Hassan A. Zavareei (State Bar No. 181547)
Katherine M. Aizpuru*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
hzavareei@tzlegal.com
kaizpuru@tzlegal.com

Annick M. Persinger (State Bar No. 272996)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6807
Facsimile: (202) 973-0950
apersinger@tzlegal.com

Counsel for Plaintiff and the Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SAMUEL TAYLOR,

On Behalf of Himself and All Others Similarly Situated,

Plaintiff,

v.

Zoom Video Communications, Inc.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT FOR DAMAGES, EQUITABLE, INJUNCTIVE, and DECLARATORY RELIEF

(1) NEGLIGENCE
(2) VIOLATION OF CAL. BUS. & PROF. CODE § 17200
(3) BREACH OF IMPLIED CONTRACT
(4) UNJUST ENRICHMENT
(5) PUBLIC DISCLOSURE OF PRIVATE FACTS
(6) VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT
(7) VIOLATION OF CONSUMER LEGAL REMEDIES ACT

JURY TRIAL DEMANDED

Plaintiff SAMUEL TAYLOR, on behalf of himself and all persons similarly situated, brings this complaint against Defendant Zoom Video Communications, Inc. ("Zoom").

I. INTRODUCTION

1. Zoom is a video communications provider, offering a cloud platform for video and audio conferencing, collaboration, chat, and webinars. Zoom promises customers that its products allow them to "meet securely" though "end-to-end encryption for all meetings, role-based user security, password protection, waiting rooms, and place attendee on hold."[1]

2. Although Zoom touts its commitment to customer privacy and security, Zoom does not disclose to customers that it routinely discloses their personally identifiable information ("PII") to unauthorized third parties, including social media network Facebook, Inc., without customer consent.

3. Zoom customers can access Zoom's services through mobile applications, as well as through desktop computers and telephones. Zoom promises customers that "Zoom Meetings for mobile provides the same great experience that you'd expect from the desktop client and more."[2]

4. But the iOS version of Zoom's mobile app sent customers' PII to Facebook for use in targeted advertising, without obtaining customers' consent—or even notifying customers of this practice.[3] Zoom provided this PII to Facebook even for Zoom customers who do not have Facebook accounts.

5. Each time a Zoom customer opened the iOS version of the Zoom app, Zoom would notify Facebook that the user had opened the app, details on the user's device such as the model, time zone, and city they were connecting from; and a unique advertiser identifier

---

[1] Zoom Meetings & Chat, https://zoom.us/meetings (last accessed March 30, 2020).
[2] *Id.*
[3] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account*, 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 (last accessed March 30, 2020 [hereinafter, *Zoom iOS App Sends Data*]).

created by the user's device which companies can use to target a user with advertisements.[4] Each of these device-specific identifiers can be linked to the individual identity of the Zoom customer.

6. Upon information and belief, Zoom provides customer PII to other unauthorized third parties for use in targeted advertising.

7. Reasonable customers do not understand that when they sign up to use Zoom's videoconferencing services that means that their PII will be provided to Facebook—a company that is notorious for lax security measures.

8. Zoom's conduct invaded the reasonable expectations of its customers, violating existing social norms and their concomitant legal standards.

9. Plaintiff downloaded and accessed the iOS version of the Zoom app. He was harmed when Zoom disclosed his PII to third parties without his consent.

II. PARTIES

23. Plaintiff Samuel Taylor is a resident of Florida. Mr. Taylor uses his Apple iPhone to access Zoom. He has downloaded, installed, and accessed the iOS version of the Zoom app. He was not aware, and did not understand, that Zoom would share information with Facebook and, upon information and belief, other third parties—including his city and time zone, the time he accessed the Zoom app, his device type, his mobile carrier, and a unique identifier tied to his device that would allow advertisers to specifically target him. He was not aware, and did not understand, that Zoom would allow third parties like Facebook to access this information and combine it with content and information from other sources to create a unique profile of him for advertising purposes. If Plaintiff had learned what he knows now about Zoom's data sharing policies, he would not have signed up for Zoom or he would not have used the iOS app to access it. Plaintiff did not consent to the sharing of his PII or any unauthorized party. He had no knowledge that Zoom had authorized this disclosure of his information and he did not consent to it.

---

[4] *Id.*

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

III. JURISDICTION AND VENUE

25. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, and members of the Class are citizens of different states from Defendant.

26. This Court has personal jurisdiction over Defendant because it maintains 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.

