

1 BOTTINI & BOTTINI, INC.
Francis A. Bottini, Jr. (SBN 175783)
2 fbottini@bottinilaw.com
3 Albert Y. Chang (SBN 296065)
achang@bottinilaw.com
4 Yury A. Kolesnikov (SBN 271173)
ykolesnikov@bottinilaw.com
5 7817 Ivanhoe Avenue, Suite 102
La Jolla, California 92037
6 Telephone: (858) 914-2001
7 Facsimile: (858) 914-2002

COTCHETT, PITRE & MCCARTHY, LLP
8 Mark C. Molumphy (SBN 168009)
mmolumphy@cpmlegal.com
9 Tyson Redenbarger (SBN 294424)
tredenbarger@cpmlegal.com
10 Anya N. Thepot (SBN 318430)
athepot@cpmlegal.com
11 San Francisco Airport Office Center
12 840 Malcolm Road, Suite 200
Burlingame, California 94010
13 Telephone: (650) 697-6000
14 Facsimile: (650) 697-0577

Attorneys for Plaintiff and the Class

15
16 UNITED STATES DISTRICT COURT
17 NORTHERN DISTRICT OF CALIFORNIA
18 SAN JOSE DIVISION

19 LISA T. JOHNSTON, individually and on
20 behalf of herself and all others similarly
situated,

21 Plaintiff,

22 vs.

23 ZOOM VIDEO COMMUNICATIONS, INC.,

24 Defendant.

Case No. _____

Class Action

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 exploded because hundreds of millions of people — all under stay-at-home orders — resort
2 to videoconferencing to connect with others for work and social functions. In recent weeks,
3 Zoom has become the virtual classroom for millions of schoolchildren and workspace for
4 many businesses and government agencies. The number of meeting participants across
5 Zoom has jumped from 10 million in December 2019 to 200 million in March 2020.

6 5. As the usage of Zoom’s services skyrockets, so do its collection and use of users’
7 personal information. And the importance of security of Zoom’s videoconferences cannot be
8 overstated because Zoom provides services to many critical government agencies
9 responsible for combating the COVID-19 pandemic, including the Center for Disease Control
10 and Prevention (“CDC”) and the U.S. Department of Homeland Security (“DHS”).¹

11 6. While Zoom enjoyed its success due to the hike of revenues and its stock price
12 resulting from the explosion of demands for its services, Zoom’s unlawful collection and use
13 of users’ personal information and its lack of adequate security came to light in a series of
14 articles published in late March and early April 2020 in *Vice*,² *The New York Times*,³ the
15 *Washington Post*,⁴ *The Wall Street Journal*,⁵ and other news outlets.⁶

16
17 ¹ Zoom for Government, available at <https://zoom.us/government> (last visited Apr.
18 6, 2020) (featuring photos of law enforcement and military personnel at work and listing
19 under “Organizations that love 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).

20 ² Joseph Cox, *Zoom iOS App Sends Data to Facebook Even If You Don’t Have a*
21 *Facebook Account*, VICE, Mar. 26, 2020, available at [https://www.vice.com/en_](https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account)
us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-
facebook-account (last visited Apr. 6, 2020) (the “Vice Report”).

22 ³ Taylor Lorenz & Davey Alba, “Zoombombing” Becomes a Dangerous Organized
23 Effort, THE NEW YORK TIMES, Apr. 3, 2020 (the “Times Zoombombing Report”); Aaron
Krollik & Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People’s*
24 *LinkedIn Profiles*, THE NEW YORK TIMES, Apr. 2, 2020 (the “Times LinkedIn Report”).

25 ⁴ Drew Harwell, *Everybody Seems to Be Using Zoom. But Its Security Flaws Could*
26 *Leave Users at Risk*, THE WASHINGTON POST, Apr. 2, 2020 (the “Post Report”).

27 ⁵ Aaron Tilley & Robert McMillan, *Zoom CEO: “I Really Messed Up” on Video*
28 *Platform’s Security*, THE WALL STREET JOURNAL, Apr. 4, 2020 (the “WSJ Report”).

⁶ Micah Lee & Yael Grauer, *Zoom Meetings Aren’t End-to-End Encrypted, Despite*
Misleading Marketing, THE INTERCEPT, Mar. 31, 2020, available at [https://theintercept.](https://theintercept.com/2020/03/31/zoom-meeting-encryption/)
com/2020/03/31/zoom-meeting-encryption/ (last visited Apr. 6, 2020).

