M. Anderson Berry (SBN 262879)
Leslie Guillon (SBN 222400)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
ABerry@Justice4You.com
LGuillon@Justice4You.com

John A. Yanchunis (*Pro Hac Vice Forthcoming*)
Ryan J. McGee (*Pro Hac Vice Forthcoming*)
Kenya J. Reddy (*Pro Hac Vice Forthcoming*)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813)
Facsimile: (813)
JYanchunis@ForThePeople.com
RMcGee@ForThePeople.com
KReddy@ForThePeople.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ADAM BUXBAUM and DEBORAH BLUM, on behalf of themselves and all others similarly situated, **Plaintiffs** **v.** **ZOOM VIDEO COMMUNICATIONS, INC.,** **Defendant.**	**CASE NO.:** **CLASS ACTION** **COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF** **DEMAND FOR JURY TRIAL**

Plaintiffs Adam Buxbaum and Deborah Blum ("Plaintiffs"), individually, by and through their undersigned counsel, bring this class action lawsuit against Zoom Video Communications Inc. ("Zoom," or "Defendant"), on behalf of themselves and all others similarly situated, and allege, based upon information and belief and the investigation of their counsel as follows:

INTRODUCTION

"[W]e recognize that we have fallen short of the community's – and our own – privacy and security expectations. For that, I am deeply sorry."

Eric S. Yuan, Founder and CEO of Zoom[1]

1. Zoom is a cloud-based video communications platform that ostensibly offers individuals, schools, businesses and governments an easy, reliable cloud platform for video and audio conferencing across mobile devices, desktops, telephones, and room systems.

2. In addition to ease of use and functionality, a cornerstone of Zoom's offering is its fundamental assurance that its video conferences are private, and the personal information entrusted to it by millions of users will be properly maintained. Among the assurances Zoom provides:

- We do not sell your personal data; [2]
- Your meetings are yours. We do not monitor them or even store them after your meeting is done;
- Zoom collects only the user data that is required to provide you Zoom services;
- We do not use data we obtain from your use of our services, including your meetings, for any advertising.
- We take security seriously and we are proud to exceed industry standards when it comes to your organizations [sic] communications.[3]
- Zoom is committed to protecting your privacy.

---

[1] Zoom, *A message to our users*, Zoom Blog (April 1, 2020) *available at* https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/ (last accessed April 28, 2020).
[2] Zoom, *Privacy Policy*, *available at* https://zoom.us/privacy (last accessed April 28, 2020).
[3] Zoom, *Security at Zoom*, *available at* https://zoom.us/security (last accessed April 28, 2020).

3. While video conferencing has enjoyed steady growth over the past several years, in the wake of the COVID-19 pandemic, its popularity has skyrocketed. Among the companies offering video conferencing, Zoom has been by far the biggest beneficiary. In December 2019, Zoom had approximately 10 million daily users. By March 2020, that number grew to 200 million.

4. Zoom's meteoric rise brought with it significant financial reward for the company, whose revenue for fiscal year ending January 31, 2020 was $622.6 million, more than quadruple its revenue a year earlier. It also brought a spotlight which revealed the dark underbelly of a company whose platform was riddled with security vulnerabilities, who transmitted user's personal information surreptitiously to third parties without the users' knowledge and consent, and whose public representations about the privacy and security of its video-conferencing platform were false and misleading.

5. Users, many of whom turned to Zoom to facilitate the most fundamental aspects of their lives in the midst of social distancing and shelter-in-place orders, are now faced with the daunting prospect that their private communications were not private at all, but subject to unwarranted viewing, intrusion and public exposure.

6. Plaintiffs, on behalf of all others similarly situated, allege claims for negligence, invasion of privacy, breach of implied contract, breach of confidence, along with violations of California's Unfair Competition Law, California Consumer Privacy Act, and California's Consumer Legal Remedies Act. By this complaint, Plaintiffs also seek to compel Zoom to adopt appropriate cyber security practices in order to ensure that personal information provided to Zoom and made through its video conferencing platform remain private and secure.[4]

[4] "'Personal information' is any information that can be used to identify an individual, and may include, but is not limited to, name, email address, postal or other physical address, credit or debit card number, title, information generated from use of our Products, and other information required to provide a Product, deliver a product, or carry out a transaction you have requested." Privacy Shield, *Purpose of Data Collection*, *available at* https://www.privacyshield.gov/participant?id=a2zt0000000TNkCAAW&status=Active (last accessed April 28, 2020).

PARTIES

7. Plaintiff Adam Buxbaum is a resident of California.

8. Plaintiff Buxbaum registered with Zoom for a free account and used Zoom's services in reliance on Zoom's promises that, among other things: (a) its videoconferences are secured with end-to-end encryption and are protected by security measures to ensure the privacy of user communications; (b) it will not sell user data without appropriate disclosure and consent; and (c) it will appropriately protect users' personal information.

9. Mr. Buxbaum was unaware that Zoom's video conferences were not fully private, that it shared user personal information without appropriate consent, and that users' personal information was routinely exposed.

10. Mr. Buxbaum participated in several Zoom video conferences, at least one of which was subject to unwanted intrusion and terminally interrupted.

11. Plaintiff Deborah Blum is a California resident.

12. Plaintiff Blum registered with Zoom for a paid account and used Zoom's services in reliance on Zoom's promises that, among other things: (a) its videoconferences are secured with end-to-end encryption and are protected by security measures to ensure the privacy of user communications; (b) it will not sell user data without appropriate disclosure and consent; and (c) it will appropriately protect users' personal information.

13. Ms. Blum was unaware that Zoom's video conferences were not fully private, that it shared user personal information without appropriate consent, and that user personal information was routinely exposed.

14. Ms. Blum paid Zoom approximately $15 a month so that she could continue providing yoga instruction on-line. Ms. Blum's classes are for her customers only, who also have a reasonable expectation that their participation will remain private. Given the recent revelation of Zoom's inadequate cyber security vulnerabilities and inadequate privacy practices, Ms. Blum is reasonably concerned about the integrity and inviolability of her conferences.

15. Defendant Zoom Video Communications, Inc. is a Delaware corporation with its principal place of business in San Jose, California. Zoom was founded in 2011 and became a public company in 2019. It currently has over 200 million users.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. While the exact number of class members is currently unknown, upon information and belief, Zoom has over 200 million users.

17. This Court has jurisdiction over the Defendant which conducts business in this District and has caused harm to Plaintiffs and Class Members residing in this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

STATEMENT OF FACTS

19. Zoom is a cloud-based video communications platform that offers individuals, businesses and governments "an easy, reliable cloud platform for video and audio conferencing, collaboration, chat, and webinars across mobile devices, desktops, telephones, and room systems."[5]

20. Zoom provides basic meeting services (100 participants up to 40 minutes) for free and a number of paid-for-plans that enable additional participants, unlimited conferencing times, and a series of additional amenities and functionalities.[6]

21. Regardless of the plan, all Zoom users are assured the same level of privacy and security of their personal information and communications made through the Zoom platform.

22. Next to functionality, privacy is paramount for video-conference users. Not surprisingly therefore, Zoom goes to great lengths to assure users that the platform is secure and personal information entrusted to Zoom is and will remain private.

