

LAW OFFICES OF JOHN L. FALLAT

John L. Fallat (SBN #114842)

Timothy J. Tomlin (SBN #142294)

Mark A. Vaughn (SBN #241228)

68 Mitchell Blvd., Suite 135

San Rafael, CA 94903-2046

Telephone: (415) 457-3773

Facsimile: (415) 457-2667

Email: jfallat@fallat.com

Email: ttomlin@fallat.com

Email: mvaughn@fallat.com

Attorneys for Plaintiff

VICTOR M. RIOS

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

**VICTOR M. RIOS, individually and on
behalf of himself and all others
similarly situated,**

Plaintiff,

vs.

**ZOOM VIDEO COMMUNICATIONS,
INC.,**

Defendant.

Case No.: _____

Class Action

**CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL**

**CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL**

1. Plaintiff Victor M. Rios ("Dr. Rios"), ("Plaintiff"), on behalf of himself and all others similarly situated (the "Class," as defined in paragraph 94 below), submit this complaint against defendant Zoom Video Communications, Inc. ("Zoom") for, among other things, negligence, breach of implied contract, and violations of the California Consumer Privacy Act ("CCPA"), the Consumers Legal Remedies Act ("CLRA"), and the Unfair Competition Law ("UCL"). In support of these claims, Plaintiff alleges the following (a) upon personal knowledge with respect to the matters pertaining to himself, and (b) upon information and belief with respect to all other matters, based upon, among other things, the investigations undertaken by Plaintiff's counsel. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth below after a reasonable opportunity for discovery.

INTRODUCTION

2. Dr. Rios, is an accredited scholar with a Ph.D. in Comparative Ethnic Studies from the University of California, Berkeley, 2005. He is currently serving as the Associate Dean of Social Sciences, Division of Social Sciences, at the University of California, Santa Barbara. (please see his *curriculum vitae* attached as Exhibit 1). He is an accomplished speaker and presenter as shown by his TED participations in 2012 and 2015. As part of his career as an educator, he reaches out to others through seminars and training in person and through video to educate underserved communities such as minority students to encourage and engage in higher education and on-line learning.

3. Dr. Rios retained Zoom to provide himself and approximate 400 participants with a secure videoconferencing platform, Zoom allowed a "known offender" - one who "has been reported multiple times to the authorities" - to

1 Zoombomb his webinar on April 30, 2020. As a result, Dr. Rios, and other
 2 attendees of the webinar - most of whom were other public school teachers -
 3 had their computer screens hijacked and their control buttons disabled while
 4 being forced to watch pornographic video footages. The footages were beyond
 5 perverse, portraying an adult engaging in a sexual act on an infant.

6 4. Because of Zoom's utter failure in providing security, Dr. Rios'
 7 webinar was Zoombombed twice within minutes. Traumatized and helpless, Dr.
 8 Rios attempted to console his attendees, and allowing them time to talk about
 9 and process what had just happened. He immediately reached out to Zoom and
 10 demanded action to rectify the situation and to improve security for future
 11 videoconferences, but Zoom did nothing.

12 5. Unfortunately, Dr. Rios and his participants in his webinar were
 13 not the only victims of Zoombombing. Indeed, many other Zoom users,¹
 14 including schoolchildren,² fell victim to similar deeply disturbing and
 15 traumatizing experiences due to Zoom's failure to maintain adequate security in
 16 Zoom videoconferences.³ As detailed below, Zoom prioritizes profit and
 17 revenue over data protection and user security while millions of users in
 18 the United States registered with Zoom based on its false advertisements and
 19

20
 21
 22 ¹ Colleen Shalby, "Disturbing Zoom-Bombing" incident Hits Fresno State Students, Official
 23 Say, L.A. TIMES, Apr. 23, 2020, available at <https://www.latimes.com/California/story/2020-04-23/coronaviruszoom-bombing-fresno-state> (May 11, 2020).

24 ² Valarie Honeycutt Spears, Pornographic Video Appeared During "Zoom bombing" in a KY
 25 school Virtual meeting, LEXINGTON HERALD LEADER, Apr. 7, 2020, available at
 26 <https://www.kentucky.com/news/local/education/article241809326.html> (last visited May 11, 2020).

27 ³ FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19
 Pandemic, FBI (Mar. 30, 2020), available at <https://www.fbi.gov/contact-us/fieldoffices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijackingduring-covid-19-pandemic> (May 11, 2020).

1 rely on Zoom's platform to conduct their business during this pandemic. This
2 civil complaint will apparently be the sixth (6th) one filed in this USDC based
3 upon this outrageous conduct.

4 6. On behalf of Plaintiff and other similarly situated Class members,
5 this class action seeks equitable relief against Zoom and damages sustained by
6 the Class as a result of Zoom's:

- 7 • unlawful sharing of users' personal information with third
8 parties including Facebook, Inc., without adequate notice to or
9 authorization from users;
- 10 • failure to safeguard its users' confidential, sensitive personal
11 information;
- 12 • failure to provide adequate security, as promised, to avoid
13 breach and infiltration (e.g., "Zoombombing") of users'
14 videoconferences; and
- 15 • unfair, unlawful, and deceptive business practices relating to
16 Zoom's data security.

17 7. Zoom provides video-communication services using a cloud
18 platform for video and audio conferencing, collaboration, chat, and webinars.
19 Founded in 2011, Zoom became a publicly traded company just a year ago (in
20 April 2019), and reported over \$622,658,000 in revenue for the fiscal year
21 ending January 31, 2020. Today, Zoom has a market capitalization of 56 billion.
22 Millions of consumers use Zoom's services daily.

23 8. In the wake of the global COVID-19 pandemic, demand for
24 Zoom's services exploded because hundreds of millions of people - all under
25 stay-at-home orders – resort to videoconferencing to connect with others for
26

1 work and social functions. In recent weeks, Zoom has become the virtual
2 classroom for millions of schoolchildren and workspace for many businesses
3 and government agencies. The number of meeting participants across Zoom has
4 jumped from 10 million in December 2019 to 200 million in March 2020.

5 9. As the usage of Zoom's services skyrockets, so do its collection
6 and use of users' personal information. The importance of security of Zoom's
7 videoconferences cannot be overstated because Zoom provides services to many
8 critical government agencies responsible for combating the COVID-19
9 pandemic, including the Center for Disease Control and Prevention ("CDC")
10 and the U.S. Department of Homeland Security ("DHS")⁴ but as to members of
11 the general public such as Dr. Rios and the class, appear to not care very much
12 at all about security and privacy issues.

13 10. While Zoom enjoyed its success due to the hike of revenues and its
14 stock price resulting from the explosion of demands for its services, Zoom's
15 unlawful collection and use of users' personal information and its lack of
16 adequate security came to light in a series of articles published in late March
17
18
19
20
21
22
23

24
25 ⁴ Zoom for Government, available at <https://zoom.us/government> (last visited Apr. 6, 2020)
26 (featuring photos of law enforcement and military personnel at work and listing under "Organizations that love
27 Zoom" eight government agencies, including the CDC, DHS, the Colorado Department of Corrections, the
Hawaii State Department of Health the Los Angeles Police Department, and the City of San Jose), whereas the
US DOD has banned use between service members and DOD civilians (www.starsandstripes) (April 14, 2020).

1 and early April 2020 in Vice,⁵ The New York Times,⁶ the Washington Post,⁷
 2 The Wall Street Journal,⁸ and other news outlets.⁹

3 11. As revealed in these news reports, Zoom uses data-mining tools to
 4 collect users' personal information and shares it with third parties without users'
 5 consent. Zoom allows these third parties to use such personal information to
 6 target users with advertisements.

7 12. Zoom also fails to implement proper security measures to protect
 8 users' privacy and secure their videoconferences. As a result, "Zoombombing"
 9 by uninvited participants has become frequent. Contrary to Zoom's promises,
 10 Zoom's videoconferences are not end-to-end (also known as "E2E") encrypted.
 11 This means that in addition to the participating users, Zoom has the technical
 12 ability to spy on the videoconferences and, when compelled by the government
 13 or others, to reveal the contents of the videoconferences without the users'
 14 consent.