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

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

12 9. Zoom's privacy violations and security breaches quickly commanded the
13 attention of 27 state attorneys general and the Federal Bureau of Investigation ("F.B.I."). On
14 March 30, 2020, the New York Attorney General sent a letter to Zoom expressing concerns
15 over and inquiring about its data-privacy and security practices. And on March 31, 2020, the
16 F.B.I. issued a warning singling out Zoom based on "multiple reports of conferences being
17 disrupted by pornographic and/or hate images and threatening language." *See Post* Report.

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

21 11. By bringing this class action on behalf of herself and other Zoom users,
22 Plaintiff seeks (a) damages for Zoom's violations of their privacy rights and its unfair,
23 unlawful, and deceptive business practices; and (b) restitution and injunctive relief
24 prohibiting Zoom from continuing its unfair, unlawful, and deceptive business practices.

25 ///

26 ///

27 ///

28

PARTIES

I. Plaintiff Lisa T. Johnston

12. Plaintiff Lisa T. Johnston resides in California and Colorado.

13. Ms. Johnston has registered an account with Zoom using an Apple laptop computer. She has also downloaded and installed the iOS version of the Zoom app using her Apple iPhone. She uses and accesses Zoom regularly using her Apple laptop computer and iPhone.

14. Ms. Johnston was not aware, and did not understand, that Zoom would share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for purposes of advertisement.

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

II. Defendant Zoom Video Communications, Inc.

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

17. Zoom provides video-communication services. The demand for Zoom's services has exploded in the wake of the COVID-19 pandemic while hundreds of millions of Americans are under orders to stay at home. As a result of the explosion of user demand, Zoom's stock price skyrocketed in recent months. On April 3, 2020, Zoom's stock closed at above \$120 per share — nearly doubling its closing price at the beginning of 2020.

1 **JURISDICTION AND VENUE**

2 18. This Court has subject-matter jurisdiction under the Class Action Fairness Act
3 of 2005, 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs,
4 exceeds the sum or value of \$5,000,000, and members of the Class are citizens of different
5 states from Zoom.

6 19. This Court has personal jurisdiction over Zoom because it maintains
7 headquarters in San Jose — within the County of Santa Clara, over which this District
8 presides. Zoom regularly conducts business in this District.

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

12 **INTRADISTRICT ASSIGNMENT**

13 21. In compliance with Local Rule 3-2(b), Plaintiff requests that this action be
14 assigned to the San Jose Division of this District because a substantial part of the events or
15 conduct giving rise to the claims in this action occurred in the County of Santa Clara.

16 **FACTUAL ALLEGATIONS**

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

19 22. A fast-growing tech company founded in San Jose in 2011, Zoom provides a
20 “video-first communications platform that ... connect[s] people through frictionless video,
21 phone, chat, and content sharing and enable[s] face-to-face video experiences for [up to]
22 thousands of people in a single meeting across disparate devices and locations.”⁷ Zoom
23 generates revenue from the “sale of subscriptions to [its] platform.” Zoom Annual Report at
24 13. As Zoom itself acknowledges, “security and privacy” are among the key factors affecting
25 its growth and revenue. *See id.*

26 ⁷ Zoom’s 2020 Annual Report filed in Form 10-K on March 20, 2020 with the U.S.
27 Securities and Exchange Commission, at 4, *available at* [https://investors.zoom.us/static-
files/09a01665-5f33-4007-8e90-de02219886aa](https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa) (last visited Apr. 6, 2020) (“Zoom Annual
28 Report”).

1 23. Zoom regularly collects from its users a massive volume of personal
2 information, including names, usernames, physical addresses, email addresses, phone
3 numbers, employment information, credit/debit cards, and cookies and pixels (*e.g.*, through
4 the use of Google Analytics and Google Ads). When users visit Zoom’s websites, such as
5 zoom.us and zoom.com, Zoom uses “cookies and tracking technologies” to collect valuable
6 personal data from users:

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

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

22 * * *

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

27 Zoom Privacy Policy, available at <https://zoom.us/privacy> (last visited Apr. 6, 2020).⁸ Even
28 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.”

29 24. In fact, Zoom boasts its commitment to user privacy:

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

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

33 _____
34 ⁸ Unless otherwise noted, all emphases are added.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- **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.
- **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.

25. 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...”

26. 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.

27. 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

1 private form of internet communication.” An end-to-end encrypted videoconference means
2 that “the video and audio content [are] encrypted in such a way that only the participants in
3 the meeting have the ability to decrypt it.” See *Intercept* Report. In other words, only the
4 videoconference participants themselves — not Zoom or any other third parties — have
5 access to the contents of their videoconferences.