27. Venue is proper in this Court under 28 U.S.C. § 1391 because significant events giving rise 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.

IV. FACTUAL ALLEGATIONS

28. Zoom is a cloud-based video communications platform that offers companies and individuals the ability to hold video conferences, webinars, conference calls, and chats. Zoom claims that it can provide "video for every need," allowing customers to "join anywhere, on any device."[5]

29. Enterprise businesses, healthcare organizations, and educational institutions around the world use the Zoom platform every day to connect their teams and grow their organizations.[6] Thus, Zoom understands that its users need a video communications provider that provides secure communications. Thus, Zoom brags that it offers "end-to-end

---

[5] Zoom Meetings & Chat, https://zoom.us/meetings (last accessed March 30, 2020).
[6] Zoom Security Guide (June 2019) at 9, https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf (last accessed March 30, 2020).

encryption for all meetings, role-based user security, password protection, waiting rooms, and place attendee on hold," as measures to allow its users to "meet securely."[7]

30. Zoom promises its customers that "we take security seriously and we are proud to exceed industry standards when it comes to your organizations communications."[8] 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."[9] According to Zoom, it "places privacy and security as the highest priority in the lifecycle operations of our communications infrastructure . . . ."[10]

Zoom disclosed customer PII to unauthorized third parties.

31. Despite its supposed commitment to user privacy and security, in fact, unbeknownst to its customers, Zoom disclosed their PII to unauthorized third parties without customer consent.

32. 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.[11]

33. 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.[12]

34. 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.[13]

---

[7] *Id.*
[8] Security at Zoom, https://zoom.us/security (last accessed March 30, 2020).
[9] *Id.*
[10] Zoom Security Guide (June 2019) at 9, https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf (last accessed March 30, 2020).
[11] *Zoom iOS App Sends Data*, *supra* n.3.
[12] *Id.*
[13] *Id.*

35. 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.

36. 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.[14] 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.[15] 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.[16]

37. 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

---

[14] *See, e.g.*, Adjust Mobile Measurement Glossary, https://www.adjust.com/glossary/idfa/ (last accessed March 30, 2020).

[15] Jim Edwards, *Apple Wants More Advertisers to Use its iPhone Tracking System*, Business Insider (June 13, 2013), https://www.businessinsider.com/apples-idfa-and-ifa-tracking-system-2013-6 (last accessed March 30, 2020).

[16] 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), *available at* https://www.democraticmedia.org/sites/default/files/COPPA%20Rule%20Comments%20of%20Children%27s%20Privacy%20Advocates.pdf (last accessed March 30, 2020).

the IDFA, the information shared is extremely detailed and can be used to identify the user personally.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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, uers 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.

43. 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.

Zoom failed to obtain customer authorization before sharing PII.

44. 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.

45. Zoom's Privacy Policy again 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."[17]

46. 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[.]"[18] Zoom claimed that it collected this information "to provide you with the best experience with our products."[19]

47. 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.

---

[17] *See* Privacy Policy (Mar. 29, 2020), https://zoom.us/privacy (last accessed March 30, 2020); *see also* Privacy Policy (Mar. 18, 2020), *accessed via* https://web.archive.org/web/20200325143843/https://zoom.us/privacy (last accessed March 30, 2020).

[18] Privacy Policy (Mar. 18, 2020), *accessed via* https://web.archive.org/web/20200325143843/https://zoom.us/privacy (last accessed March 30, 2020).

[19] *Id.*

48. 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:

> 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. [20]

49. 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.

50. 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."[21]

51. Zoom violated its promises to its customers when it shared their PII without their authorization or consent. And by disclosing Plaintiff's 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.

---

[20] *Id*. *See also id*. ("Zoom does use certain standard advertising tools which require Personal Data (think, for example, Google Ads and Google Analytics). We use these tools to help us improve your advertising experience (such as serving advertisements on our behalf across the Internet, serving personalized ads on our website, and providing analytics services) . . . .")

[21] *Id*.

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

52. Zoom's conduct violated its users' privacy in a significant way.

53. 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, 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.

54. 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.[22]

55. 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

---

[22] Staff Report, "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy," Permanent Subcommittee on Investigations of the U.S. Senate Homeland Security and Governmental Affairs Committee (May 15, 2014), at 1, *available at* https://archive.org/stream/gov.gpo.fdsys.CHRG-113shrg89686/CHRG-113shrg89686_djvu.txt (last accessed March 30, 2020).

responded "very important,' 16% responded "somewhat important," and 26% responded "not too important."[23] 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.