15 13. Zoom's privacy violations and security breaches quickly
 16 commanded the attention of 27 state attorneys general and the Federal Bureau
 17

18
 19
 20 ⁵ Joseph Cox, Zoom iOS App Sends Data to Facebook Even If You Don't Have a Facebook
 21 Account VICE, Mar. 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 visited May 11, 2020)(the "vice Report").

22 ⁶ Taylor Lorenz & Davey Alba, "Zoombombing" Becomes a Dangerous Organized Effort,
 23 THE NEW YORK TIMES, Apr. 3, 2020 (the "Times Zoombombing Report"); Aaron Krollik & Natasha
 24 Singer, a Feature on Zoom Secretly displayed Data from People's LinkedIn Profiles, THE NEW YORK
 25 TIMES, Apr.2, 2020 (the Times LinkedIn Report").

26 ⁷ Drew Harwell, Everybody Seems to be Using Zoom. But Its Security flaws Could Leave
 27 users at Risk, THE WASHINGTON POST, Apr. 2, 2020 (the "Post Report").

⁸ Aaron Tilley & Robert McMillan, Zoom CEO: "I Really Messed Up" on Video Platform's
 Security, THE WALL STREET JOURNAL, Apr. 4, 2020 (the WSJ Report").

⁹ Micah Lee & Yael Grauer, Zoom Meetings Aren't End-to-End Encrypted, Despite
 Misleading Marketing, THE INTERCEPT, Mar. 31, 2020, available at
<https://theintercept.com/2020/03/31/zoom-meeting-encryption/> (last visited May 11, 2020).

1 of Investigation ("F.B.I."). On March 30, 2020, the New York Attorney General
2 sent a letter to Zoom expressing concerns over and inquiring about its data-
3 privacy and security practices. And on March 31, 2020, the F.B.I. issued a
4 warning singling out Zoom based on "multiple reports of conferences being
5 disrupted by pornographic and/or hate images and threatening language." *See*
6 *Post Report*, fn. 7.

7 14. While millions of consumers and thousands of businesses and
8 government agencies continue to rely on Zoom to conduct their business during
9 the COVID-19 pandemic, the data-privacy violations and security
10 vulnerabilities at Zoom remain unremedied.

11 15. By bringing this class action on behalf of themselves and other
12 Zoom users, Plaintiff seeks (a) damages for his loss of revenue and reputation
13 for Zoom's violations of his and the privacy rights of the class and its unfair,
14 unlawful, and deceptive business practices; and (b) restitution and injunctive
15 relief prohibiting Zoom from continuing its unfair, unlawful, and deceptive
16 business practices.

17 PARTIES

18 I. Victor M. Rios

19 16. Plaintiff Dr. Rios is a citizen of California.

20 17. Dr. Rios registered an account with Zoom on April 13, 2020 using
21 an Apple computer at his home office. He has registered this account with
22 Zoom for personal use, to stay in contact with his current and former clients,
23 using his personal email address and personal computer.

24 18. Dr. Rios was not aware, and did not understand, that Zoom would
25 share his personal information with third parties, including Facebook. Nor was
26

1 he aware that Zoom would allow third parties, like Facebook, to access his
2 personal information and combine it with content and information from other
3 sources to create a unique identifier or profile of him for purposes of
4 advertisement.

5 19. In fact, Dr. Rios registered with Zoom as a user and used Zoom's
6 services in reliance on Zoom's promises that (a) Zoom does not sell users' data;
7 (b) Zoom takes privacy seriously and adequately protects users' personal
8 information; and (c) Zoom's videoconferences are secured with end-to-end
9 encryption and are protected by passwords and other security measures.

10 II. Defendant Zoom Video Communications, Inc.

11 20. Defendant Zoom Video Communications, Inc. is a Delaware
12 corporation with its principal place of business in San Jose, California. Zoom
13 was founded in 2011 and became a public company in April 2019. Today, Zoom
14 employs a staff of over 1,700 and generates hundreds of millions of dollars in
15 annual revenue.

16 21. Zoom provides video-communication services. The demand for
17 Zoom's services has exploded in the wake of the COVID-19 pandemic while
18 hundreds of millions of Americans are under orders to stay at home. As a result
19 of the explosion of user demand, Zoom's stock price skyrocketed in recent
20 months. On June 1, 2020, Zoom's stock closed at above \$204.00 per share –
21 nearly tripling its closing price at the beginning of 2020.
22

23 JURISDICTION AND VENUE

24 22. This Court has subject-matter jurisdiction under the Class Action
25 Fairness Act of 2005, 28 U.S.C. § 1332(d)(2). The matter in controversy,
26
27

1 exclusive of interest and costs, exceeds the sum or value of \$5,000,000, and
2 members of the Class are citizens of different states from Zoom.

3 23. This Court has personal jurisdiction over Zoom because it
4 maintains headquarters in San Jose within the County of Santa Clara, over
5 which this District presides. Zoom regularly conducts business in this District.

6 24. Venue is proper in this Court under 28 U.S.C. § 1391 because (a)
7 Zoom transacts business in this District; (b) substantial events and transactions
8 giving rise to this action took place in this District; and (c) many members of
9 the Class reside in this District.

10 INTRADISTRICT ASSIGNMENT

11 25. In compliance with Local Rule 3-2(b), Plaintiff requests that this
12 action be assigned to the San Jose Division of this District because a substantial
13 part of the events or conduct giving rise to the claims in this action occurred in
14 the County of Santa Clara, and this complaint appears to be the sixth (6th) case
15 filed on these issues in the Division largely assigned to the Honorable Lucy Koh.

16 FACTUAL ALLEGATIONS

17 I. Zoom Targets Consumers, Businesses, and Government 18 Agencies with Promises of Protecting User Privacy and Ensuring Data 19 Security

20 26. A fast-growing tech company founded in San Jose in 2011, Zoom
21 provides a "video-first communications platform that ... connect[s] people
22 through frictionless video, phone, chat, and content sharing and enable[s] face-
23 to-face video experiences for [up to] thousands of people in a single meeting
24
25
26
27

1 across disparate devices and locations."¹⁰ Zoom generates revenue from the
2 "sale of subscriptions to [its] platform." Zoom Annual Report at 13. As Zoom
3 itself acknowledges, "security and privacy" are among the key factors affecting
4 its growth and revenue. *Id.*

5 27. Zoom regularly collects from its users a massive volume of
6 personal information, including names, usernames, physical addresses, email
7 addresses, phone numbers, employment information, credit/debit cards, and
8 cookies and pixels, e.g., through the use of Google Analytics and Google Ads.
9 When users visit Zoom's websites, such as zoom.us and zoom.com, Zoom uses
10 "cookies and tracking technologies" to collect valuable personal data from
11 users:

12 **Zoom collects information about you when you**
13 **visit our marketing websites**, unless you tell us not to
14 by adjusting your cookie setting. We use such things as
15 cookies and tracking technologies from our advertising
16 service provider tools (e.g., Google Ads). Information
17 collected includes Internet protocol (IP) addresses,
18 browser type, Internet service provider (ISP), referrer
19 URL, exit pages, the: files viewed on our marketing sites
20 (e.g., HTML pages, graphics, etc.), operating system,
21 date/time stamp, and/or clickstream data.
22

23
24
25
26 ¹⁰ Zoom's 2020 Annual report filed in Form 10-K on March 20, 2020 with the U.S. Securities
27 and Exchange Commission, at 4, available at <https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa> (visited Apr. 6, 2020) ("Zoom Annual Report").

We use this information to determine the offers to make for our services, analyze trends on and run the marketing site, and understand users' movements around the marketing site. We also gather information about our visitors, such as location information at the city level (which we get from IP addresses) for tailoring advertising and selecting the language to use to display the website.

Zoom does use certain standard advertising tools on our marketing sites which, provided you have allowed it in your cookie preferences, sends personal data to the tool providers, such as Google.