---

[5] Zoom, *About*, *available at* https://zoom.us/about (last accessed April 28, 2020).
[6] Zoom, *Pricing*, *available at* https://zoom.us/pricing (last accessed April 28, 2020).

23. Zoom maintains a Privacy Policy wherein it reassures users, among other things, that it is "committed to protecting the privacy and security of [] personal data."[7]

- We do not sell your data.[8]
- We do not sell your personal data.[9]
- Your meetings are yours. We do not monitor them or even store them after your meeting is done unless we are requested to record and store them by the meeting host.[10]
- Zoom collects only the user data that is required to provide you Zoom services.[11]
- We do not use data we obtain from your use of our services, including your meetings, for any advertising.[12]
- Zoom does not monitor or use customer content for any reason other than as part of providing our services.[13]
- Zoom does not sell customer content to anyone or use it for any advertising purposes.[14]
- Zoom is committed to protecting your privacy and ensuring you have a positive experience when using the services we provide.[15]
- We do not allow marketing companies, advertisers or similar companies to access personal data in exchange for payment. We do not allow third parties to use any personal data obtained from us for their own purposes, unless you consent.[16]
- Zoom is committed to protecting your personal data. We use a combination of industry-standard security technologies, procedures, and organizational controls and measures to protect your data from unauthorized access, use, or disclosure.[17]

---

[7] Zoom, *Privacy Policy* (March 29, 2020), *available at* https://zoom.us/privacy (last accessed April 28, 2020).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*

- Zoom keeps privacy and security top of mind for all end users. Find resources and features on how Zoom secures your data and protects your privacy.[18]

- You are entrusting us with your valuable data and information and we take great care to ensure your data is secure at all times. [19]

- Zoom takes your privacy extremely seriously and only collects the data from individuals using the Zoom platform required to provide the service and ensure it is delivered effectively. [20]

24. Despite the litany of privacy assurances, the stark truth is that the Zoom platform is riddled with cyber security vulnerabilities that Zoom was negligent in allowing and failing to timely address. Its failures are exacerbated by its false and misleading representations about the viability of its security measures and its generally poor security hygiene, the combination of which has jeopardized the privacy of millions of its users.

A. Zoom's Platform is Riddled With Security Vulnerabilities That Zoom failed to Timely Identify or Address

25. Like many on-line businesses, Dropbox saw an opportunity to integrate Zoom's video conferencing capabilities as a useful feature for its customers.[21] Soon after integration, however, Dropbox began receiving reports that the Zoom's platform was riddled with security flaws that ranged from those that would enable attackers to "take over users' actions on the Zoom web app," to those that would enable attackers "to run malicious code on computers using Zoom software." [22]

26. Independently, a research engineer at Tenable, a security vulnerability assessment company, "uncovered a serious flaw in Zoom that would have allowed an attacker to remotely

---

[18] *Id.*
[19] Zoom, *Privacy & Security for Zoom Video Communications, available at* https://zoom.us/docs/en-us/privacy-and-security.html (last accessed April 28, 2020).
[20] *Id.*
[21] Dropbox, *How to Use Zoom with Dropbox*, *available at* https://help.dropbox.com/installs-integrations/third-party/zoom (last accessed April 28, 2020).
[22] *Zoom's Security Woes Were No Secret to Business Partners Like Dropbox*, New York Times (April 20, 2020) *available at* https://www.nytimes.com/2020/04/20/technology/zoom-security-dropbox-hackers.html (last accessed April 28, 2020).

disrupt a meeting — without even being on the call" and enabling the attacker to take control over a Zoom user's screen and keyboard and/or "covertly install malware on their computer." *Id.*

27. Concerned that Zoom security vulnerabilities could impact its customers, in 2018, Dropbox "privately offered to pay top hackers it regularly worked with to find problems with Zoom's software. It even had its own security engineers confirm the bugs and look for related problems before passing them on to Zoom." *Id.*

28. In early 2019, Dropbox sponsored HackerOne Singapore, a live hacking competition in which ethical hackers were challenged to find security flaws in a variety of systems. To put pressure on Zoom to take security more seriously, Dropbox included Zoom among companies for which it offered bug bounties at the event.

29. As a result, hackers discovered flaws that would allow attackers to "secretly observe users' video calls" or use the Zoom system "to gain access to the deepest levels of a user's computer." *Id.* Shockingly, Zoom waited more than three months to address the flaw. *Id.*

30. In July 2019, The Electronic Privacy Information Center ("EPIC") submitted a 22-page complaint to the Federal Trade Commission ("FTC") warning that Zoom's business practices jeopardize the "privacy and security of the users of its services." [23] The complaint alleged that "Zoom intentionally designed their web conferencing service to bypass browser security settings and remotely enable a user's web camera without the consent of the user. As a result, Zoom exposed users to the risk of remote surveillance, unwanted videocalls, and denial-of-service attacks. When informed of the vulnerabilities, Zoom did not act until the risks were made public, several months after the matter was brought to the company's attention." *Id.*

31. Months earlier, in March 2019, a software engineer, Jonathan Leitschuh, discovered a significant vulnerability in the Zoom platform affecting Apple Mac users wherein "any website could

[23] *In the Matter of Zoom Video Communications, Inc*. available at https://epic.org/privacy/zoom/EPIC-FTC-Complaint-In-re-Zoom-7-19.pdf (last accessed April 28, 2020).

forcibly join a user to a Zoom call, with their video camera activated, without the user's permission."[24] "A vulnerability in the Mac Zoom Client allows any malicious website to enable your camera without your permission. The flaw potentially exposes up to 750,000 companies around the world that use Zoom to conduct day-to-day business."[25]

32. On March 26, 2019, Leitschuh contacted Zoom to inform it of the vulnerability and presented it with a quick fix solution. The engineer also gave Zoom a 90-day disclosure deadline before the matter would be made public. Despite having a "quick fix solution" that could have been implemented in a matter of days, Zoom waited nearly 3 months before implementing a fix, which unfortunately did not resolve the vulnerability.

> The fix proposed by the Zoom team was to digitally 'sign' the request made to the client. However, this simply means that an attacker would have to have a backend server that makes requests to the Zoom site first to gain a valid signature before forwarding the signature on to the client. They also proposed locking the signature to the IP that made the request. This would mean that as long as the attacker's server was behind the same NAT router as the victim, the attack would still work. I described to the Zoom team how both of these solutions were not enough to fully protect their users. Unfortunately, this left the Zoom team with only 18 days before public disclosure to come up with some better solution. Unfortunately, even after my warning, this was the solution they chose to go with.
>
> Ultimately, Zoom failed at quickly confirming that the reported vulnerability actually existed and they failed at having a fix to the issue delivered to customers in a timely manner. An organization of this profile and with such a large user base should have been more proactive in protecting their users from attack. [26]

33. Separately, Leitschuh also found an install vulnerability wherein once Zoom is installed, the web server "continues to run [even] if you uninstall Zoom from your computer." In response to the public disclosure of this vulnerability, Apple immediately released a silent update—

---

[24] *Apple has pushed a silent Mac update to remove hidden Zoom web server*, Tech Crunch (July 11, 2019) *available at* https://techcrunch.com/2019/07/10/apple-silent-update-zoom-app/ (last accessed April 28, 2020).