6 28. As detailed below, however, Zoom’s promise of end-to-end encryption is false.
7 In fact, in response to the *Intercept*’s revelation of its false promises regarding end-to-end
8 encryption, a Zoom spokesperson admitted in late March 2020 that “[c]urrently, it is not
9 possible to enable E2E encryption for Zoom video meetings” due to the design and operation
10 of Zoom’s platform.

11 29. In addition to end-to-end encryption, Zoom also boasts its capacity to “secure”
12 a meeting “with password” using its “[r]ole-based user security”:

13 Client Application

14 Role-based user security

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

- 17 • **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

18 * * *

19 Meeting Security

20 Role-based user security

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

- 23 • **Secure a meeting with E2E encryption**
- 24 ...
- 25 • **Expel a participant or all participants**
- End a meeting
- 26 • **Lock a meeting**
- 27 ...
- Mute/unmute a participant or all participants
- 28 ...
- Enable/disable a participant or all participants to record ...

27 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

1 regarding security of its videoconferences are false because “Zoombombing’ ... by uninvited
2 participants ha[s] become frequent.” *See Times Zoombombing Report.*

3 30. Yet, Zoom profits from these false promises of data protection and security.
4 Before the COVID-19 outbreak, Zoom induced — using these false promises — millions of
5 consumers, as well as business and government agencies, to register for its services. The
6 volume of Zoom’s business generated an annual revenue of \$622.7 million in the fiscal year
7 of 2020 (ending January 31, 2020). Zoom Annual Report at 38. In April 2019, Zoom issued
8 20 million shares of its common stock at \$36 per share in a successful initial public offering.

9 31. Since the outbreak of the COVID-19 pandemic, the demand for Zoom’s services
10 has skyrocketed:

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

15 *See Post Report.* According to the app data firm SensorTower, “first-time installs of the
16 videoconferencing company’s mobile app rose by 1,126 percent in March to more than 76
17 million, up from just 6.2 million in February.” *Times Zoombombing Report.*

18 32. Likewise, Zoom’s stock price skyrocketed — trading at one point at a high of
19 \$164.94 per share (on March 23, 2020). Today, Zoom amasses over \$30 billion in market
20 capitalization. Zoom’s exponential growth of market capitalization is predicated upon users’
21 trust in its promises of data privacy and security. But these promises are false.

22 **II. Zoom Broke Its Promises of Data Privacy and Security**

23 **A. Zoom Collected and Disclosed Users’ Personal Information 24 Without Authorization or Consent**

25 33. Zoom’s promises of data privacy and security are false. As revealed in the *Vice*
26 Report, the iOS version of Zoom’s mobile app sent users’ personal information to Facebook
27 for use in targeted advertising, ***without first notifying the users or obtaining their***
28 ***consent.*** Zoom provided users’ personal information to Facebook even for users who do

1 not have Facebook accounts. *See Vice Report.*

2 34. According to the *Vice Report*, upon downloading and opening the app, Zoom
3 would connect to Facebook’s Graph API (“application program interface”) — a primary way
4 to get data into and out of the Facebook platform.

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

15 36. According to one privacy-protection expert, Zoom’s practices of data collection
16 and data sharing are “shocking,” because “[t]here is nothing in [Zoom’s] privacy policy that
17 addresses that.” *See Vice Report.*

18 37. Aside from the lack of any notice, Zoom’s data-sharing activity was not visible
19 to users because they can only see the Zoom app interface. Thus, Zoom provides users **no**
20 **opportunity to consent to or opt out of** Zoom’s data-sharing with Facebook. Zoom’s
21 lack of disclosure and failure to provide an opportunity to opt out is particularly glaring in
22 light of Facebook’s own admonition to developers like Zoom to give notice:

23 Facebook told [*Vice*] it **requires developers to be transparent**
24 **with users about the data their apps send to Facebook.** Facebook’s
25 terms say “If you use our pixels or SDK [(software development kits)], you
26 further represent and warrant that you have provided **robust and**
27 **sufficiently prominent notice to users regarding the Customer**
28 **Data collection, sharing and usage,**” and specifically for apps, “**that**
third parties, including Facebook, may collect or receive
information from your app and other apps and use that
information to provide measurement services and targeted ads.”

1 See Vice Report.

2 38. Indeed, after being confronted with Vice’s findings, “**Zoom confirmed the**
3 **data collection** in a statement to [Vice]”:

4 We originally implemented the ‘Login with Facebook’ feature using the
5 Facebook SDK in order to provide our users with another convenient way to
6 access our platform. However, **we were recently made aware that the**
7 **Facebook SDK was collecting unnecessary device data** [as identified
8 by Vice.] ...