Zoom Privacy Policy, available at <https://zoom.us/privacy> (last visited Apr.6, 2020).¹¹ Even though Zoom concedes that its "use" of personal information "may be considered a 'sale' within the meaning of the CCPA, Zoom insists that it "is not selling any data."

28. In fact, Zoom boasts of its commitment to user privacy:

Privacy is an extremely important topic, and we want you to know that at Zoom, we take it very seriously

- **We do not sell your personal data. ...**

Zoom collects only the user data that is required to provide you Zoom services. This includes technical and operational support and service improvement. For example, we collect information such as a user's IP address and OS and device details to deliver the best possible Zoom experience to you regardless of how and from where you join.

¹¹ Unless otherwise noted, all emphases are added.

- **We do not use data we obtain from your use of our services, including your meetings, for any advertising.** We do use data we obtain from you when you visit our marketing websites, such as zoom.us and zoom.com. You have control over your own cookie settings when visiting our marketing websites.

29. Zoom also advertises that it "take[s] security seriously." On its website, Zoom boasts that it "exceed[s] industry standards" in terms of security measures. Zoom further promises that it "is committed to protecting [users'] privacy," and claims that it has "designed policies and controls to safeguard the collection, use, and disclosure of [users'] information." According to Zoom, it "places privacy and security as the highest priority in the lifecycle operations of our communications infrastructure..."

30. With regard to security in videoconferences, Zoom has, in various parts of its website and in its marketing materials, represented that it uses end-to-end (or E2E) encryption to secure its videoconferences:

Meet securely

End-to-end encryption for all meetings ...

Protect your Meetings

The following in-meeting security capabilities are available to the meeting host:

- **Secure a meeting with end-to-end encryption**

* * *

Enables HIPPA, PIPEDA & PHIPA Compliance

Zoom's solution and security architecture provides end-to-end encryption and meeting access controls so data in transit cannot be intercepted.

31. As noted in the Intercept Report, Zoom's bald and unequivocal promise of end-to-end encryption is important to consumers because it is "widely understood as the most private form of internet communication." An end-to-end encrypted videoconference means that "the video and audio content [are] encrypted in such a way that only the participants in the meeting have the ability to decrypt it." See Intercept Report. In other words, only the videoconference participants themselves - not Zoom or any other third parties - have access to the contents of their videoconferences.

32. As detailed below, however, Zoom's promise of end-to-end encryption is false. In fact, in response to the Intercept's revelation of its false promises regarding end-to-end encryption, a Zoom spokesperson admitted in late March 2020 that "[c]urrently, it is not possible to enable E2E encryption for Zoom video meetings" due to the design and operation of Zoom's platform.

33. In addition to end-to-end encryption, Zoom also boasts its capacity to "secure" a meeting "with password" using its "[r]ole-based user security":

Client Application

Role-based user security

The following pre-meeting security capabilities are available to the meeting host:

Enable an end-to-end (E2E) encrypted meeting

- Secure log-in using standard username and password ... sign-on
- Start a secured meeting with password

- Schedule a secured meeting with password

* * *

Meeting Security

Role-based user security

The following m-meeting security capabilities are available to the meeting host:

- Secure a meeting with E2E encryption

...

- Expel a participant or all participants

- End a meeting

- Lock a meeting

...

- Mute/unmute a participant or all participants

...

- Enable/disable a participant or all participants to

record ...

See Zoom Security Guide, available at <https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf> (last visited Apr. 6, 2020). As detailed below, however, Zoom's representations regarding security of its videoconferences are false because "'Zoombombing' ... by uninvited participants ha[s] become frequent." *See* fn. 6, New York Times Zoombombing Report.

34. Yet Zoom profits from these false promises of data protection and security. Before the COVID-19 outbreak, Zoom induced - using these false promises - millions of consumers, as well as business and government agencies, to register for its services. The volume of Zoom's business generated an annual

1 revenue of \$622.7 million in the fiscal year of 2020 (ending January 31, 2020).
2 *See* fn. 10, Zoom Annual Report at 38. In April 2019, Zoom issued 20 million
3 shares of its common stock at \$36 per share in a successful initial public
4 offering.

5 35. Since the outbreak of the COVID-19 pandemic, the demand for
6 Zoom's services has skyrocketed:

7 Zoom was used by more than 200 million callers
8 [in March 2020], up from 10 million in December
9 [2019], and is used in more than 90,000 schools
10 across 20 countries More than 5 million people
11 in the United States used Zoom's mobile apps on
12 [April 1, 2020], five times more than a month ago,
13 dwarfing the competition of its top rivals, including
14 Skype, Slack, Google Hangouts and Microsoft
15 Teams
16

17 *See* Post Report. According to the app data firm SensorTower, "first-time
18 installs of the videoconferencing company's mobile app rose by 1,126 percent
19 in March to more than 76 million, up from just 6.2 million in February. "*See*
20 fn. 6, New York Times Zoombombing Report.
21

22 36. Likewise, Zoom's stock price has skyrocketed. Today, Zoom
23 amasses over \$57 billion in market capitalization. Zoom's exponential growth
24 of market capitalization is predicated upon users' trust in its promises of data
25 privacy and security, but these promises are false.
26
27

II. Zoom Broke Its Promises of Data Privacy and Security

A. Zoom Collected and Disclosed Users' Personal Information Without Authorization or Consent

37. Zoom's promises of data privacy and security are false. As revealed in the Vice Report, the iOS version of Zoom's mobile app sent users' personal information to Facebook for use in targeted advertising, without first notifying the users or obtaining their consent. Zoom provided users' personal information to Facebook even for users who do not have Facebook accounts. *See* fn. 5, Vice Report.

38. According to the Vice Report, upon downloading and opening the app, Zoom would connect to Facebook's Graph API ("application program interface") a primary way to get data into and out of the Facebook platform.

39. When a Zoom user opens the iOS version of the Zoom app, Zoom would notify Facebook that the user has opened the app and identify the user's device, i.e., the model, time zone, physical location, and telephone carrier. Such personal information then generates a unique identifier that enables companies like Facebook to target the user with advertisements. Advertisers then use the identifier to track data so that they can deliver customized advertising. The identifier is also used for tracking and identifying a user, allowing whoever is tracking it to identify a user when he or she interacts with or responds to advertisements. An identifier is similar to a cookie as it allows advertisers to know that a specific user is viewing a specific publication so that it can serve an advertisement targeting that user. Such identifiers are extremely valuable in the online advertising industry.

1 40. According to one privacy-protection expert, Zoom's practices
2 of data collection and data sharing are "shocking," because "[t]here is
3 nothing in [Zoom's] privacy policy that addresses that." *Id.*

4 41. Aside from the lack of any notice, Zoom's data-sharing activity
5 was not visible to users because they can only see the Zoom app interface.
6 Thus, Zoom provides users **no opportunity to consent to or opt out of**
7 Zoom's data-sharing with Facebook. Zoom's lack of disclosure and failure to
8 provide an opportunity to opt out is particularly glaring in light of Facebook's
9 own admonition to developers like Zoom to give notice:
10

11 Facebook told [Vice] it requires developers to be transparent with
12 users about the data their apps send to Facebook. Facebook's terms
13 say "If you use our pixels or SDK [(software development kits)], you
14 further represent and warrant that you have provided robust
15 and sufficiently prominent notice to users regarding the Customer
16 Data collection, sharing and usage," and specifically for apps, "that
17 third parties, including Facebook, may collect or receive information
18 from your app and other apps and use that information to provide
19 measurement services and targeted ads." *Id.*
20

21 42. Indeed, after being confronted with Vice's findings, "Zoom
22 confirmed the data collection in a statement to [Vice]":

23 We originally implemented the 'Login with Facebook'
24 feature using the Facebook SDK in order to provide our users with
25 another convenient way to access our platform. However, we were
26
27

1 recently made aware that the Facebook SDK was collecti.ng
2 unnecessary device data [as identified by Vice.]...