56. Smartphone owners are especially active 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.[24]

57. 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."[25]

58. 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%.[26]

59. 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 algorithmically

---

[23] Lee Rainie, et al., Anonymity, Privacy, and Security Online, Pew Research Center 7, Sept. 5, 2013, available at https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/ (last accessed March 30, 2020).

[24] Jan Lauren Boyles, et al., Privacy and Data Management on Mobile Devices, Pew Research Center, Sept. 5, 2012, available at https://www.pewresearch.org/internet/2012/09/05/privacy-and-data-management-on-mobile-devices/ (last accessed March 30, 2020).

[25] Kristen Purcell, et al., Search Engine Use, Pew Research Center 2012, available at https://www.pewresearch.org/internet/2012/03/09/search-engine-use-2012/ (last accessed Mar. 30, 2020).

[26] Joseph Turow, et al., Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It (2009), available at http://ssrn.com/abstract=1478214 (last accessed Mar. 30, 2020).

targeted, the research suggests, is much the same as what we feel when our trust is betrayed in the analog world."[27]

60. 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.[28] 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.[29]

61. But even Facebook urged 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."[30] 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

---

[27] Sam Biddle, "You Can't Handle the Truth about Facebook Ads, New Harvard Study Shows" The Intercept, May 9, 2018, available at https://theintercept.com/2018/05/09/facebook-ads-tracking-algorithm/ (last accessed Mar. 30, 2020).

[28] *See, e.g.*, Josh Constine, Facebook now has 2 billion monthly users ... and responsibility, TechCrunch, https://techcrunch.com/2017/06/27/facebook-2-billion-users/ (last visited Mar. 30, 2020)

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

[30] Facebook Business Tools Terms, https://www.facebook.com/legal/technology_terms (last accessed Mar. 30, 2020).

include links showing "how and where users can opt-out."[31] Zoom did not display these disclosures or offer a link to Facebook's data collecting activity, or give users the opportunity to opt out.

62. 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 trust and of social norms.

63. Had consumers including Plaintiff 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 use, pay for, or pay as much for, the Zoom mobile application. As such, Plaintiff 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.

V. FRAUDULENT CONCEALMENT AND TOLLING

64. The applicable statutes of limitations are tolled by virtue of Zoom's knowing and active concealment of the facts alleged above. Plaintiff and the Class Members were ignorant of the information essential to the pursuit of these claims through no fault or their own and not due to any lack of diligence on their own part.

VI. CLASS ALLEGATIONS

65. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff, individually and on behalf of all others similarly situated, brings this lawsuit on behalf of himself and as a class action on behalf of the following Classes:

> **Class:** All persons who used the Zoom app for iOS during the applicable limitations period.

66. Excluded from the Class are any entities, including Defendant, and Defendant's officers, agents, and employees. Also excluded from the Class are counsel for Plaintiff, the judge assigned to this action, and any member of the judge's immediate family.

---

[31] *Id.*

67. Members of the Class are so numerous that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff, it is believed that the Class is comprised of thousands of members.

68. Common questions of law and fact exist as to all members of the Class. These questions predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Class. Such common and legal factual questions include:

a. Whether Defendant's acts and practices complained of herein amount to egregious breaches of social norms;

b. Whether Defendant violated Plaintiff's and Class Members' privacy rights;

c. Whether Defendant acted negligently;

d. Whether Plaintiff and the Class Members were harmed;

e. Whether Defendant intruded upon Plaintiff's and the Class Members' seclusion;

f. Whether Defendant and Plaintiff formed implied contracts;

g. Whether Defendant breached implied contracts with Plaintiff and the Class Members;

h. Whether Defendant's conduct was unfair;

i. Whether Defendant's conduct was fraudulent;

j. Whether Defendant omitted or misrepresented material facts regarding the PII of Plaintiffs and Class Members it shared with third parties, including Facebook;

k. Whether Defendants owed duties to Plaintiff and Class Members to disclose that it was sharing their PII with third parties, including Facebook;

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

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

69. Plaintiff's claims are typical of the members of the Class as all members of the Classes are similarly affected by the Defendant's actionable conduct. Defendant's conduct that gave rise to the claims of Plaintiff and members of the Classes is the same for all members of the Classes.