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

15 See Vice Report.

16 39. Despite admitting to the “oversight” and purporting to release a new version
17 of the Zoom app (as of March 27, 2020) as a remedy, the harm to Plaintiff and other Class
18 members, as well as the violations of their privacy, have occurred and continue to occur
19 because, even assuming no unauthorized disclosure of personal information is made
20 through the new version, the previous version of the app remains operational. Moreover,
21 Zoom failed to mandate the use of the new version of the app. Nor did Zoom do anything to
22 rectify its previous egregious violations of users’ privacy rights.

23 40. Upon information and belief, Zoom provides users’ personal information to
24 other third parties, in addition to Facebook, for unauthorized purposes, including use in
25 targeted advertising.

26 41. Plaintiff and other reasonable Zoom users did not know that when they signed
27 up to use Zoom’s services that Zoom would share their personal information with third
28 parties for the purpose and in the manner set forth above, and that their privacy rights would
be violated. Had Plaintiff and other users known about Zoom’s data-sharing practices, they
would not have signed up with Zoom and would not have used Zoom’s services.

42. Zoom’s unlawful disclosure of users’ personal information is not limited to

1 Facebook. According to the *Times* LinkedIn Report, Zoom used data-mining tools to collect
2 users' personal information without authorization, then used the personal information to
3 match the users' LinkedIn profiles:

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

8 But what many people may not know is that, until Thursday, **a data-**
9 **mining feature on Zoom allowed some participants to**
10 **surreptitiously have access to LinkedIn profile data about other**
11 **users — without Zoom asking for their permission during the**
12 **meeting or even notifying them that someone else was snooping**
13 **on them.**

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

18 An analysis by *The New York Times* found that when people signed in
19 to a meeting, **Zoom's software automatically sent their names and**
20 **email addresses to a company system it used to match them with**
21 **their LinkedIn profiles.**

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

29 44. Although Zoom claims that, after the revelations made in the *Times* LinkedIn
30 Report, it discontinued the practice of mining and revealing users' LinkedIn information
31 without authorization, Zoom has done nothing to rectify its past violations of users' privacy
32 and unlawful practices of unauthorized data mining, collection, and disclosure.

1 **B. Zoom Failed to Maintain Adequate Measures to Protect Data**
2 **Privacy and Ensure Videoconference Security**

3 45. On Zoom’s websites and in its marketing materials, Zoom has repeatedly
4 touted the security of its videoconferences — that they are protected by passwords and end-
5 to-end encryption. In reality, however, Zoom’s videoconferences are vulnerable to hacking
6 — as evident in the increased frequency of Zoombombing. Worse, as Zoom admitted in its
7 recent disclosures, ***Zoom lacks the capacity to implement end-to-end encryption.***

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

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

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

22 The encryption that Zoom uses to protect meetings is TLS, the same
23 technology that web servers use to secure HTTPS websites. This means that
24 the connection between the Zoom app running on a user’s computer or phone
25 and Zoom’s server is encrypted in the same way the connection between your
26 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 access the
unencrypted video and audio content of Zoom meetings. So when
you have a Zoom meeting, the video and audio content will stay private from
anyone spying on your Wi-Fi, but it won’t stay private from the company. (In
a statement, Zoom said it does not directly access, mine, or sell user data; more
below.)

27 ...
28 ***“When we use the phrase ‘End to End’ in our other literature,***
it is in reference to the connection being encrypted from Zoom end

1 **point to Zoom end point,”** the Zoom spokesperson wrote, **apparently**
2 **referring to Zoom servers as “end points” even though they sit**
3 **between Zoom clients.** “The content is not decrypted as it transfers across
the Zoom cloud” through the networking between these machines.

4 *See Intercept Report.*

5 48. According to one cryptographer, Professor Matthew D. Green of Johns
6 Hopkins University’s Department of Computer Science, Zoom is twisting the common
7 meaning of “end-to-end” in a **“dishonest way”**:

8 “They’re a little bit fuzzy about what’s end-to-end encrypted,” Green
9 said of Zoom. “I think they’re doing this in a slightly dishonest way. It would
be nice if they just came clean.”