[25] *Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!,* Medium (July 8, 2019) *available at* https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5 (last accessed April 28, 2020).

[26] *Id.*

one that does not require any user interaction and is deployed automatically—that addressed the matter. "Apple often pushes silent signature updates to Macs to thwart known malware …. but it's rare for Apple to take action publicly against a known or popular app. The company said it pushed the update to protect users from the risks posed by the exposed web server." [27]

34. Unfortunately, Zoom's poor privacy hygiene and failure to timely address security flaws was endemic to its business culture and a harbinger of worse things to come.

B. Zoom Failed to Provide Conferencing End-to-End Encryption as Promised, Putting User Privacy at Risk

35. With the onset of COVID-19, social distancing and shelter-at-home orders, demand for video conferencing skyrocketed. Virtually overnight, Zoom had become one of its biggest beneficiaries—its popularity based in large part on its ability to provide an easy to use private platform that enabled users (from all segments of society) to engage in their daily functions and maintain some semblance of normalcy.

36. Zoom's meteoric rise, however, was not because it was the only video-conferencing platform on the market when the need arose. To the contrary, the landscape for videoconferencing is competitive. Platforms compete on ease of use, cost and basic features, the most important of which is privacy.

37. Among the cornerstones of Zoom's privacy promises was that its video-conferencing platform was secure – conversations among invited participants would remain between those participants. The representation was bolstered by Zoom's claim that conferencing was subject to end-to-end encryption ("E2E") – commonly understood to be the most private form of internet communication, protecting conversations from all outside parties. Indeed, Zoom unequivocally promised users that:

- E2E Chat Encryption: Zoom E2E chat encryption allows for a secured communication where only the intended recipient can read the secured message. Zoom uses public and private key to encrypt the chat session with Advanced Encryption Standard (AES-256). Session keys

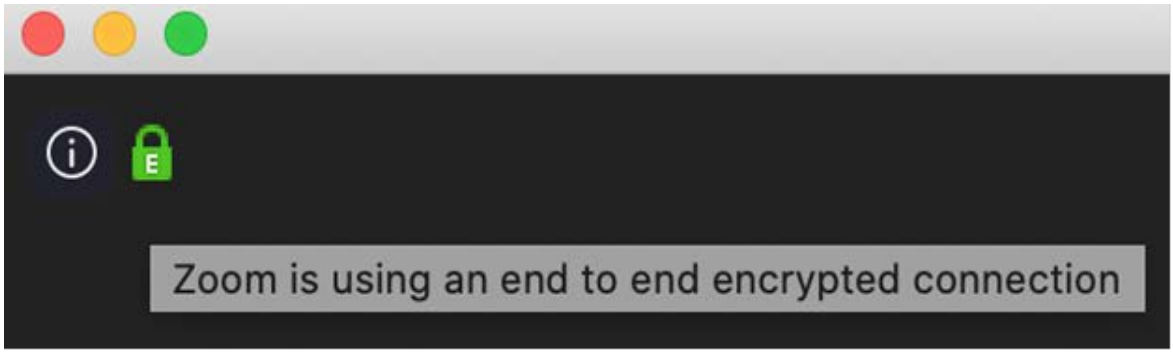
[27] *Apple has pushed a silent Mac update to remove hidden Zoom web server*, Tech Crunch (July 11, 2019) *available at* https://techcrunch.com/2019/07/10/apple-silent-update-zoom-app/ (last accessed April 28, 2020).

are generated with a device-unique hardware ID to avoid data being read from other devices. This ensures that the session cannot be eavesdropped on or tampered with.

- The following pre-meeting security capabilities are available to the meeting host: Enable an end-to-end (E2E) encrypted meeting
- The following in-meeting security capabilities are available to the meeting host: Secure a meeting with E2E encryption[28]

38. Unfortunately, as unsuspecting users soon discovered, Zoom not only failed to provide end-to-end encryption, but it also lacked the technical capacity to do so.

39. On April 3, 2020, The Citizen's Lab issued a report debunking Zoom's representations.[29] While Zoom documentation, as well as the Zoom app itself, "claims that Zoom offers a feature for "end-to-end (E2E) encrypted meetings," the representation is untrue.[30]



40. "Typically, the computer security community understands the term 'end-to-end encrypted' to mean that only the parties to the communication can access it (and not any middlemen

---

[28] *See* Zoom Security Guide (ver. June 2019), *available at* https://web.archive.org/web/20200331082306/https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf. (last visited April 28, 2020)

[29] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security, *available at* https://citizenlab.ca/about/ (last accessed April 28, 2020).

[30] *Move Fast and Roll Your Own Crypto A Quick Look at the Confidentiality of Zoom Meetings*, The Citizens Lab (April 3, 2020) ("CL Report") *available at* https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/ (last accessed April 28, 2020).

that relay the communication)."[31] However, Zoom's service is not end-to-end encrypted, and as a result, the company has access to all encryption keys and to all video and audio content traversing its cloud.[32]

41. "[D]espite this misleading marketing, the service actually does not support end-to-end encryption for video and audio content, at least as the term is commonly understood. Instead it offers what is usually called transport encryption […] which is different from end-to-end encryption because the Zoom service itself can access the unencrypted video and audio content of Zoom meetings. So when [a user] has a Zoom meeting, the video and audio content will stay private from anyone spying on a [] [user's] Wi-Fi, but it won't stay private from the company."[33]

42. While E2E encryption is more difficult and costly to implement, it most certainly can be done, and is in fact offered by many of Zoom 's competitors such as Apple's FaceTime and Signal.

43. When confronted with this revelation, a Zoom spokesperson admitted that, "[c]urrently, it is not possible to enable E2E encryption for Zoom video meetings." [34]

44. "When we use the phrase 'End to End' in our other literature, it is in reference to the connection being encrypted from Zoom end point to Zoom end point," the Zoom spokesperson wrote, apparently referring to Zoom servers as "end points" even though they sit between Zoom clients. "The content is not decrypted as it transfers across the Zoom cloud" through the networking between these machines.[35] According to one cryptographer, Professor Matthew D. Green of Johns

---

[31] *Id.* (CL Report).
[32] *Zoom's Encryption Is "Not Suited For Secrets" And Has Surprising Links To China, Researchers Discover*, The Intercept (April 3, 2020) *available at* https://theintercept.com/2020/04/03/zooms-encryption-is-not-suited-for-secrets-and-has-surprising-links-to-china-researchers-discover/ (last accessed April 28, 2020).
[33] *Zoom Meetings Aren't End-To-End Encrypted, Despite Misleading Marketing*, The Intercept, (March 31, 2020) available at https://theintercept.com/2020/03/31/zoom-meeting-encryption/ (last accessed April 28, 2020).
[34] *Id.*
[35] *Id.*

Hopkins University's Department of Computer Science, Zoom is twisting the common meaning of "end-to-end" in a "dishonest way." [36]

45. The Citizen's Lab Report found that Zoom "rolled their own" encryption scheme, which has "significant weaknesses" [37] and ultimately concluded that Zoom's service is simply "not suited for secrets."[38]

46. In the wake of this monumental transgression, Zoom only apologized for and "confusion" stating that "[w]e recognize that we can do better with our encryption design."[39]

47. In addition to Zoom's false and misleading statements about its capacity to provide end-to-end encryption, its platform was also littered with a litany of cyber security vulnerabilities that demonstrated its negligent disregard for cyber security hygiene.