3 To address this, in the next few days, we will be removing the
4 Facebook SDK and reconfiguring the feature so that users will still
5 be able to login with Facebook via their browser. Users will need to
6 update to the latest version of our application once it becomes
7 available in order for these changes to take hold, and we encourage
8 them to do so. We sincerely apologize for this oversight, and remain
9 firmly committed to the protection of our users' data. *Id.*

10
11 43. Despite admitting to the "oversight" and purporting to release a
12 new version of the Zoom app (as of March 27, 2020) as a remedy, the harm to
13 Plaintiff and other Class members, as well as the violations of their privacy,
14 have occurred and continue to occur because, even assuming no unauthorized
15 disclosure of personal information is made through the new version, the
16 previous version of the app remains operational. Moreover, Zoom failed to
17 mandate the use of the new version of the app. Nor did Zoom do anything to
18 rectify its previous egregious violations of users' privacy rights.

19 44. Upon information and belief, Zoom provides users' personal
20 information to other third parties, in addition to Facebook, for unauthorized
21 purposes, including use in targeted advertising.

22 45. Plaintiff and other reasonable Zoom users did not know that when
23 they signed up to use Zoom's services that Zoom would share their personal
24 information with third parties for the purpose and in the manner set forth above,
25 and that their privacy rights would be violated. Had Plaintiff and other users
26
27

1 known about Zoom's data-sharing practices, they would not have signed up
2 with Zoom and would not have used Zoom's services.

3 46. Zoom's unlawful disclosure of users' personal information is not
4 limited to Facebook. According to the Times LinkedIn Report (fn. 6), Zoom
5 used data-mining tools to collect users' personal information without
6 authorization, then used the personal information to match the users' LinkedIn
7 profiles:

8 For Americans sheltering at home during the coronavirus
9 pandemic, the Zoom videoconferencing platform has become
10 a lifeline, enabling millions of people to easily keep in touch
11 with family members, friends, students, teachers and work
12 colleagues.

13 But what many people may not know is that, until Thursday, a
14 data- mining feature on Zoom allowed some participants to
15 surreptitiously have access to LinkedIn profile data about other
16 users -without Zoom asking for their permission during the
17 meeting or even notifying them that someone el.se was snooping
18 on them.

19 The undisclosed data mining adds to growing concerns about
20 Zoom's business practices at a moment when public schools,
21 health providers, employers, fitness trainers, prime ministers and
22 queer dance parties are embracing the platform.

23
24 An analysis by *The New York Times* found that when people
25 signed in to a meeting, *Zoom's software automatically*
26 *sent their names and* email addresses to a company
27

1 system it used to match them with *their LinkedIn profiles*.

2 47. As *The New York Times* noted, "neither Zoom's privacy policy nor
3 its terms of service specifically disclosed that Zoom could covertly display
4 meeting participants' LinkedIn data to other users or that it might communicate
5 the names and email addresses of participants in private Zoom meetings to
6 LinkedIn." *Id.* In fact, "user instructions on Zoom suggested just the opposite:
7 that meeting attendees may control who sees their real names." *Id.*
8 Accordingly, "*privacy experts criticized Zoom for making the data-*
9 *mining tools available during meetings without alerting participants as*
10 *they were being subjected to them.*" *Id.*

11 48. Although Zoom claims that, after the revelations made in the Times
12 LinkedIn Report, it discontinued the practice of mining and revealing users'
13 LinkedIn information without authorization, Zoom has done nothing to rectify its
14 past violations of users' privacy and unlawful practices of unauthorized data
15 mining, collection, and disclosure.

16 **B. Zoom Failed to Implement Adequate Security Protocols**
17 **Jeopardizing Users' Account Security**

18 49. Zoom's inadequate security practices were exposed again on April
19 15, 2020, when an information security and technology news publication,
20 *BleepingComputer*, reported that hackers were selling half a million Zoom
21 account in the dark web.¹²

22
23
24
25 ¹² Sergiu Gatlan, Exploit for Zoom Windows Zero-Day Being Sold for \$500,000.00,
26 BLEEPINGCOMPUTER, Apr. 15, 2020, available at
27 [https://www.bleepingcomputer.com/news/security/exploit-for-zoom-windows-zero-day-being-sold-for 500-000/](https://www.bleepingcomputer.com/news/security/exploit-for-zoom-windows-zero-day-being-sold-for-500-000/) (last visited May 11, 2020).

1 An exploit for a zero-day remote code execution
2 vulnerability affecting the Zoom Windows client is currently
3 being sold for \$500,000, together with one designed to abuse a
4 bug in the video conferencing platform's macOS client.

5 * * *

6 As BleepingComputer reported on Monday, more than
7 500,000 Zoom accounts are being sold on hacker forums and on
8 the dark web for less than a penny each, and, in some cases, also
9 given away for free to be used in zoombombing pranks and
10 various other malicious activities.

11
12 50. The information relating to these half a million Zoom accounts
13 was published and exchanged online without Zoom users' consent or
14 knowledge. Zoom is responsible for violating users' privacy due to its failure
15 to implement adequate security protocols and review procedures that could
16 have and should have prevented the hacking of these accounts.

17 51. As a result of Zoom's failures, Plaintiff and other Class members
18 are subjected to increased risks of imminent harm to their privacy rights.

19
20 **C. Zoom Failed to Maintain Adequate Measures to Protect Data**
21 **Privacy and Ensure Videoconference Security**

22 52. On Zoom's websites and in its marketing materials, Zoom has
23 repeatedly touted the security of its videoconferences in that they are protected
24 by passwords and end-to-end encryption. In reality, however, Zoom's
25 videoconferences are vulnerable to hacking as evident in the increased
26 frequency of Zoombombing. Worse, as Zoom admitted in its recent
27

disclosures, **Zoom lacks the capacity to implement end-to-end encryption.**

53. As noted in the Intercept Report at fn.9, Zoom "claims to implement end-to-end encryption, widely understood as the most private form of internet communication, protecting conversations from all outside parties." But this is false. In fact, "Zoom is using its own definition of the term, **one that lets Zoom itself access unencrypted video and audio from meetings.**"

54. When confronted by the Intercept regarding this false representation, Zoom all but admitted that it lacks the technology to protect videoconferences with end-to-end encryption:

But when reached for comment about whether video meetings are actually end-to-end encrypted, a Zoom spokesperson wrote, "Currently, it is not possible to enable E2E encryption for Zoom video meetings. Zoom video meetings use a combination of TCP and UDP. TCP connections are made using TLS and UDP connections are encrypted with AES using a key negotiated over a TLS connection."

The encryption that Zoom uses to protect meetings is TLS, the same technology that web servers use to secure HTTPS websites. This means that the connection between the Zoom app running on a user's computer or phone and Zoom's server is encrypted in the same way the connection between your web browser and this article (on <https://theintercept.com>) is encrypted. **This is known as transport encryption, which is different from end-to-end encryption because the Zoom service itself can**

1 access the unencrypted video and audio content of Zoom
2 meetings. So when you have a Zoom meeting, the video and audio
3 content will stay private from anyone spying on your Wi-Fi, but it
4 won't stay private from the company. (In a statement, Zoom said
5 it does not directly access, mine, or sell user data; more below.)...

6
7 "When we use the phrase 'End to End' in our other
8 literature, it is in reference to the connection being encrypted
9 from Zoom end point to Zoom end point," the Zoom
10 spokesperson wrote, apparently referring to Zoom servers as
11 "end points" even though they sit between Zoom clients. "The
12 content is not decrypted as it transfers across the Zoom cloud"
13 through the networking between these machines. *Id.*

14 55. According to one cryptographer, Professor Matthew D. Green
15 of Johns Hopkins University's Department of Computer Science, Zoom is
16 twisting the common meaning of "end-to-end" in a **"dishonest way"**:

17 "They're a little bit fuzzy about what's end-to-end
18 encrypted," Green said of Zoom. "I think they're doing this in a
19 slightly dishonest way. It would be nice if they just came
20 clean." *Id.*

21 56. Caught red-handed, Zoom apologized on April 1, 2020 "in a
22 blog post for the 'discrepancy between the commonly accepted definition
23 of end-to-end encryption and how [Zoom was] using it." *See* fn. 7, Post
24 Report.