10 *See id.*

11 49. Caught red-handed, Zoom apologized on April 1, 2020 “in a blog post for the
12 ‘discrepancy between the commonly accepted definition of end-to-end encryption and how
13 [Zoom was] using it.” *Post Report.*

14 50. Zoom’s dishonesty is particularly glaring in light of the fact that several of
15 Zoom’s competitors, including Apple FaceTime and Signal, offer real end-to-end encryption
16 in their videoconferences:

17 “If it’s all end-to-end encrypted, you need to add some extra
18 mechanisms to make sure you can do that kind of ‘who’s talking’ switch, and
19 you can do it in a way that doesn’t leak a lot of information. You have to push
20 that logic out to the endpoints,” he told *The Intercept*. This isn’t impossible,
though, Green said, as demonstrated by Apple’s FaceTime, which allows group
video conferencing that’s end-to-end encrypted. **“It’s doable. It’s just not
easy.”**

21 *See Intercept Report.*

22 51. Thus, it is not that Zoom could not have fulfilled its promise of end-to-end
23 encryption. It is that Zoom made a conscious decision to make the false promise — knowing
24 that it lacked the technology to keep the promise.

25 52. Moreover, Zoom has done nothing, aside from issuing empty words in a blog-
26 posted “apology,” to improve security in its videoconferences and to rectify past security
27 breaches.

1 53. Likewise, as discussed above, Zoom’s marketing materials provide users with
2 a false sense of security regarding its videoconferences.

3 54. But Zoom’s videoconferences are anything but secure. In recent weeks,
4 Zoombombing has become a daily element of Zoom’s videoconferences:

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

12 *See Post Report.*

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

15 An analysis by *The New York Times* found 153 Instagram accounts,
16 dozens of Twitter accounts and private chats, and several active message
17 boards on Reddit and 4Chan where thousands of people had gathered to
18 organize Zoom harassment campaigns, sharing meeting passwords and plans
19 for sowing chaos in public and private meetings. (Since this article’s
20 publication, Reddit has shut down the message boards where Zoom raids were
21 discussed.)

22 Zoom raiders often employ shocking imagery, racial epithets and
23 profanity to derail video conferences. Though a meeting organizer can remove
24 a participant at any time, the perpetrators of these attacks can be hard to
25 identify; there may be several in a single call, and they can appear to jump from
26 one alias to another.

27 *See Times Zoombombing Report.*

28 56. “The frequency and reach of the incidents on Zoom prompted the F.B.I. to
issue a warning on [March 31, 2020], singling out the [Zoom] app and stating that it had
‘received multiple reports of conferences being disrupted by pornographic or hate images
and threatening language’ nationwide.” *Id.*

57. In addition to the F.B.I., other state and federal authorities also intervened.
The attorneys generals of 27 states, including New York, have raised questions about privacy
issues and demanded that Zoom cooperate with them in multiple investigations. *See WSJ*

1 Report. Senator Richard Blumenthal of Connecticut wrote a letter to Zoom on March 31,
2 2020 demanding answers about Zoom’s “troubling history of software design practices and
3 security lapses.” *Id.* Senator Blumenthal expressed grave concerns over Zoom’s privacy
4 violations and security breaches:

5 ***The millions of Americans*** now unexpectedly attending school,
6 celebrating birthdays, seeking medical help, and sharing evening drinks with
7 friends over Zoom during the coronavirus pandemic, ... ***should not have to***
8 ***add privacy and cybersecurity fears to their ever-growing list of***
9 ***worries.***

10 *Id.* (internal quotation marks omitted).

11 58. In its public disclosures, Zoom admits that its security is inadequate. Zoom’s
12 founder and Chief Executive Officer, Eric Yuan, told *The Wall Street Journal*: “***I really***
13 ***messed up***” on Zoom’s security. *See id.* But Zoom has done little to improve security. While
14 Mr. Yuan promised to develop “an option for end-to-end encryption to safeguard
15 conversations, ... [the] feature won’t be ready for a few months.” *Id.*

16 59. While Zoom continues to make empty, false promises, American consumers
17 are left to deal with the privacy violations and security breaches inflicted by Zoom and, in
18 Senator Blumenthal’s words, “add[ing] privacy and cybersecurity fears to their ever-growing
19 list of worries.” *Id.*

20 60. On behalf of these American consumers, Plaintiff brings this action for
21 damages and injunctive relief to rectify Zoom’s misconduct.