C. *Zoom Transmits User Data Surreptitiously to Facebook Without User Knowledge or Consent*

48. Zoom provides interested users the ability to log in via Facebook. The feature was enabled through Facebook's standard software development kit ("SDK"), a bundle of code that developers often use to help implement certain features into their own app. Prior to utilizing this code, Facebook makes clear that using the SDK will result in the transmission of analytics and other user information to Facebook—an action that necessitates sufficient notice to users. "Facebook requires developers to be transparent with users about the data their apps send to Facebook. Facebook's terms clearly state that, '[i]f you use our pixels or SDKs, you further represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Customer Data collection, sharing and usage,' and specifically for apps, 'that third parties, including

---

[36] *Id.*

[37] CL Report, *supra* n.31.

[38] *Zoom's Encryption Is "Not Suited For Secrets" And Has Surprising Links To China, Researchers Discover,* The Intercept (April 3, 2020) *available at* https://theintercept.com/2020/04/03/zooms-encryption-is-not-suited-for-secrets-and-has-surprising-links-to-china-researchers-discover/ (last accessed April 28, 2020).

[39] *Zoom security issues: Zoombombings continue, include racist language and child abuse*, CNET, (April 24, 2020) *available at* https://www.cnet.com/news/zoom-security-issues-zoombombings-continue-include-racist-language-and-child-abuse/ (last accessed April 28, 2020).

Facebook, may collect or receive information from your app and other apps and use that information to provide measurement services and targeted ads.'"[40]

49. Upon downloading and opening the app, Zoom automatically notifies Facebook and provides it with user details including when a user opened the app, their time zone, city, and information about their device including a unique advertiser identifier which can subsequently be used to identify user interests and target the user with advertisements.

50. Shockingly, Zoom transfers user data regardless of whether the user has a Facebook account, or has integrated their Facebook profile through Zoom.

51. Despite Facebook's admonition to warn consumers about the transmission of their data, and Zoom's independent legal obligation to do the same, Zoom failed to notify its users, seek their consent or provide them with an opportunity to opt out of Zoom's data-sharing with Facebook.

52. When confronted with this data leak, Zoom claimed only that it was unaware "the Facebook SDK was collecting unnecessary device data," but will now remove it and reconfigure the feature so that users will still be able to login with Facebook via their browser.[41]

D. Zoom Surreptitiously Mines User Data and Transmits to LinkedIn

53. Zoom's claim that it was "unaware" of the user data it was transmitting to Facebook is disingenuous in light of the fact that Zoom routinely contracts with third parties to use its platform, and in so doing allows them to mine user data.

54. According to an analysis conducted by the New York Times, Zoom used data-mining tools to collect users' personal information without authorization, then used the personal information to match the users' LinkedIn profiles. "For Americans sheltering at home during the coronavirus pandemic, the Zoom videoconferencing platform has become a lifeline, enabling millions of people to easily keep in touch with family members, friends, students, teachers and work

---

[40] *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account*, Vice, (March 26, 2020) *available at* https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account (last accessed April 28, 2020).

[41] *Zoom Removes Code That Sends Data to Facebook,* Vice (March 28, 2020) *available at* https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook (last accessed April 28, 2020).

colleagues. But what many people may not know is that, until [recently], a data-mining feature on Zoom allowed some participants to surreptitiously have access to LinkedIn profile data about other users — without Zoom asking for their permission during the meeting or even notifying them that someone else was snooping on them." [42]

55. The data-mining feature was available to Zoom users who subscribed to a LinkedIn service for sales prospecting, called LinkedIn Sales Navigator. Once a Zoom user enabled the feature, that person could quickly and covertly view LinkedIn profile data—like locations, employer names and job titles—for people in the Zoom meeting by clicking on a LinkedIn icon next to their names.

56. As with its data transmission to Facebook, "neither Zoom's privacy policy nor its terms of service specifically disclosed that Zoom could covertly display meeting participants' LinkedIn data to other users—or that it might communicate the names and email addresses of participants in private Zoom meetings to LinkedIn. In fact, user instructions on Zoom suggested just the opposite: that meeting attendees may control who sees their real names." *Id.*

57. As with prior privacy incidents, Zoom repeated its same mantra, apologizing for the privacy breach, promising to remove or disable the offending feature, and rotely stating that it takes users' privacy "extremely seriously." *Id.*

58. In the wake of repeated privacy breaches, however, as summed up by Jonathan Mayer, an assistant professor of computer science and public affairs at Princeton University, "[i]t's very clear that they have not prioritized privacy and security in the way they should have, which is obviously more than a little concerning."

[42] *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*, New York Times, (April 2, 2020) *available at* https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html (last accessed April 28, 2020).

E. Leak of Users' Personal Information

59. In yet another example of Zoom's poor privacy practices, on April 1, 2020, Vice revealed that that Zoom was leaking PII belonging to thousands of its users.[43] "Zoom is leaking personal information of at least thousands of users, including their email address and photo, and giving strangers the ability to attempt to start a video call with them through Zoom."[44]

60. The issue related to Zoom's Company Directory setting, which automatically groups people that signed up with email addresses that share the same domain. Ostensibly this can make it easier to find colleagues within a company, but again, due to poor security practices, the feature also has the effect of grouping and exposing all people who have signed up with the same domain, regardless of whether that domain is a company. "If you subscribe to Zoom with a non-standard provider," then you get access to "the full names, mail addresses, profile pictures and status[es]" of all subscribed users with that domain.[45]

F. Zoom Exploit for Sale on the Dark Web

61. Yet another example of Zoom's unacceptably poor security practices was recently evidenced when Zero-day exploits were offered for sale on the dark web.

62. Zero-day exploits are vulnerabilities that have not yet been patched by the affected vendor and that allow attackers to compromise any targets running or using the unpatched products.[46] Zero-day exploits can be sold for thousands or even millions of dollars.

---

[43] *Zoom is Leaking Peoples' Email Addresses and Photos to Strangers*, Vice (April 1, 2020) *available at* https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos (last accessed April 28, 2020).

[44] *Id.*

[45] *Id.*

[46] *Exploit for Zoom Windows zero-day being sold for $500,000*, Bleeping Computer (April 15, 2020) *available at* https://www.bleepingcomputer.com/news/security/exploit-for-zoom-windows-zero-day-being-sold-for-500-000/ (last accessed April 28, 2020).

63. On April 15, 2020, news sources revealed that two Zoom specific zero-day exploits were available for sale on the dark web. "The two flaws… are currently present in Zoom's Windows and MacOS clients … [and] would allow someone to hack users and spy on their calls"[47]

64. The Zoom Windows zero-day exploit is a remote code execution vulnerability that could allow potential attackers to execute arbitrary code on systems running a Zoom Windows client and even take full control of the device if coupled with other bugs. The exploit was being sold for $500,000, a price tag that might be justified as it is "perfect for industrial espionage."[48]

G. Exposure of User Zoom Videos

65. On April 17, 2020, the *Washington Post* revealed that "thousands of personal Zoom videos have been left viewable on the open Web," highlighting yet another Zoom security flaw putting user privacy at risk.