1 57. Zoom's dishonesty is particularly glaring in light of the fact
2 that several of Zoom's competitors, including Apple FaceTime and Signal,
3 offer real end-to-end encryption in their videoconferences:
4

5 "If it's all end-to-end encrypted, you need to add
6 some extra mechanisms to make sure you can do that kind of
7 'who's talking' switch, and you can do it in a way that doesn't
8 leak a lot of information. You have to push that logic out to the
9 endpoints," he told The Intercept. This isn't impossible,
10 though, Green said, as demonstrated by Apple's FaceTime,
11 which allows group video conferencing that's end-to-end
12 encrypted. **"It's doable. It's just not easy."** See fn. 9, the
13 Intercept Report.
14

15 58. Thus, it is not that Zoom could not have fulfilled its promise of
16 end-to-end encryption. It is that Zoom made a conscious decision to make the
17 false promise knowing that it lacked the technology to keep the promise.
18

19 59. Moreover, Zoom has done nothing, aside from issuing empty
20 words in a blog- posted "apology," to improve security in its videoconferences
21 and to rectify past security breaches.
22

23 60. Likewise, as discussed above, Zoom's marketing materials
24 provide users with a false sense of security regarding its videoconferences.
25

26 61. But Zoom's videoconferences are anything but secure. In recent
27 weeks, Zoombombing has become a daily element of Zoom's
videoconferences:

1 [Zoom] has faced added pressure from the rise of
2 "zoombombing" raids, in which anonymous trolls barge into
3 unlocked Zoom meetings, shouting profane insults and racist slurs.
4 Videos of the raids, some of which have been removed by
5 YouTube for violating hate-speech policies, show giggling trolls
6 posting pornography into online grade-school lessons, pulling
7 their pants down in front of company conference calls, and
8 dancing with bottles of bourbon in what appeared to be an online
9 Alcoholics Anonymous meeting.

10 *See* fn. 7, Post Report.

11 62. By failing to properly maintain security in its videoconferences,
12 Zoom has enabled hackers and pranksters to perpetrate online abuse on a
13 massive scale:

14 An analysis by The New York Times found 153 Instagram
15 accounts, dozens of Twitter accounts and private chats, and
16 several active message boards on Reddit and Chan where
17 thousands of people had gathered to organize Zoom harassment
18 campaigns, sharing meeting passwords and plans for sowing
19 chaos in public and private meetings (since this article's
20 publication, Reddit has shut down the message boards where
21 Zoom raids were discussed).

22 Zoom raiders often employ shocking imagery, racial
23 epithets and profanity to derail video conferences. Though a
24 meeting organizer can remove a participant at any time, the
25 perpetrators of these attacks can be hard to identify; there may be
26

1 several in a single call, and they can appear to jump from one
2 alias to another.

3 *See* fn. 6, *New York Times* Zoombombing Report.

4 63. The frequency and reach of the incidents on Zoom prompted the
5 F.B.I. to issue a warning on [March 31, 2020], singling out the [Zoom] app and
6 stating that it had "received multiple: reports of conferences being disrupted
7 by pornographic or hate images and threatening language' nationwide." *Id.*

8 64. In addition to the F.B.I., other state and federal authorities also
9 intervened. The attorneys generals of 27 states, including New York, have
10 raised questions about privacy issues and demanded that Zoom cooperate with
11 them in multiple investigations. *See* fn. 8, the WSJ Report. Senator Richard
12 Blumenthal of Connecticut wrote a letter to Zoom on March 31, 2020
13 demanding answers about Zoom's "'troubling history of software design
14 practices and security lapses.'" *Id.* Senator Blumenthal expressed grave
15 concerns over Zoom's privacy violations and security breaches:

16 **The millions of Americans** now unexpectedly attending
17 school, celebrating birthdays, seeking medical help, and sharing
18 evening drinks with friends over Zoom during the coronavirus
19 pandemic, ... **should not have to add privacy and cyber**
20 **security fears to their ever-growing list of worries.**

21
22 *Id.* (internal quotation marks omitted).

23 65. In its public disclosures, Zoom admits that its security is
24 inadequate. Zoom's founder and Chief Executive Officer, Eric Yuan, told The
25 Wall Street Journal: "I really messed up" on Zoom's security. *See* fn. 8, the
26 WSJ Report. But Zoom has done little to improve security. While Mr. Yuan
27

1 promised to develop "an option for end-to-end encryption to safeguard
2 conversations, ... [the] feature won't be ready for a few months." *Id.*

3 66. While Zoom continues to make empty, false promises, American
4 consumers are left to deal with the privacy violations and security breaches
5 inflicted by Zoom and, in Senator Blumenthal's words, "add[ing] privacy and
6 cybersecurity fears to their ever-growing list of worries." *Id.*

7 67. On behalf of these American consumers, Plaintiff brings this
8 action for damages and injunctive relief to rectify Zoom's misconduct.

9 **III. Plaintiff Experience with Zoom and Zoombombing**

10 **A. Dr. Rios Registered his Account with Zoom in**
11 **Reliance on Its False Representations of Data Protection and**
12 **Conference Security**

13 68. Dr. Rios has been conducting seminars, workshops, trainings, and
14 motivational programs for at-risk students and teachers for over a decade.

15 69. Following California's March 4, 2020 declaration of a state of
16 emergency as a result of the COVID-19 pandemic, Dr. Rios began searching
17 for alternative meeting venues to conduct his regular seminars with educators
18 and students. Based on Zoom's advertisements of a user-friendly and secure
19 platform, Zoom videoconferencing stood out as a prime candidate for
20 conducting online classes.
21

22 70. On April 13, 2020, Dr. Rios, serving as his administrator,
23 registered an account with Zoom, using his personal email address. On March
24 23, 2020, following the March 19, 2020 issuance of the statewide Executive
25 Order N-33-20 (directing all California residents to stay at home), Dr. Rios
26 upgraded his Zoom account to "premium" status by paying a monthly fee of
27

1 \$14.99. He also upgraded his Zoom account to host up to 500 participants for
2 \$112.00 per month. Dr. Rios downloaded Zoom's software onto an Apple
3 desktop computer.

4 71. At the time when Dr. Rios registered his account with Zoom, Dr.
5 Rios was not aware, and did not understand, that Zoom would share Dr. Rios'
6 personal information with third parties, including Facebook. Nor was Dr. Rios
7 aware that Zoom would allow third parties, like Facebook, to access his
8 personal information and combine it with content and information from other
9 sources to create a unique identifier or profile of Dr. Rios for purposes of
10 advertisement.

11 72. In fact, Dr. Rios registered with Zoom as a user and used Zoom's
12 services in reliance on Zoom's promises that (a) Zoom does not sell users' data;
13 (b) Zoom takes privacy seriously and adequately protects users' personal
14 information; and (c) Zoom's videoconferences are secured with end-to-end
15 encryption and are protected by passwords and other security measures.
16

17 **B. Dr. Rios and His Participants Became Victims of**
18 **Zoombombing**

19 73. Dr. Rios prepared for a Zoom videoconference to educate
20 teachers on how to connect with at-risk students who were not logging in to
21 remote learning sessions. This was a free community service he was providing
22 teachers who were interested. He set up the Zoom videoconference, following
23 Zoom's instructions. Based on Zoom's representations, he understood that the
24 videoconference would be protected and secure, and that, as the organizer, he
25 would have the ability to control the webinar, including being safe from any
26 uninvited or malicious participants.
27

1 74. For the April 30, 2020 webinar (starting at 3:00 p.m. Pacific
2 Time), Dr. Rios setup a Zoom videoconference, following Zoom's instructions.

3 75. The April 30, 2020 webinar was held on Zoom with over four
4 hundred (400) participants, including Dr. Rios as the organizer. The class was
5 uneventful until approximately 15 minutes into the class, when an intruder with
6 the name "Christine's iPad" hacked into the videoconference.

