy's and the Class Members' behavior through its access to their private mobile devices and videoconferences. The

surreptitious, highly technical, and non-intuitive nature of Zoom's disclosure of their PII further underscores the reasonableness of their expectations of privacy.

201. Plaintiff Murphy's and Class Members' privacy interest is legally protected because they have an interest in precluding the dissemination or misuse of sensitive information and an interest in making intimate personal decisions and conducting activities like videoconferencing without observation, intrusion, or interference.

202. Zoom shared Plaintiff Murphy's and the Class Members' PII with unauthorized third parties, including Facebook, without their permission or consent.

203. Zoom's acts and omissions caused the exposure and publicity of private details about Plaintiff Murphy and the Class Members—matters that are of no concern to the public.

204. This intrusion is highly offensive to a reasonable person. Zoom's actions alleged herein are particularly egregious because Zoom concealed its conduct from Plaintiff Murphy and the Class Members and because Zoom represented to Plaintiff Murphy and the Class Members that it took their privacy seriously.

205. Plaintiff Murphy and Class Members were harmed by the public disclosure of their private affairs.

206. Zoom's actions were a substantial factor in causing the harm suffered by Plaintiff Murphy and Class Members.

207. As a result of Zoom's actions, Plaintiff Murphy and Class Members seek damages, including compensatory, nominal, and punitive damages, in an amount to be determined at trial.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Zoom as follows:

A. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs Kondrat and Wolfe as the class representatives of Class A and Plaintiff Murphy as the class representative of Class B and the undersigned counsel as class counsel;

B. For an award of injunctive and other equitable relief as the Court deems just and proper;

C. For an award of damages, including nominal and statutory damages, as allowed by law in an amount to be determined;

D. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

E. For prejudgment interest on all amounts awarded; and

F. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: April 13, 2020

/s/ *Jason S. Hartley*
Jason S. Hartley
HARTLEY LLP
101 West Broadway, Suite 820
San Diego, California 92101
Telephone: 619-400-5822
hartley@hartleyllp.com

Norman E. Siegel (*pro hac vice* forthcoming)
J. Austin Moore (*pro hac vice* forthcoming)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: 816-714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

Counsel for Plaintiffs and the Classes