66. Videos easily accessed and viewed by the *Post* included private therapy sessions, telehealth calls, business meetings containing sensitive financial information and elementary school classes, revealing a treasure trove of sensitive personally identifiable information and personal health information.[49]

67. "Many of the videos include personally identifiable information and deeply intimate conversations, recorded in people's homes. But 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."[50] "The publicly exposed videos could be a surprise for people who expected

---

[47] *Hackers Are Selling a Critical Zoom Zero-Day Exploit for $500,000*, Motherboard (April 15, 2020) *available at* https://www.vice.com/en_us/article/qjdqgv/hackers-selling-critical-zoom-zero-day-exploit-for-500000 (last accessed April 28, 2020).

[48] *Exploit for Zoom Windows zero-day being sold for $500,000,* Bleeping Computer (April 15, 2020) *available at* https://www.bleepingcomputer.com/news/security/exploit-for-zoom-windows-zero-day-being-sold-for-500-000/ (last accessed April 28, 2020).

[49] *Thousands of Zoom video calls left exposed on open Web*, The Washington Post (April 3, 2020) available at https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/ (last accessed April 28, 2020).

[50] *Id.*

their sensitive discussions would be kept private. But they could also put people at real personal risk."[51]

68. In designing the platform, "Zoom's engineers bypassed some common security features of other video-chat programs, such as requiring people to use a unique file name before saving their own clips. 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."[52]

69. Indeed, various security researches have highlighted security flaws that could allow strangers to "steal log-in information, view messages and take control of users' cameras and microphones."[53]

70. The service has also been abused by uninvited miscreants who invade unlocked Zoom meetings in order to spy and/or disrupt video conferences often accompanied by pornographic images and racial slurs. Even worse, a recording of the video conference may then be uploaded for all to see. These interruptions have reached such epidemic numbers that have been colloquially referred to as "Zoom bombings." Reporting from both CNET and *The New York Times* revealed social media platforms, including Twitter and Instagram, were being used by anonymous attackers as spaces to organize "Zoom raids"—the term for coordinated mass Zoom bombings.[54] Recent headlines alone provide a small sample of the on-going problem.

---

[51] *Id.*
[52] *Id.*
[53] *Id.*; *see also* https://www.tomsguide.com/news/zoom-security-privacy-woes (A Kurdish security researcher said Zoom had paid him 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) (last accessed April 28, 2020).
[54] *Instagram, Twitter used to organize harassment campaigns on Zoom*, CNET (April 6, 2020) *available at* https://www.cnet.com/news/instagram-twitter-used-to-organize-harassment-campaigns-on-zoom/ (last accessed April 28, 2020).

- Los Angeles Times, April 23, 2020, "*Disturbing Zoom-bombing' incident hits Fresno State students, officials say*"[55]
- Threat Post, April 17, 2020, "*Zoom Bombing Attack Hits U.S. Government Meeting*"[56]
- Lexington Herald, April 7, 2020 "*Pornographic video appeared during 'Zoom bombing' in a KY school virtual meeting*"[57]
- Inside Higher Ed, March 26, 2020, '*Zoombombing' Attacks Disrupt Classes*"[58]
- Entrepreneur, April 3, 2020, *Were You Zoom-Bombed? Video of It May Now Be on YouTube, TikTok for All to See*"[59]

71. According to data gathered by a new automated Zoom meeting discovery tool dubbed 'zWarDial,' "a crazy number of meetings at major corporations are not being protected by a password."[60]

72. Each Zoom conference call is assigned a Meeting ID that consists of 9 to 11 digits. Naturally, hackers have figured out they can simply guess or automate the guessing of random IDs within that space of digits.

---

[55] *Disturbing Zoom-Bombing incident hits Fresno State Students, officials say*, Los Angeles Times (April 23, 2020) *available at* https://www.latimes.com/california/story/2020-04-23/coronavirus-zoom-bombing-fresno-state (last accessed April 28, 2020).

[56] *Zoom Bombing Attack Hits U.S. Government Meeting*, threatpost (April 17, 2020) *available at* https://threatpost.com/zoom-bombing-attack-hits-u-s-government-meeting/154903/ (last accessed April 28, 2020).

[57] *Pornographic video appeared during 'Zoom Bombing' in a KY school virtual meeting*, Lexington Herald Leader (April 7, 2020) *available at* https://www.kentucky.com/news/local/education/article241809326.html (last accessed April 28, 2020).

[58] *Zoomboming Attacks Disrupt Classes*, Inside Higher Ed (March 26, 2020) *available at* https://www.insidehighered.com/news/2020/03/26/zoombombers-disrupt-online-classes-racist-pornographic-content (last accessed April 28, 2020).

[59] *Were You Zoom-Bombed? Video of It May Now Be on YouTube, TikTok for All to See*, Entrepreneur (April 3, 2020) *available at* https://www.entrepreneur.com/article/348720 ("You can now easily find video footage of "Zoom-bombing" incidents on both YouTube and TikTok. And some of the content is heinous and disturbing.") (last accessed April 28, 2020).

[60] *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/ (last accessed April 28, 2020).

73. "A single instance of zWarDial can find approximately 100 meetings per hour, but that multiple instances of the tool running in parallel could probably discover most of the open Zoom meetings on any given day. Each instance [] has a success rate of approximately 14 percent, meaning for each random meeting number it tries, the program has a 14 percent chance of finding an open meeting."[61]

74. Output of one day's worth of zWarDial scanning "were staggering, and revealed details about Zoom meetings scheduled by some of the world's largest companies, including major banks, international consulting firms, ride-hailing services, government contractors, and investment ratings firms."[62]

75. Ostensibly users could protect their meetings with a password, however, given the shocking number of Zoom meetings that were exposed by use of the discovery tool, security researchers questioned whether Zoom users disabled passwords by default or that Zoom's new security feature simply is not working as intended for all users. Indeed, "new data and acknowledgments by Zoom itself suggest the latter may be more likely." *Id*. In response, Zoom said "it was investigating the possibility that its password-by-default approach may fail under certain circumstances."[63]

H. Zoom Data Breach Resulting in the Exposure of 500,000 User Names and Passwords

76. In addition to the security infirmities built into its platform, Zoom's own internal cyber security practices are grossly inadequate. On April 15, 2020, news sources reported that the personally identifiable information of over 500,000 Zoom accounts had been exposed and was being "sold on the dark web [] for less than a penny each, and in some cases, given away for free."[64]

77. The accounts included email addresses, passwords, personal meeting URL, and their HostKey – more than enough information for a hacker to infiltrate meetings.

---

[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Over 500,000 Zoom accounts sold on hacker forums, the dark web, Bleeping Computer* (April 13, 2020) *available at* https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/ (last accessed April 28, 2020).

I. Aftermath

78. As a result of the litany of privacy concerns were raised by investigative journalists, researchers and the public, federal and state authorities stepped in.