70. Plaintiff will fairly and adequately protect the interests of the Classes because they have no interests antagonistic to, or in conflict with, the Classes that Plaintiff seeks to represent. Furthermore, Plaintiff has retained counsel experienced and competent in the prosecution of complex class action litigation, including data privacy litigation.

71. Class action treatment is a superior method for the fair and efficient adjudication of this controversy, in that, among other things, such treatment will permit a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

72. Plaintiff knows of no difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

73. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

74. Plaintiff suffers a substantial and imminent risk of repeated injury in the future.

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

76. The State of California has sufficient contacts to Defendant'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.

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

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

79. 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. Zoom instructs users with questions about privacy to contact Zoom at an address in San Jose.

80. 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.

VII. CLAIMS FOR RELIEF

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

81. Plaintiff re-alleges and incorporates the allegations in Paragraphs 1 through 79 set forth above as if fully written herein.

82. As alleged herein, Plaintiff and the Class Members enjoy a special relationship with Defendant.

83. Defendant provided services to Plaintiff 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 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 Defendant.

84. Defendant owed a duty to Plaintiff 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's and the Class Members' PII.

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

86. It was entirely foreseeable to Defendant that Plaintiff and the Class Members would be harmed if Defendant disclosed their PII to third parties for advertising purposes.

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

88. Defendant'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, Defendant has not taken sufficient actions to prevent the unauthorized disclosure of PII.

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

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

COUNT II
Violation of California Unfair Competition Law ("UCL")
(On behalf of Plaintiff and the Class)

91. Plaintiff re-alleges and incorporate the allegations in Paragraphs 1 through 79 set forth above as if fully written herein.

92. Plaintiff has standing to pursue this cause of action because Plaintiff suffered injury in fact as a result of Defendant's misconduct described herein.

93. As described herein, Defendant advertised their products and services as

94. Plaintiff 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 PII going forward.

95. 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. Defendant has engaged in business acts and practices that, as alleged above, constitute unfair competition in violation of Business and Professions Code section 17200.

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

97. Defendant'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.

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

99. Defendant's business practices described herein also violate the UCL because Defendant falsely represented that goods or services have characteristics they do not have, namely, good security; 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.

100. As a result of Defendant's unfair business practices, Plaintiff and the Class Members suffered injury.

101. If Defendant 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, Plaintiff and the Class have no adequate remedy at law in that Defendant will continue to engage in the wrongful conduct alleged herein, thus engendering a multiplicity of judicial proceedings. Plaintiff and the Class request and are entitled to injunctive relief, enjoining Defendant from engaging in the unfair and fraudulent acts described herein.

102. Had consumers including Plaintiff 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 use, pay for, or pay as much for, the Zoom mobile application. As such, Plaintiff 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.

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

COUNT III
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

104. Plaintiff re-alleges and incorporate the allegations in Paragraphs 1 through 79 set forth above as if fully written herein.

105. Defendant offered its videoconferencing capabilities to Plaintiff and the Class Members. In exchange, Defendant received benefits in the form of monetary payments and access to Plaintiff's valuable personal information.

106. Defendant has acknowledged these benefits and accepted or retained them.

107. Implicit in the exchange of the products and services for the benefits provided by Plaintiff and the Class Members is an agreement that Defendant would safeguard their personal information.

108. Without such implied contracts, Plaintiff and the Class Members would not have paid for and conferred benefits on Defendant, but rather would have chosen an alternative videoconference platform that did not share their PII with undisclosed and unauthorized third parties.

109. Plaintiff and the Class Members fully performed their obligations under their implied contracts with Defendant, but Defendant did not.

110. Defendant breached its implied contracts with Plaintiff and the Class Members when it disclosed their PII to unauthorized third parties like Facebook. These circumstances are such that it would be inequitable for Defendant to retain the benefits received.

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

112. Had consumers including Plaintiff 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 use, pay for, or pay as much for, the Zoom mobile application. As such, Plaintiff 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.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiff and the Class)

113. Plaintiff re-alleges and incorporate the allegations in Paragraphs 1 through 79 set forth above as if fully written herein, and to the extent necessary, assert this count in the alternative to the breach of implied contract claim.

114. Defendant has profited and benefited from the use of its videoconferencing services by Plaintiff and the Class in exchange for monetary benefits and access to PII.

115. Defendant 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, Plaintiff and the Class Members did not receive products of the quality, nature, fitness or value represented by Defendant and that reasonable consumers expected.