7 76. Immediately following the break-in, pornographic video footages
8 began to run on all participants' computers in a full-screen mode and with loud
9 audio. Dr. Rios and the other participants were forced to view footage of an
10 adult performing a sexual act on an infant. Dr. Rios was supervising break-out
11 sessions during the attack and neither him or other participants were unable to
12 minimize or close the video screen. Nor were they able to use any of the Zoom
13 functions to refuse viewing the pornographic video or eject the intruder
14 (Christine's iPad) from the Zoom meeting. After attempting to avoid the
15 pornographic video and eject the intruder to no avail - the intruder returned
16 immediately.
17

18 77. Pornographic video footages reappeared on every participant's
19 computer -again on full screen mode with loud audio. The footages again
20 involved an adult engaging in sexual acts and performing sexual acts on a
21 crying infant.
22

23 78. After many attempts, Dr. Rios figured out how to lock the meeting
24 and eliminate the intruder.

25 79. The depravity of the video footages was beyond description. Dr.
26 Rios and the other participants were traumatized and deeply disturbed. In fact,
27

1 two (2) of the participants have filed worker's compensation claims based upon
2 their having participated.

3 80. Dr. Rios had no choice but to try to talk participants through what
4 had just happened and offer his support to process the very traumatic situation.
5 He also paid for a licensed clinical social worker to host follow up sessions
6 with participants in case they wanted to process this traumatic event. He
7 reached out to Zoom twice about the incident. As of June 1, 2020, Zoom had
8 not responded.

9 **C. Zoom Rejected Dr. Rios's Repeated Pleas to Improve Security**

10 81. Immediately following the traumatizing incident, Dr. Rios sought
11 help from Zoom by contacting Zoom online and by telephone. Dr. Rios sent
12 an online request to Zoom, reporting the incident and demanding action to
13 remedy the situation and prevent to further Zoombombing.

14 82. In his own investigation and through emails and other
15 communications with attendees, Dr. Rios believes that the pornographic
16 images that appeared at his webinar were the same as those that are the subject
17 of the case *Saint Paulus Lutheran Church and Helen N. Cundle, et al. v. Zoom*
18 *Video Communications, Inc.*, USDC Case #5:20-cv-03252 – LK.

19 83. In an email response to Saint Paulus Lutheran Church dated May
20 6, 2020, Zoom's Trust & Safety department stated that it had identified the
21 intruder and blocked the intruder "from joining future meetings using the same
22 Zoom software." But Zoom refused to take any further action to remedy the
23 situation or to improve the security of its videoconferences. Shockingly, Zoom
24 admitted that the intruder was "a known serial offender who disrupts open
25
26
27

1 meetings by showing the same video," and had "been reported multiple times
2 to the authorities":

3 We identified in your meeting a **known serial offender**
4 **who disrupts open meetings by showing the same video,**
5 **and which has been reported multiple times to the**
6 **authorities.** This intruder has the following identifying
7 information:

8 Christine (iPad)

9 The report ID for Christine (iPad) is 71731955. You can use this
10 number when you submit your report to link both reports.
11

12 It is baffling, to say the least, how Zoom failed to protect Dr. Rios' seminar
13 from a "serial offender" who has been "reported multiple times to the
14 authorities" and who had just recently struck at a church gathering.

15 84. Dr. Rios, reported the incidents to the F.B.I. twice as they have
16 now created a special form for on-line reporting these zoombombing
17 pornographic incidents.

18 **FRAUDULENT CONCEALMENT AND TOLLING**

19 85. The applicable statutes of limitations are tolled because Zoom
20 knowingly and actively concealed the facts alleged above. Until the revelations
21 made in March 2020, Plaintiff and the Class members did not know and could
22 not have known of the information essential to the pursuit of these claims
23 through no fault of their own and not due to any lack of diligence on their part.

24 **CLASS ACTION ALLEGATIONS**

1 86. Plaintiff brings this action as a class action under Rule 23 of the
2 Federal Rules of Civil Procedure, on behalf of a proposed class (the "Class"),
3 defined as:

4 All persons in the United States who used Zoom during the applicable
5 limitations period.

6 87. Excluded from the Class are any entities, including Zoom, in
7 which Zoom or its subsidiaries or affiliates have a controlling interest,
8 Zoom's officers, agents and employees, the judicial officer to whom this
9 action is assigned and any member of the Court's staff and immediate families,
10 as well as claims for personal injury, wrongful death, and emotional distress.

11 88. **Numerosity Under Rule 23(a)(1).** The members of the Class are
12 so numerous that joinder of all members would be impracticable. Based on
13 information and belief, Plaintiff allege that the Class includes millions of
14 members.

15 89. **Commonality and Predominance Under Rule**
16 **23(a)(2) and 23(b)(3).** This action involves common questions of law
17 or fact, which predominate over any questions affecting individual Class
18 members, including:

19 (a) whether Zoom shared the personal information of Plaintiff
20 and other Class members with third parties without their authorization
21 or consent;

22 (b) whether Zoom violated Plaintiff' and Class members'
23 privacy rights;

24 (c) whether Zoom intruded upon Plaintiff' and the Class
25 members' seclusion;
26

1 (d) whether Zoom acted negligently;

2 (e) whether Plaintiff and other Class members formed implied
3 contracts with Zoom;

4 (f) whether Zoom breached implied contracts with Plaintiff
5 and the Class members and breached the implied covenant of good faith
6 and fair dealing;

7 (g) whether Zoom violated the CCPA;

8 (h) whether Zoom violated the CLRA;

9 (i) whether Zoom violated the UCL;

10 (j) whether Plaintiff and the Class members were harmed as a
11 result of Zoom's conduct;

12 (k) whether Plaintiff and the Class members are entitled to
13 actual, statutory, or other forms of damages or any other monetary relief;
14 and

15 (l) whether Plaintiff and the Class members are entitled to
16 equitable relief.

17 90. Plaintiff's claims are typical of the members of the Class as all
18 members of the Class are similarly affected by Zoom's actionable conduct.
19 Zoom's conduct that gave rise to Plaintiff's claims is the same for all members
20 of the Class.
21

22 91. Zoom engaged in a common course of conduct giving rise to the
23 legal rights sought to be enforced by Plaintiff and on behalf of the other Class
24 members. Similar or identical statutory and common-law violations, business
25 practices, and injuries are involved. Individual questions, if any, pale by
26
27

1 comparison, in both quantity and quality, to the numerous questions that
2 dominate this action.

3 92. Typicality Under Rule 23(a)(3). Plaintiff claims are typical of the
4 claims of the other Class members because, among other things, (a) Plaintiff
5 and the other Class members provided personal information to Zoom; and (b)
6 in its uniform misconduct alleged above, Zoom shared the personal
7 information of Plaintiff and other Class members without their authorization
8 or consent. Plaintiff and other Class members are advancing the same claims
9 and based on the same legal theories. There are no defenses that are unique to
10 Plaintiff.

11 93. Adequacy of Representation Under Rule 23(a)(4). Plaintiff is an
12 adequate representative of the Class because (a) his interests do not conflict
13 with the interests of the other Class members it seeks to represent; (b) they
14 have retained counsel competent and experienced in complex class action
15 litigation, (c) they will prosecute this action vigorously; and (d) he has no
16 interests that are contrary to or in conflict with the interests of other Class
17 members.

18 94. **Superiority Under Rule 23(b)(3).** A class action is superior to
19 other available methods for the fair and efficient adjudication of this
20 controversy because joinder of all the members of the Class is impracticable.

21 95. Furthermore, the adjudication of this controversy through a class
22 action will avoid the possibility of inconsistent and potentially conflicting
23 adjudication of the asserted claims. There should be no difficulty in managing
24 this action as a class action.
25
26
27

96. Class certification is also appropriate under Rule 23(b)(2) because Zoom has acted or has refused to act on grounds generally applicable to the Class, so that corresponding declaratory relief is appropriate to the Classes as a whole.

97. California law applies to the claims asserted in this complaint because:

- Zoom is headquartered in California;
- All of Zoom's key decisions and a substantial part of its operations emanate from California;
- A substantial number of the Class members reside in California;
- California has a strong interest in preventing corporations headquartered

in the state from engaging in unfair, unlawful, and deceptive business practices; and

- California has a strong interest in providing redress for its citizens for Zoom's illegal conduct.