22 **FRAUDULENT CONCEALMENT AND TOLLING**

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

28 ///

///

1 **CLASS ACTION ALLEGATIONS**

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

4 All persons who used the Zoom app for iOS during the applicable
5 limitations period.

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

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

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

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

19 (b) whether Zoom violated Plaintiff’s and Class members’ privacy rights;

20 (c) whether Zoom intruded upon Plaintiff’s and the Class members’
21 seclusion;

22 (d) whether Zoom acted negligently;

23 (e) whether Plaintiff and other Class members formed implied contracts
24 with Zoom;

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

27 (g) whether Zoom violated the CCPA;

28 (h) whether Zoom violated the CLRA;

1 (i) whether Zoom violated the UCL;

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

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

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

7 66. Plaintiff's claims are typical of the members of the Class as all members of the
8 Class are similarly affected by Zoom's actionable conduct. Zoom's conduct that gave rise to
9 Plaintiff's claims is the same for all members of the Class.

10 67. Zoom engaged in a common course of conduct giving rise to the legal rights
11 sought to be enforced by Plaintiff individually and on behalf of the other Class members.
12 Similar or identical statutory and common-law violations, business practices, and injuries
13 are involved. Individual questions, if any, pale by comparison, in both quantity and quality,
14 to the numerous questions that dominate this action.

15 68. **Typicality Under Rule 23(a)(3).** Plaintiff's claims are typical of the claims
16 of the other Class members because, among other things, (a) Plaintiff and the other Class
17 members provided personal information to Zoom; and (b) in its uniform misconduct alleged
18 above, Zoom shared the personal information of Plaintiff and other Class members without
19 their authorization or consent. Plaintiff and other Class members are advancing the same
20 claims and based on the same legal theories. There are no defenses that are unique to
21 Plaintiff.

22 69. **Adequacy of Representation Under Rule 23(a)(4).** Plaintiff is an
23 adequate representative of the Class because (a) her interests do not conflict with the
24 interests of the other Class members she seeks to represent; (b) she has retained counsel
25 competent and experienced in complex class action litigation, including data-privacy
26 litigation; (c) she will prosecute this action vigorously; and (d) she has no interests that are
27 contrary to or in conflict with the interests of other Class members.

1 is obligated to implement and maintain adequate security measures to protect its users'
2 personal information and to avoid disclosure of its users' personal information to any third
3 parties without their knowledge and consent.

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

6 76. Zoom, however, breached its duties by, among other things:
7 • disclosing Plaintiff's and other Class members' personal information to
8 unauthorized third parties, including Facebook;
9 • allowing third parties to access the personal information of Plaintiff and
10 other Class members;
11 • failing to implement and maintain adequate security measures to
12 safeguard users' personal information;
13 • failing to timely notify Plaintiff and other Class members of the unlawful
14 disclosure of their personal information; and
15 • failing to maintain adequate security and proper encryption in Zoom's
16 videoconferences.

17 77. Zoom's misconduct is inconsistent with industry regulations and standards.

18 78. Plaintiff and other Class members did not contribute to Zoom's misconduct.

19 79. The harm inflicted upon Plaintiff and other Class members is reasonably
20 foreseeable to Zoom.

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

24 **Count II**
25 **Breach of Implied Contract**

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

28 82. To generate revenues, attract advertisers, and increase market share, Zoom

1 offered Plaintiff and other Class members to use its services by creating Zoom accounts,
2 which require the provision of confidential, sensitive personal information.

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

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

12 85. Without such an implicit agreement by Zoom, Plaintiff and other Class
13 members would not have entrusted their personal information to Zoom or paid for its
14 services. Instead, Plaintiff and other Class members would have chosen an alternative
15 videoconference platform that would refrain from sharing their personal information with
16 undisclosed and unauthorized third parties and maintain adequate security and proper
17 encryption in videoconferences.

18 86. Plaintiff and other Class members fully performed their obligations under the
19 implied contract with Zoom.

20 87. Zoom, however, breached the implied contracts it made with Plaintiff and
21 other Class members by, among other things:

- 22 • disclosing Plaintiff's and other Class members' personal information to
23 unauthorized third parties, including Facebook;
- 24 • allowing third parties to access the personal information of Plaintiff and
25 other Class members;
- 26 • failing to implement and maintain adequate security measures to
27 safeguard users' personal information;

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

5 88. By breaching its implied contracts with Plaintiff and other Class members,
6 Zoom is not entitled to retain the benefits it received.

7 89. As a direct and proximate result of Zoom’s breaches of the implied contracts,
8 Plaintiff and other Class members have suffered actual losses and damages.

9 **Count III**
10 **Breach of the Implied Covenant of Good Faith and Fair Dealing**

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

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

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

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

- 27 • disclosing Plaintiff’s and other Class members’ personal information to
- 28 unauthorized third parties, including Facebook;

- 1 • allowing third parties to access the personal information of Plaintiff and
- 2 other Class members;
- 3 • failing to implement and maintain adequate security measures to
- 4 safeguard users' personal information;
- 5 • failing to timely notify Plaintiff and other Class members of the unlawful
- 6 disclosure of their personal information; and
- 7 • failing to maintain adequate security and proper encryption in Zoom's
- 8 videoconferences.