79. On March 30, 2020, The FBI issued a warning due to the proliferation of Zoom-bombings. "The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language …. As individuals continue the transition to online lessons and meetings, the FBI recommends exercising due diligence and caution in your cybersecurity efforts."[65]

80. Similarly, Attorneys General from several states have raised concerns about Zoom's privacy practices.[66] "Connecticut Attorney General William Tong said he was attending a conference this week with state Lt. Gov. Susan Bysiewicz via the video conferencing app Zoom when hackers inundated the meeting with "hundreds of profane and racist comments. It's a sign of the need to evaluate the California-based online platform's online security and privacy."[67] "We are alarmed by the Zoom-bombing incidents and are seeking more information from the company about its privacy and security measures in coordination with other state attorneys general."[68]

---

[65] *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*, FBI (March 30, 2020) *available at* https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic (last accessed April 28, 2020).

[66] See e.g., *Two U.S. State AGs Seek Info on Zoom's Privacy Practices,* US News (April 3, 2020) *available at* https://www.usnews.com/news/top-news/articles/2020-04-03/two-us-state-attorneys-general-seek-info-on-zooms-privacy-practices; *New York Attorney General Examining Zoom Privacy Practices*, National Law Review (March 31, 2020) *available at* https://www.nationalreview .com/news/new-york-attorney-general-examining-zoom-privacy-practices/ (last accessed April 28, 2020).

[67] *Hackers Bombarded Zoom Conference With AG on Line: 5 Tips for Lawyers*, Connecticut Law Tribune (April 3, 2020) *available at* https://www.law.com/ctlawtribune/2020/04/03/hackers-bombarded-a-zoom-conference-with-an-ag-on-the-line-5-tips-for-lawyers/?slreturn=20200323071648 (last accessed April 28, 2020).

[68] *Multiple state AGs looking into Zoom's privacy practices,* Politico (April 3, 2020) *available at* https://www.politico.com/news/2020/04/03/multiple-state-ags-looking-into-zooms-privacy-practices-162743 (last accessed April 28, 2020).

81. Ohio Sen. Sherrod Brown, the ranking member of the Banking, Housing and Urban Affairs Committee, sent a letter to the FTC asking it to take action and alleging that Zoom had made "deceptive" claims to users.[69] Numerous other members of Congress transmitted letters directly to Zoom expressing their concerns over the company's privacy practices and demanding answers. "Millions of Americans are now using @zoom_us to attend school, seek medical help, & socialize with their friends. Privacy & cybersecurity risks shouldn't be added to their list of worries. I'm calling for answers from Zoom on how it handles our private data" said Senator Richard Blumenthal.[70]

82. Representative Jerry McNerney and a group of almost two dozen other House Democrats sent a separate letter to Zoom "expressing concerns around data protection, while multiple secretaries of state across the U.S. are also looking into the company."[71]

83. As Congressional members expressed their outrage on behalf of the public, the Senate sergeant at arms warned congressional offices that Zoom poses a high risk to privacy to them and could leave their data and systems exposed. Zoom has been "issued a high-risk notice" and poses the threat of "potential compromise of systems and loss of data, interruptions during a conference, and lack of privacy." [72]

---

[69] *Senator Asks FTC To Investigate Zoom's 'Deceptive' Security Claims*, NPR (April 3, 2020) *available at* https://www.npr.org/2020/04/03/826968159/senator-zoom-deceived-users-over-its-security-claims (last accessed April 28, 2020).

[70] *Senator Blumenthal Is Super Mad That Zoom Isn't Actually Offering The End To End Encryption His Law Will Outlaw*, Tech Dirt (April 1, 2020) *available at* https://www.techdirt.com/articles/ 20200401/16571344217/senator-blumenthal-is-super-mad-that-zoom-isnt-actually-offering-end-to-end-encryption-his-law-will-outlaw.shtml (last accessed April 28, 2020).

[71] *Democratic senator criticizes Zoom's security and privacy policies*, The Hill (April 6, 2020) *available at* https://thehill.com/policy/cybersecurity/491380-democratic-senator-criticizes-zooms-security-and-privacy-policies (last accessed April 28, 2020).

[72] *Internal Senate memo warns Zoom poses 'high risk' to privacy, security*, Politico (April 9, 2020) *available at* https://www.politico.com/news/2020/04/09/internal-senate-memo-warns-zoom-poses-high-risk-to-privacy-security-177347 (last accessed April 28, 2020).

84. In the cascade of its cyber security flaws, misleading representations and inadequate privacy practices, Zoom had to admit that its security is inadequate. "***I really messed up***" stated Zoom's founder and Chief Executive Officer, Eric Yuan as he suspended all new functionality and dedicated the next 90 days to focus on security issues.

85. Zoom's CEO explained that "We did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home," and "We now have a much broader set of users who are utilizing our product in a myriad of unexpected ways, presenting us with challenges we did not anticipate when the platform was conceived." [73]

86. The explanation, however, was non-sensical as cyber security protocols, measures to ensure privacy, and true and correct statements regarding a company's capabilities should be in place at the inception of any business, regardless of the constituency of ultimate users or their numbers.

87. For these serious transgressions, Zoom must now be held accountable.

CLASS ACTION ALLEGATIONS

88. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a Nationwide class defined as follows:

> All persons in the United States who used Zoom during the applicable limitations period (the "Nationwide Class").

89. Plaintiffs also seek to certify a California Sub-Class defined as follows:

> All persons residing in the State of California who used Zoom during the applicable limitations period (the "California Sub-Class").

[73] *Multiple state AGs looking into Zoom's privacy practices*, Politico (April 3, 2020) *available at* https://www.politico.com/news/2020/04/03/multiple-state-ags-looking-into-zooms-privacy-practices-162743 (last accessed April 28, 2020).

90. Excluded from the Nationwide Class and California Sub-Class (collectively, the "Classes") are Zoom and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Classes; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

91. 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.

92. The proposed Classes meet the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

93. **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.

94. **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 members of the Classes. The common questions include:

a. Whether Zoom acted negligently;

b. Whether Zoom violated Plaintiffs' and members of the Classes' privacy rights;

c. Whether Zoom shared the personal information of Plaintiffs and other members of the Classes with third parties without Plaintiffs' and other members of the Classes authorization or consent;

d. Whether Plaintiffs and other members of the Classes formed implied contracts with Zoom;

e. Whether Zoom breached implied contracts with Plaintiffs and the members of the Classes and breached the implied covenant of good faith and fair dealing;

f. Whether Zoom violated California's Consumer Privacy Act;

g. Whether Zoom violated California's Consumer Legal Remedies Act;

h. Whether Zoom violated California's Unfair Competition Law;

i. Whether Plaintiffs and members of the Classes were injured and suffered damages or other losses as a result of Zoom's conduct; and

j. Whether Plaintiffs and members of the Classes are entitled to relief.

95. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other members of the Classes. Plaintiffs each registered with Zoom and used the platform for video conferencing. Plaintiffs' damages and injuries are akin to other members of the Classes, and Plaintiffs seek relief consistent with the relief sought by the Classes.

96. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Classes because Plaintiffs are members of the Classes they seek to represent; are committed to pursuing this matter against Zoom to obtain relief for the Classes; and have no conflicts of interest with the Classes. Moreover, Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Classes' interests.

97. **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 quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an 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 member of each Class 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.