CAUSES OF ACTION

Count 1

Negligence

98. Plaintiff repeats and incorporates by reference each and every allegation set forth above, as though fully set forth herein.

99. Zoom owed a duty to Plaintiff 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

1 security in Zoom's videoconferences. To fulfill this duty, Zoom is obligated to
2 implement and maintain adequate security measures to protect its users'
3 personal information and to avoid disclosure of its users' personal information
4 to any third parties without their knowledge and consent.

5 100. Plaintiff and the Class members used Zoom's services in reliance
6 on its exercise of due care and fulfillment of its duties.

7 101. Zoom, however, breached its duties by, among other things:

- 8 • disclosing Plaintiff's and other Class members' personal
9 information to unauthorized third parties, including Facebook;
- 10 • allowing third parties to access the personal information of
11 Plaintiff and other Class members;
- 12 • failing to implement and maintain adequate security
13 measures to safeguard users' personal information;
- 14 • failing to timely notify Plaintiff and other Class members
15 of the unlawful disclosure of their personal information; and
- 16 • failing to maintain adequate security and proper encryption
17 in Zoom's videoconferences.

18 102. Zoom's misconduct is inconsistent with industry regulations and
19 standards.
20

21 103. Plaintiff and other Class members did not contribute to Zoom's
22 misconduct.

23 104. The harm inflicted upon Plaintiff and other Class members is
24 reasonably foreseeable to Zoom.
25
26
27

105. As a direct and proximate result of Zoom's misconduct, Plaintiff and other Class members have suffered damages relating to, among other things, loss of income, privacy and emotional distress.

Count II

Breach of Implied Contract

106. Plaintiff repeats and incorporates by reference each and every allegation set forth above, as though fully set forth herein.

107. To generate revenues, attract advertisers, and increase market share, Zoom offered Plaintiff and other Class members to use its services by creating Zoom accounts, which require the provision of confidential, sensitive personal information.

108. Accepting Zoom's offer, Plaintiff and other Class members obtained user accounts from Zoom and provided Zoom with confidential, sensitive personal information.

109. By becoming users of Zoom's services, Plaintiff and other Class members entered into implied contracts with Zoom, under which Zoom, for its own benefit, obtained from Plaintiff and other Class members their confidential, sensitive personal information, as well as money. In exchange, Zoom agreed, at least implicitly, to (a) safeguard such information against unauthorized disclosure, access, or use; (b) timely notify Plaintiff and other Class members of any unauthorized disclosure of, access to, or use of such information; and (c) maintain adequate security and proper encryption in Zoom's videoconferences.

110. Without such an implicit agreement by Zoom, Plaintiff and other Class members would not have entrusted their personal information to Zoom

1 or paid for its services. Instead, Plaintiff and other Class members would have
2 chosen an alternative videoconference platform that would refrain from
3 sharing their personal information with undisclosed and unauthorized third
4 parties and maintain adequate security and proper encryption in
5 videoconferences.

6 111. Plaintiff and other Class members fully performed their
7 obligations under the implied contract with Zoom.

8 112. Zoom, however, breached the implied contracts it made with
9 Plaintiff and other Class members by, among other things:

- 10 • disclosing Plaintiff's and other Class members' personal
11 information to unauthorized third parties, including
12 Facebook;
- 13 • allowing third parties to access the personal information of
14 Plaintiff and other Class members;
- 15 • failing to implement and maintain adequate security
16 measures to safeguard users' personal information;
- 17 • failing to timely notify Plaintiff and other Class members
18 of the unlawful disclosure of their personal information; and
19 • failing to maintain adequate security and proper encryption
20 in Zoom's videoconferences.

21
22 113. By breaching its implied contracts with Plaintiff and other Class
23 members, Zoom is not entitled to retain the benefits it received.

24 114. As a direct and proximate result of Zoom's breaches of the implied
25 contracts, Plaintiff and other Class members have suffered actual losses and
26 damages.
27

Count III

Breach of the Implied Covenant of Good Faith and Fair Dealing

115. Plaintiff repeats and incorporates by reference each and every allegation set forth above, as though fully set forth herein.

116. There is a covenant of good faith and fair dealing implied in every implied contract. This implied covenant requires each contracting party to refrain from doing anything to injure the right of the other to receive the benefits of the agreement. To fulfill its covenant, a party must give at least as much consideration to the interests of the other party as it gives to its own interests.

117. Under the implied covenant of good faith and fair dealing, Zoom is obligated to, at a minimum, (a) implement proper procedures to safeguard the personal information of Plaintiff and other Class members; (b) refrain from disclosing, without authorization or consent, the personal information of Plaintiff and other Class members to any third parties; (c) promptly and accurately notify Plaintiff and other Class members of any unauthorized disclosure of, access to, and use of their personal information; and (d) maintain adequate security and proper encryption in Zoom's videoconferences.

118. Zoom breached the implied covenant of good faith and fair dealing by, among other things:

- disclosing Plaintiff's and other Class members' personal information to unauthorized third parties, including Facebook;
- allowing third parties to access the personal information of Plaintiff and other Class members;
- failing to implement and maintain adequate security measures to

safeguard users' personal information;

- failing to timely notify Plaintiff and other Class members of the unlawful disclosure of their personal information; and
- failing to maintain adequate security and proper encryption in Zoom's videoconferences.

119. As a direct and proximate result of Zoom's breaches of the implied covenant of good faith and fair dealing, Plaintiff and other Class members have suffered actual losses and damages.

Count IV

Unjust Enrichment

120. Plaintiff repeats and incorporates by reference each and every allegation set forth above, as though fully set forth herein.

121. Zoom has benefited and profited from Plaintiff's and other Class members' use of its videoconferencing services by obtaining their personal information and money.

122. Zoom, however, failed to provide Plaintiff and other Class members the services they reasonably expected because Zoom:

- disclosed Plaintiff's and other Class members' personal information to unauthorized third parties, including Facebook;
- allowed third parties to access the personal information of Plaintiff and other Class members;
- failed to implement and maintain adequate security measures to safeguard users' personal information;
- failed to timely notify Plaintiff and other Class members of the unlawful disclosure of their personal information; and

124. Plaintiff seeks an order directing Zoom to disgorge these benefits and profits and pay restitution to Plaintiff and other Class members.

Violation of the California Consumer Privacy Act

126. The CCPA prohibits collection and use of consumers' personal information from collection and use by businesses without consumers' notice and consent.

128. Zoom also violated the CCPA by failing to provide notice to Plaintiff and other Class members of their right to opt out of the disclosure or use of their personal information to third parties. *See* CAL. CIV. CODE §1788.100(b), 1798.120(b). Zoom failed to give Plaintiff and the Class members the opportunity to opt out before sharing their personal information with unauthorized parties.

129. Plaintiff seeks damages on behalf of himself and the Class, as well as injunctive relief in the form of an order enjoining Zoom from continuing to violate the CCPA.

Count VI

Violation of California's Consumer Legal Remedies Act

130. Plaintiff repeats and incorporates by reference each and every allegation set forth above, as though fully set forth herein.

131. Plaintiff and each Class Member are "consumers" under the CLRA, see CAL. CIV. CODE §1761(d).

132. Zoom is a "person" as defined by the CLRA, see CAL. CIV. CODE § 1761(c).

133. Zoom's marketing and sale of the Zoom app is the sale of a "good" and "service" to consumers within the meaning of the CLRA, see CAL. CIV. CODE §§ 1761(a)-(b), 1770(a).

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

135. As detailed above in paragraphs 26 through 33, Zoom promised to protect data privacy and secure videoconferences. Zoom violated the CLRA by, among other things:

- disclosing Plaintiff's and other Class members' personal information to unauthorized third parties, including Facebook;
- allowing third parties to access the personal information of Plaintiff and other Class members;

- 1 • failing to implement and maintain adequate security measures to
- 2 safeguard users' personal information;
- 3 • failing to, in a timely manner, (a) investigate the unauthorized
- 4 disclosures described above, and (b) notify Plaintiff and other
- 5 Class members of the unauthorized disclosure of, access to, and
- 6 use of their personal information; and
- 7 • failing to maintain adequate security and proper encryption in
- 8 Zoom's videoconferences.