116. Defendant has been unjustly enriched by its withholding of and retention of these benefits, at the expense of Plaintiff and the Class Members.

117. Equity and justice militate against permitting Defendant to retain these profits and benefits.

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

COUNT V
Invasion of Privacy (Public Disclosure of Private Facts)
(On behalf of Plaintiff and the Class)

119. Plaintiff re-alleges and incorporate the allegations in Paragraphs 1 through 79 set forth above as if fully written herein.

120. Plaintiff 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.

121. The reasonableness of such expectations of privacy is supported by Zoom's unique position to monitor Plaintiff'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.

122. Plaintiff'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.

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

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

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

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

127. Defendant's actions were a substantial factor in causing the harm suffered by Plaintiff and Class Members.

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

COUNT VI
Violation of California's Consumer Privacy Act
(On behalf of Plaintiff and the Class)

129. Plaintiff re-alleges and incorporate the allegations in Paragraphs 1 through 79 set forth above as if fully written herein.

130. California's Consumer Privacy Act ("CCPA") protects consumers' personal information from collection and use by businesses without consumers' notice and consent.

131. Defendant violated the CPPA by using customers' PII without providing the required notice under the CPPA. *See* Cal. Civ. Code § 1798.100(b). Defendant did not notify

Plaintiff and the Class Members that it was disclosing their PII to unauthorized parties like Facebook.

132. Defendant also violated the CPPA by failing to provide notice to its customers of their right to opt-out of the disclosure of their PII to unauthorized parties like Facebook. *See* Cal. Civ. Code § 1798.120(b). Defendant did not give Plaintiff and the Class Members the opportunity to opt out before it provided their PII to unauthorized parties like Facebook.

133. Plaintiff seeks injunctive relief in the form of an order enjoining Defendant from continuing to violate the CPPA, as well as actual damages on behalf of himself and the Class.

COUNT VII
Violation of California's Consumer Legal Remedies Act ("CLRA")
Civ. Code §§ 1750 *et seq.*
(On behalf of Plaintiff and the Class)

125. Plaintiff re-alleges and incorporate the allegations in Paragraphs 1 through 79 set forth above as if fully written herein.

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

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

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

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

130. Defendant violated the CLRA by engaging in unfair and deceptive practices and by causing harm to Plaintiff and the Class.

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

132. Defendant's failure to disclose this practice violated the CLRA in multiple ways:

a. Defendant represented that its product had characteristics it did not have, Cal. Civ. Code § 1770(a)(5);

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

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

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

133. Defendant'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 disclosure of PII because it knew that consumers would not use its products, and instead would use other products, if they knew the truth.

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

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

136. Plaintiff and the Class Members reasonably expected that Zoom would safeguard their PII and not disclose it without their consent.

137. Due to Defendant's violations of the CLRA, Plaintiff and the Class Members suffered injury.

138. Had consumers including Plaintiff 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 use, pay for, or pay as

much for, the Zoom mobile application. As such, Plaintiff 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.

139. Plaintiff and the Class Members seek an injunction barring Zoom from disclosing their PII without their consent.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Class Members, respectfully requests that this Court enter a Judgment:

(a) Certifying the Classes and appointing Plaintiff as Class Representative;

(b) Finding that Defendant's conduct was unlawful as alleged herein;

(c) Awarding such injunctive and other equitable relief as the Court deems just and proper; and

As to Counts I through VI:

(d) Awarding Plaintiff and the Class Members nominal, actual, compensatory, consequential, and punitive damages;

(e) Awarding Plaintiff and the Class Members pre-judgment and post-judgment interest;

(f) Awarding Plaintiff and the Class Members reasonable attorneys' fees, costs, and expenses; and

(g) Granting such other relief as the Court deems just and proper.

IX. JURY DEMAND

Plaintiff demands trial by jury on all counts for which a jury trial is permitted.

Dated: March 31, 2020

Respectfully submitted,

/s/ Hassan A. Zavareei

Hassan A. Zavareei (State Bar No. 181547)
Katherine M. Aizpuru*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036

Telephone: (202) 973-0900
Facsimile: (202) 973-0950
Email: hzavareei@tzlegal.com
kaizpuru@tzlegal.com

Annick M. Persinger (State Bar No. 272996)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6807
Facsimile: (202) 973-0950
Email: apersinger@tzlegal.com

**pro hac vice* application forthcoming

Counsel for Plaintiff and the Class