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

12 **Count IV**
13 **Unjust Enrichment**

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

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

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

- 20 • disclosed Plaintiff's and other Class members' personal information to
- 21 unauthorized third parties, including Facebook;
- 22 • allowed third parties to access the personal information of Plaintiff and
- 23 other Class members;
- 24 • failed to implement and maintain adequate security measures to safeguard
- 25 users' personal information;
- 26 • failed to timely notify Plaintiff and other Class members of the unlawful
- 27 disclosure of their personal information; and
- 28 • failed to maintain adequate security and proper encryption in Zoom's

1 videoconferences.

2 98. Zoom has therefore been unjustly enriched by its retention of the benefits and
3 profits at the expense of Plaintiff and other Class members. Equity and justice require that
4 Zoom disgorge the benefits and profits.

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

7 **Count V**
8 **Violation of the California Consumer Privacy Act**

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

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

13 102. Zoom violated the CCPA by using the personal information of Plaintiff and
14 other Class members without providing the required notice under the CCPA. *See* CAL. CIV.
15 CODE § 1798.100(b). Zoom did not notify Plaintiff and the Class members that it was
16 disclosing their personal information to unauthorized parties.

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

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

24 **Count VI**
25 **Violation of California's Consumer Legal Remedies Act**

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

28 106. Plaintiff and each Class Member are "consumers" under the CLRA, *see* CAL.

1 CIV. CODE § 1761(d).

2 107. Zoom is a “person” as defined by the CLRA, *see* CAL. CIV. CODE § 1761(c).

3 108. Zoom’s marketing and sale of the Zoom app is the sale of a “good” and “service”
4 to consumers within the meaning of the CLRA, *see* CAL. CIV. CODE §§ 1761(a)–(b), 1770(a).

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

7 110. As detailed above in paragraphs 22 through 29, Zoom promised to protect data
8 privacy and secure videoconferences. Zoom violated the CLRA by, among other things:

- 9
- 10 • disclosing Plaintiff’s and other Class members’ personal information to
unauthorized third parties, including Facebook;
 - 11 • allowing third parties to access the personal information of Plaintiff and
12 other Class members;
 - 13 • failing to implement and maintain adequate security measures to
14 safeguard users’ personal information;
 - 15 • failing to, in a timely manner, (a) investigate the unauthorized disclosures
16 described above, and (b) notify Plaintiff and other Class members of the
17 unauthorized disclosure of, access to, and use of their personal
18 information; and
 - 19 • failing to maintain adequate security and proper encryption in Zoom’s
20 videoconferences.

21 111. Zoom’s conduct is deceptive and unfair and violates Subsection 1770(a) of the
22 California Civil Code because:

- 23
- 24 • Zoom represented that its product had characteristics it did not have in
violation of Subsection (a)(5);
 - 25 • Zoom represented its products were of a particular standard, grade, or
26 quality when they were of another in violation of Subsection (a)(7);
 - 27 • Zoom advertised its services with intent not to sell them as advertised in
28

1 violation of Subsection (a)(9); and

- 2 • Zoom knowingly and intentionally withheld material information from
3 Plaintiff and the Class members in violation of Subsection (a)(14).

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

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

13 114. Plaintiff and the Class members could not reasonably have been expected to
14 learn or discover Zoom's disclosure of their personal information to unauthorized parties or
15 Zoom's lack of capacity to secure videoconferences.

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

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

21 117. Due to Zoom's violations of the CLRA, Plaintiff and the Class members
22 suffered damages and did not receive the benefit of their bargain with Zoom because they
23 paid for a value of services, either through personal information or a combination of their
24 personal information and money.

25 118. Plaintiff and the Class members seek an injunction barring Zoom from
26 disclosing their personal information without their consent and requiring Zoom to ensure
27 security in videoconferences.

1 **Count VII**
2 **Violation of the Unfair Competition Law**

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

5 120. Zoom engaged in unfair, unlawful, and fraudulent business practices within
6 the meaning of the UCL, CAL. BUS. & PROF. CODE §§ 17200, *et seq.*

7 121. Zoom collected and stored confidential, sensitive personal information from
8 Plaintiff and other Class members. Zoom falsely represented to Plaintiff and other Class
9 members that:

10 (a) “[w]e do not sell your data”;

11 (b) Zoom maintains adequate security measures to safeguard and keep
12 confidential users’ personal information;

13 (c) Zoom limits its use of users’ personal information “to determine the
14 offers to make for [its] services, analyze trends on and run the marketing site, and
15 understand users’ movements around the marketing site”; and

16 (d) Zoom provides “[s]ecurity and encryption ... with complete end-to-end
17 256-bit AES encryption[.]”