9 136. Zoom's conduct is deceptive and unfair and violates Subsection
10 1770(a) of the California Civil Code because:

- 11 • Zoom represented that its product had characteristics it did not
- 12 have in violation of Subsection (a)(5);
- 13 • Zoom represented its products were of a particular standard, grade,
- 14 or quality when they were of another in violation of Subsection
- 15 (a)(7);
- 16 • Zoom advertised its services with intent not to sell them as
- 17 advertised in violation of Subsection (a)(9); and
- 18 • Zoom knowingly and intentionally withheld material information
- 19 from Plaintiff and the Class members in violation of Subsection (a)(14).
- 20

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

138. 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' information to third parties and whether it can ensure security in videoconferences.

139. Plaintiff and the 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.

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

141. Plaintiff and the Class members reasonably expected that Zoom would (a) safeguard their personal information and refrain from disclosing it without their consent; and (b) ensure security in Zoom's videoconferences.

142. Due to Zoom's violations of the CLRA, Plaintiff and the 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.

143. Plaintiff and the Class members seek an injunction barring Zoom from disclosing their personal information without their consent and requiring Zoom to ensure Zoom's security in videoconferences.

Count VII

Violation of the Unfair Competition Law

144. Plaintiff repeats and incorporates by reference each and every allegation set forth above, as though fully set forth herein.

1 145. Zoom engaged in unfair, unlawful, and fraudulent business
2 practices within the meaning of the UCL, CAL. Bus. & PROF. CODE §§
3 17200, *et seq.*

4 146. Zoom collected and stored confidential, sensitive personal
5 information from Plaintiff and other Class members. Zoom falsely represented
6 to Plaintiff and other Class members that:

7 (a) "[w]e do not sell your data";

8 (b) Zoom maintains adequate security measures to safeguard and
9 keep confidential users' personal information;

10 (c) Zoom limits its use of users' personal information "to determine
11 the offers to make for [its] services, analyze trends on and run the
12 marketing site, and understand users' movements around the marketing
13 site"; and

14 (d) Zoom provides "[s]ecurity and encryption ... with complete end-
15 to-end 256-bit AES encryption[.]"

16 147. In reliance on Zoom's representations, Plaintiff and other Class
17 members obtained Zoom accounts and provided Zoom with confidential,
18 sensitive personal information.
19

20 148. Zoom's misrepresentations and omissions caused Plaintiff and
21 other Class members to become Zoom users and provide Zoom with their
22 confidential, sensitive personal information. Plaintiff and other Class members
23 would not have done so, but for Zoom's misrepresentations and omissions.

24 149. Zoom's misrepresentations and omissions are unfair,
25 unlawful, and fraudulent. Zoom's acts, as alleged above, are "unfair" because
26 they offend an established public policy and are immoral, unethical, and
27

1 unscrupulous or substantially injurious to consumers. Zoom's acts, as alleged
2 above, are "unlawful" because they violate the common law and several
3 California statutes, including the CCPA and CLRA. Zoom's acts, as alleged
4 above, are "fraudulent" because they are likely to deceive the general public.

5 150. In addition to making these misrepresentations and omissions,
6 Zoom also violated the UCL by (a) failing to timely notify Plaintiff and other
7 Class members of the unauthorized disclosure of, access to, and use of their
8 personal information; (b) preventing Plaintiff and other Class members from
9 taking the necessary measures to remedy the unauthorized disclosure of their
10 personal information; and (c) failing to maintain adequate security and proper
11 encryption in Zoom's videoconferences.

12 151. Zoom's business practices violate the UCL also because Zoom (a)
13 falsely represented that goods or services have characteristics they do not have,
14 namely, adequate security; (b) falsely represented that its goods or services are
15 of a particular standard when they are of another; (c) advertised its goods and
16 services with intent not to sell them as advertised; (d) represented that the
17 subject of a transaction was supplied in accordance with a previous
18 representation when it was not; and (e) made material omissions regarding its
19 safeguarding of users' personal information.
20

21 152. Plaintiff and other Class members suffered injury in fact and lost
22 money or property as the result of Zoom's violations of the UCL.

23 153. Plaintiff requests that Zoom be (a) enjoined from further
24 violations of the UCL; and (b) required to restore to Plaintiff and other Class
25 members any money it had acquired by unfair competition, including
26 restitution and restitutionary disgorgement.
27

Count VIII

Invasion of Privacy in

Violation of Common Law and the California Constitution

154. Plaintiff repeats and incorporates by reference each and every allegation set forth above, as though fully set forth herein.

155. Under the common law and Section 1 in Article I of the California Constitution, Plaintiff and the Class members have a reasonable expectation of privacy in their personal information, their electronic devices (including computers, tablets, and mobile phones), and their online behavior and history (including their use of Zoom's services).

156. The reasonableness of such expectations of privacy finds support in Zoom's unique position to monitor Plaintiff's and the Class members' behavior through its access to their electronic devices and videoconferences. The surreptitious, highly technical, and non-intuitive nature of Zoom's disclosure of their personal information further underscores the reasonableness of their expectations of privacy.

157. 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 a videoconferencing without observation, intrusion, or interference.

158. Zoom shared Plaintiff's and the Class members' personal information, without their authorization or consent, with third parties, including Facebook.

1 159. Zoom's acts and omissions caused the exposure and publicity of
2 private details about Plaintiff and other Class members - matters that are of no
3 concern to the public.

4 160. This intrusion is highly offensive to a reasonable person. Zoom's
5 conduct alleged above is particularly egregious because Zoom concealed its
6 conduct from Plaintiff and other Class members, and because Zoom
7 represented to Plaintiff and other Class members that it considered privacy to
8 be "an extremely important topic" and took their privacy "very seriously."

9 161. As a direct and proximate result of Zoom's conduct, Plaintiff and
10 Class members were harmed by the public disclosure of their private affairs.

11 162. Plaintiff and other Class members seek damages in an amount to
12 be determined at trial.

13 PRAYER FOR RELIEF

14 WHEREFORE, Plaintiff, on behalf of himself and on behalf of all
15 members of the Class, respectfully request that the Court enter judgment in
16 favor of them and against Zoom:

17 A. certifying this action as a class action under Federal Rule of Civil
18 Procedure 23, appointing Plaintiff as Class Representatives, and appointing his
19 counsel as Class Counsel;

20 B. declaring that Zoom's conduct alleged in this complaint is unfair,
21 unlawful, and fraudulent in violation of the CCPA, the CLRA, and the UCL,
22 and that Zoom is liable for negligence, breach of implied contract, breach of
23 the implied covenant of good faith and fair dealing, and unjust enrichment;

24 C. enjoining Zoom from engaging in the negligent, unfair, unlawful,
25 and fraudulent business practices alleged in this complaint;
26

1 D. awarding Plaintiff and other Class members actual, compensatory,
2 consequential, punitive, and treble damages to the extent permitted by law,
3 including statutory damages available under the CCPA, except as to Count VI
4 for violation of the CLRA;

5 E. ordering Zoom to disgorge all benefits and profits unjustly
6 retained through its misconduct alleged in this complaint;

7 F. awarding Plaintiff and other Class members pre-judgment and
8 post-judgment interest;

9 G. awarding Plaintiff and other Class members reasonable attorneys'
10 fees and costs, including expert witness fees; and

11 H. granting such other and further relief as the Court deems just and
12 proper.

13 **DEMAND FOR JURY TRIAL**

14 Plaintiff demands a trial by jury.

15
16 Dated: June 2, 2020

17 Respectfully submitted,

18
19 
20 LAW OFFICES OF JOHN L. FALLAT
21 John L. Fallat (SBN #114842)
22 Timothy J. Tomlin (SBN #142294)
23 Mark A. Vaughn (SBN #241228)
24 68 Mitchell Blvd., Suite 135
25 San Rafael, CA 94903-2046
26 Telephone: (415) 457-3773
27 Facsimile: (415) 457-2667