98. **Applicability of California Law to the Nationwide Class.** Zoom is based in San Jose, California, and upon information and belief, all managerial decisions emanate from San Jose, California, the representations on Defendant's website originate from San Jose, California, Defendant's misrepresentations originated from San Jose, California, and therefore application of California law to the Nationwide Class is applicable.

99. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, 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 Class as a whole.

100. 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.

101. Finally, all members of the proposed Classes are readily ascertainable. Zoom has access to names and locations for members of the Classes. Using this information, members of the Classes can be identified and ascertained for the purpose of providing notice.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

102. Plaintiffs restate and reallege paragraphs 1 through 102 above as if fully set forth herein.

103. As a condition of receiving Zoom's services, Plaintiffs and Class Members were obligated to provide Zoom with their personal information and entrust the personal information transmitted via the Zoom platform would remain private and secure.

104. Zoom owed a duty to Plaintiffs and the other Class Members to exercise reasonable care in: (a) using their personal information in compliance with all applicable law and the terms of

Zoom's privacy policy; (b) safeguarding their personal information in its possession; and (c) ensuring Zoom's video-conferences were private and secure.

105. Plaintiffs and the Class Members entrusted Zoom with their personal information with the understanding that Zoom would safeguard their information.

106. Defendant had full knowledge of the sensitivity of the personal information entrusted to it and the types of harm that Plaintiffs and Class Members could and would suffer if such information were wrongfully disclosed.

107. Plaintiffs and Class Members used Zoom's services in reliance on its alleged exercise of due care and fulfillment of its duties which Zoom breached by, among other things: (a) disclosing Plaintiffs' and Class Members' personal information to third parties without knowledge or consent; (b) misleadingly representing that Zoom's video conference was private and secure; (c) failing to maintain measures sufficient to protect users' privacy and to implement proper cyber security hygiene.

108. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised and/or disclosed to unauthorized parties.

109. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures.

110. Defendant's conduct created a foreseeable risk of harm to Plaintiffs and the Class Members.

111. Plaintiffs and the Class Members had no ability to protect their personal information that was in Zoom's possession or made available to Zoom through video conferencing.

112. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the conduct complained herein.

113. Defendant improperly and inadequately safeguarded Plaintiffs' and Class members' personal information in deviation of standard industry rules, regulations, and practices.

114. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' personal information would not have been compromised.

115. As a result of Defendant's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

116. Plaintiffs restate and reallege paragraphs 1 through 102 above as if fully set forth herein.

117. Plaintiffs and Class Members had a legitimate expectation of privacy with respect to their personal information and were entitled to the protection of this information against disclosure to unauthorized third parties.

118. Defendant owed a duty to its users, including Plaintiffs and Class Members, to keep their personal information confidential.

119. Defendant failed to protect and released to unknown and unauthorized third parties data containing the PII of Plaintiffs and Class Members.

120. Among other things, Defendant allowed: (1) third parties to access and mine users' data without their knowledge or consent; (2) allowed unauthorized third parties to access what were reasonably believed to be private video conferences; and (3) allowed the exfiltration of the personal information of myriad users as a result of inadequate cyber security practices.

121. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their personal information to Defendant as part of their use of Defendant's services, but privately with an intention that such information would be kept confidential, within the confines of the conversations enabled by the Zoom platform, and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

122. The privacy breaches at the hands of Defendant constitute an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

123. Defendant acted with a knowing state of mind when it permitted these privacy breaches because it was with actual knowledge that its information security practices were inadequate and insufficient.

124. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' personal information was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

125. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the personal information maintained by Defendant can be viewed, distributed, and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class Members.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

126. Plaintiffs restate and reallege paragraphs 1 through 102 above as if fully set forth herein.

127. Plaintiffs and Class Members provided Defendant with their personal information both in registering as a user and each and every time they utilized the Zoom platform.

128. In its written privacy policies, Zoom expressly promised Plaintiffs and Class Members that it would protect the integrity of their personal information.

129. Implicit in the agreement between the Defendant and its users, including Plaintiffs and Class Members, was Defendant's obligation to: (a) use personal information for business purposes only; (b) take reasonable steps to secure and safeguard personal information, and not make unauthorized disclosures of such data to unauthorized third parties; (c) maintain adequate security

and proper encryption with respect to its videoconferences; and (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access of their personal information.

130. Without such implied contracts, Plaintiffs and Class Members would not have provided and/or authorized the release of their personal information to Defendant.

131. Defendant had an implied duty to reasonably safeguard and protect the personal information of Plaintiffs and Class members from unauthorized disclosure or uses.

132. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

133. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' personal information.

134. Defendant's failures to meet these promises constitute breaches of the implied contracts.

135. Because Defendant allowed unauthorized access to Plaintiffs' and Class Members' personal information and failed to safeguard the PII, Defendant breached its contracts with Plaintiffs and Class Members.

136. Defendant breached its contracts by not meeting the minimum level of protection of Plaintiffs and Class Members' personal information.

137. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiffs and Class Members that were of a diminished value.

138. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

FOURTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

139. Plaintiffs restate and reallege paragraphs 1 through 102 above as if fully set forth herein.

139. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' personal information that Plaintiffs and Class Members provided to Defendant.

140. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' personal information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

141. Plaintiffs and Class Members provided their personal information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit personal information to be disseminated to any unauthorized parties.

142. Plaintiffs and Class Members also provided their personal information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that personal information from unauthorized disclosure, such as following basic principles of information security practices.

143. Defendant voluntarily received in confidence Plaintiffs' and Class Members' personal information with the understanding that such information would not be disclosed or disseminated to the public or any unauthorized third parties.

144. Due to Defendant's failure to prevent, detect, or avoid the privacy breaches from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiffs' and Class Members' personal information, Plaintiffs' and Class Members' personal information was disclosed beyond Plaintiffs' and Class Members' confidence, and without their express permission.

145. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

146. But for Defendant's disclosure of Plaintiffs' and Class Members' personal information in violation of the parties' understanding of confidence, their protected personal information would not have been compromised, viewed, accessed, and used by unauthorized third parties.

147. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' personal information.

148. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to injury and/or harm in the form of economic and non-economic losses.

FIFTH CAUSE OF ACTION
Violation of Bus. & Prof. Code §§ 17200, *et seq.* – Unfair Business Practices
(On Behalf of Plaintiffs and the Nationwide Class)

149. Plaintiffs restate and reallege paragraphs 1 through 102 above as if fully set forth herein.

150. 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.

151. Zoom collected and stored confidential, sensitive personal information from Plaintiffs and other Class Members. In so doing, Zoom deceptively, misleadingly and falsely represented to Plaintiffs and Class members, *inter alia*, that: (a) it maintains adequate security measures to safeguard and keep confidential users' personal information; (b) it does not sell user data; (c) and its video conferences are end-to-end encrypted, providing the highest level of privacy.

152. In reliance on Zoom's representations, Plaintiffs and other Class Members acquired Zoom accounts and provided Zoom with sensitive personal information.

153. Zoom's misrepresentations and omissions caused Plaintiffs and other Class Members to become Zoom users and provide Zoom with their confidential, sensitive personal information.

Plaintiffs and other Class Members would not have done so, but for Zoom's misrepresentations and omissions.