18 122. In reliance on Zoom’s representations, Plaintiff and other Class members
19 obtained Zoom accounts and provided Zoom with confidential, sensitive personal
20 information.

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

25 124. Zoom’s misrepresentations and omissions are unfair, unlawful, and
26 fraudulent. Zoom’s acts, as alleged above, are “unfair” because they offend an established
27 public policy and are immoral, unethical, and unscrupulous or substantially injurious to
28 consumers. Zoom’s acts, as alleged above, are “unlawful” because they violate the common

1 law and several California statutes, including the CCPA and CLRA. Zoom’s acts, as alleged
2 above, are “fraudulent” because they are likely to deceive the general public.

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

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

16 127. Plaintiff and other Class members suffered injury in fact and lost money or
17 property as the result of Zoom’s violations of the UCL.

18 128. Plaintiff requests that Zoom be (a) enjoined from further violations of the UCL;
19 and (b) required to restore to Plaintiff and other Class members any money it had acquired
20 by unfair competition, including restitution and restitutionary disgorgement.

21 **Count VIII**
22 **Invasion of Privacy in**
Violation of Common Law and the California Constitution

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

25 130. Under the common law and Section 1 in Article I of the California Constitution,
26 Plaintiff and the Class members have a reasonable expectation of privacy in their personal
27 information, their electronic devices (including computers, tablets, and mobile phones), and
28

1 their online behavior and history (including their use of Zoom’s services).

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

7 132. Plaintiff’s and Class members’ privacy interest is legally protected because they
8 have an interest in precluding the dissemination or misuse of sensitive information and an
9 interest in making intimate personal decisions and conducting activities like
10 videoconferencing without observation, intrusion, or interference.

11 133. Zoom shared Plaintiff’s and the Class members’ personal information, without
12 their authorization or consent, with third parties, including Facebook.

13 134. Zoom’s acts and omissions caused the exposure and publicity of private details
14 about Plaintiff and other Class members — matters that are of no concern to the public.

15 135. This intrusion is highly offensive to a reasonable person. Zoom’s conduct
16 alleged above is particularly egregious because Zoom concealed its conduct from Plaintiff
17 and other Class members, and because Zoom represented to Plaintiff and other Class
18 members that it considered privacy to be “an extremely important topic” and took their
19 privacy “very seriously.”

20 136. As a direct and proximate result of Zoom’s conduct, Plaintiff and Class
21 members were harmed by the public disclosure of their private affairs.

22 137. Plaintiff and other Class members seek damages in an amount to be
23 determined at trial.

24 ///

25 ///

26 ///

27 ///

28

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all members of the Class, respectfully requests that the Court enter judgment in favor of them and against Zoom:

A. certifying this action as a class action under Federal Rule of Civil Procedure 23, appointing Plaintiff as Class Representative, and appointing her counsel as Class Counsel;

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

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

D. awarding Plaintiff and other Class members actual, compensatory, consequential, punitive, and treble damages to the extent permitted by law, including statutory damages available under the CCPA;

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

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

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

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

///

///

///

///

///

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JURY DEMAND

Plaintiff demands a trial by jury.

Dated: April 8, 2020

Respectfully submitted,
BOTTINI & BOTTINI, INC.
Francis A. Bottini, Jr. (SBN 175783)
Albert Y. Chang (SBN 296065)
Yury A. Kolesnikov (SBN 271173)

s/ Francis A. Bottini, Jr.

Francis A. Bottini, Jr.
7817 Ivanhoe Avenue, Suite 102
La Jolla, California 92037
Telephone: (858) 914-2001
Facsimile: (858) 914-2002
fbottini@bottinilaw.com
achang@bottinilaw.com
ykolesnikov@bottinilaw.com

COTCHETT, PITRE & MCCARTHY, LLP
Mark C. Molumphy (SBN 168009)
Tyson Redenbarger (SBN 294424)
Anya N. Thepot (SBN 318430)
San Francisco Airport Office Center
840 Malcolm Road, Suite 200
Burlingame, California 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577
mmolumphy@cpmlegal.com
tredenbarger@cpmlegal.com
athepot@cpmlegal.com

Attorneys for Plaintiff and the Class