154. A business act or practice is "unfair" under the Unfair Competition Law if the reasons, justifications and motives of the alleged wrongdoer are outweighed by the gravity of the harm to the alleged victims.

155. Zoom has and continues to violate the "unfair" prong of the UCL through its poor cyber security practices and false and misleading promises of privacy and security.

156. The gravity of the harm to Plaintiffs and Class Members resulting from such unfair acts and practices outweighs any conceivable reasons, justifications, or motives of Zoom for engaging in such deceptive acts and practices. By committing the acts and practices alleged above, Zoom has engaged, and continues to engage, in unfair business practices within the meaning of California Business and Professions Code §§ 17200, et seq.

157. A business act or practice is "unlawful" if it violates any established state or federal law.

158. A business act or practice is "fraudulent" under the Unfair Competition Law if it actually deceives or is likely to deceive members of the consuming public. Zoom's acts, as alleged above, are "fraudulent" because they are likely to deceive the general public.

159. Plaintiffs and other Class Members suffered injury in fact and/or lost money or property as the result of Zoom's violations of the Unfair Competition Law.

160. Plaintiffs request that Zoom be: (a) enjoined from further violations of the UCL; and (b) required to restore to Plaintiffs and other Class Members any money it had acquired by unfair competition, including restitution and restitutionary disgorgement. Otherwise the Class may be irreparably harmed and denied an effective and complete remedy if such an Order is not granted.

SIXTH CAUSE OF ACTION
Breach of the California Consumer Privacy Act of 2018 ("CCPA")
California Civil Code §§ 1798.100, *et seq*.
(On behalf of Plaintiffs and the California Sub-Class)

161. Plaintiffs restate and reallege paragraphs 1 through 102 above as if fully set forth herein.

162. Among other things, the CCPA prohibits collection and use of consumers' personal information from collection and use by businesses without consumers' notice and consent.

163. Plaintiffs and members of the California Sub-Class are consumers, are natural persons who are California residents, as defined in Section 17014 of Title 18 of the California Code of Regulations within the meaning of the Cal. Civ. Code §1798.140(g).

164. Personal information means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Cal. Civ. Code §1798.140 (o).

165. Cal. Civ. Code §1798.120(a) provides a consumer the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information ("opt out"). Moreover, a business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the right to opt out of the sale of their personal information. Cal. Civ. Code §1798.120(b).

166. Zoom violates Cal. Civ. Code §1798.120 by, *inter alia*, failing to notify consumers that it has acquired personal information from the consumer, that such information is being sold, and that the consumer has right to opt out of the sale of their personal information. Upon information and belief, users' personal information being transmitted to Facebook, LinkedIn, and other third parties in a manner which results in pecuniary gain for Zoom.

167. The CCPA provides that a consumer may commence a civil action if the consumer's nonencrypted and nonredacted personal information, as defined in Cal. Civ. Code §1798.150, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' 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.

168. Personal information is defined to include a username or email address in combination with a password or security question and answer that would permit access to an online

account. Cal. Civ. Code § 1798.81.5(d)(1)(B). By allowing user names and passwords to be exfiltrated, Zoom violated the CCPA.

169. As a result of Defendant's unlawful conduct, as alleged herein, Plaintiffs and California Sub-Class Members have suffered and will continue to suffer harm resulting from Zoom's conduct.

170. Plaintiffs seek damages on behalf of themselves and the California Sub-Class, as well as injunctive relief in the form of an order enjoining Zoom from continuing to violate the CCPA.

SEVENTH CAUSE OF ACTION
Violation of Consumer Legal Remedies Act
California Civil Code §§ 1750, *et seq*.
(On Behalf of Plaintiffs and the California Sub-Class)

171. Plaintiffs restate and reallege paragraphs 1 through 102 above as if fully set forth herein.

172. This cause of action is brought pursuant to the Consumers Legal Remedies Act, California Civil Code §§ 1750, *et seq*. (the "CLRA").

173. Plaintiffs and each member of the California Sub-Class are "consumers" within the meaning of Cal. Civ. Code § 1761(d).

174. Zoom is a "person" as defined by Cal. Civ. Code § 1761(c).

175. Zoom's marketing and sale of the Zoom app is the sale of a "good" and "service" to consumers within the meaning of Cal. Civ. Code §§ 1761(a)–(b), 1770(a).

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

177. By failing to maintain the privacy of Plaintiffs' and California Sub-Class Members' personal information, exposed as a result of inadequate security practices, protocols, and measures, Zoom has violated, and continues to violate, the CLRA in at least the following respects:

a. in violation of Civil Code § 1770(a)(5), Zoom represented that its product had characteristics which it did not have;

b. in violation of Civil Code § 1770(a)(7), Zoom represented that its product was of a particular standard, quality or grade, which it was not; and

c. in violation of Civil Code § 1770(a)(9), Zoom advertised its product with the intent not to provide what it advertised.

178. Zoom's unfair or deceptive acts and practices were capable of deceiving a substantial portion of the public. Zoom did not disclose the facts of its disclosure of personal information and its lack of capacity to secure videoconferences because it knew that consumers would not use its products or services, and instead would use other products or services, had they known the truth.

179. Zoom had a duty to disclose the truth about its privacy practices and security capabilities because it is in a superior position to know whether, when, and how it discloses users' personal information to third parties and whether it can ensure security in videoconferences.

180. Plaintiffs and the California Sub-Class Members could not reasonably have been expected to learn or discover Zoom's disclosure of their personal information to unauthorized parties or Zoom's lack of capacity to secure videoconferences.

181. The facts concealed by Zoom are material because a reasonable consumer would have considered them to be important in deciding whether to use Zoom.

182. Plaintiffs and the California Sub-Class Members reasonably expected that Zoom would safeguard their personal information from unauthorized disclosure and ensure Zoom's videoconferences were private.

183. As a result of Zoom's violation of the CLRA, Plaintiffs and the California Sub-Class Members suffered damages and did not receive the benefit of their bargain with Zoom because they paid for a value of services, either through personal information or a combination of their personal information and money.

184. Plaintiffs and the California Sub-Class Members request that this Court enjoin Zoom from continuing to engage in the unlawful and deceptive methods, acts and practices alleged above, pursuant to California Civil Code § 1780(a)(2). Unless Zoom is permanently enjoined from continuing to engage in such violations of the CLRA, future users of Zoom's platform will be damaged by its acts and practices in the same way as have Plaintiffs and the California Sub-Class Members.

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request the following relief:

a. An Order certifying this case as a class action;

b. An Order appointing Plaintiffs as the class representatives;

c. An Order appointing undersigned counsel as class counsel;

d. A mandatory injunction directing the Defendant to safeguard Plaintiffs' and Class Members' personal information;

e. An award of damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

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

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial as to all issues triable by a jury.

Dated: April 29, 2020

By: */s/ M. Anderson Berry*

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Leslie Guillon (SBN 222400)
lguillon@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

John A. Yanchunis
JYanchunis@ForThePeople.com
Ryan J. McGee
RMcGee@ForThePeople.com
Kenya J. Reddy
KReddy@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, Florida 33602

Telephone: (813) 223-5505
Facscimile: (813) 223-5402

Attorneys for Plaintiffs