Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore Maya (SBN 223242)
tmaya@ahdootwolfson.com
Bradley K. King (SBN 274399)
bking@ahdootwolfson.com
Christopher E. Stiner (SBN 276033)
cstiner@ahdootwolfson.com
Rachel Johnson (SBN 331351)
rjohnson@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585

Mark C. Molumphy (SBN 168009)
mmolumphy@cpmlegal.com
Joseph W. Cotchett (SBN 36324)
jcotchett@cpmlegal.com
Tyson Redenbarger (SBN 294424)
tredenbarger@cpmlegal.com
Noorjahan Rahman (SBN 330572)
nrahman@cpmlegal.com
Julia Peng (SBN 318396)
jpeng@cpmlegal.com
COTCHETT, PITRE & McCARTHY LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: 650.697.6000
Facsimile: 650.697.0577

Interim Co-Lead Class Counsel
Additional Counsel on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: ZOOM VIDEO COMMUNICATIONS, INC. PRIVACY LITIGATION

This Document Relates To: All Actions

Case No. 5:20-CV-02155-LHK

SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

JUDGE: Hon. Lucy H. Koh
CTRM: 8—4th Floor

Plaintiffs Caitlin Brice, Heddi N. Cundle, Angela Doyle, Isabelle Gmerek, Kristen Hartmann, Peter Hirshberg, M.F. and his parent Therese Jimenez, Lisa T. Johnston, Oak Life Church, Saint Paulus Lutheran Church and Stacey Simins ("Plaintiffs") allege the following against Defendant Zoom Video Communications, Inc. ("Defendant" or "Zoom"), acting individually and on behalf of all others similarly situated:

BRIEF SUMMARY OF THE CASE

1. Plaintiffs bring this case to stop Zoom, currently the most popular videoconferencing platform, from invading consumers' privacy and from promoting its product under false assurances of privacy. Further, Plaintiffs seek compensation for themselves and all others similarly situated for past privacy violations.

2. Zoom is a supplier of video conferencing services founded in 2011 by Eric Yuan, a former corporate vice president for Cisco Webex. In January 2017, Zoom raised $100 million in Series D funding from Sequoia Capital at a $1 billion valuation, and achieved "unicorn" status—a privately held startup that has reached a $1 billion valuation. On April 18, 2019, the company became a public company via an initial public offering. On its first day of trading Zoom's share price increased over 72%, and by the end of the day Zoom was valued at $16 billion. By June 2020, Zoom was valued at over $67 billion.

3. Zoom achieved this remarkable growth by, as explained by Mr. Yuan, taking "the work out of meetings." "We've dedicated ourselves to the features and enhancements that pull all the friction out of video communications. We've made it easier to buy and deploy Zoom Rooms, we've made it simpler to schedule meetings and manage rooms."[1] What was not explained, and what has become evident since Zoom's widespread adoption, is that Zoom's focus on its goal of "frictionless" video conferencing came at the cost of proper attention being placed on security and on ensuring that Zoom users' private moments would not be shared with, exploited by, or obscenely hijacked by others.

[1] Priscilla Barolo, *Zoom Launches Enhanced Product Suite to Deliver Frictionless Communications* (Jan. 3, 2018), available at <https://blog.zoom.us/zoom-launches-enhanced-product-suite-to-deliver-frictionless-communications/> (Last Visited July 28, 2020).

4. In early 2020, usage of video conferencing, especially Zoom, increased dramatically in response to the COVID-19 pandemic. As of the end of December 2019, the maximum number of daily meeting participants, both free and paid, conducted on Zoom was approximately 10 million. In March 2020, Zoom reached more than 200 million daily meeting participants, both free and paid.[2] With the surge in usage also came increased scrutiny on Zoom's privacy policies and new flaws were revealed almost on a daily basis.[3]

5. On March 26, 2020, an article on Vice News' Motherboard tech blog revealed that, unbeknownst to users, the Zoom iPhone app was sending users' personal data to Facebook even if users did not have a Facebook account.[4] Zoom was providing a trove of data to third parties through its Apple iOS app, which implemented Facebook's user login "Software Development Kit" ("SDK"). Zoom admitted that it permitted the Facebook SDK to collect and share user information including: device carrier, iOS Advertiser ID, iOS Device CPU Cores, iOS Device Display Dimension, iOS Device Model, iOS Language, iOS Time zone, iOS Version.[5] While Zoom reported to have removed the Facebook SDK, Zoom continues to share similarly valuable user data with Google via Google's Firebase Analytics SDK, also integrated into the Zoom app. Plaintiffs never granted permission for third parties to extract and use such data—indeed, they were not even aware of the data transmission.

6. First and foremost this collection and sharing of Plaintiffs' data presented an egregious invasion of their privacy. As well, surreptitious transfer of data by Zoom to third

---

[2] Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[3] BBC News, *Zoom Under Increased Scrutiny As Popularity Soars* (April 1, 2020), available at <https://www.bbc.com/news/business-52115434> (Last Visited July 29, 2020).

[4] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account* (March 26, 2020), available at <https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account> (Last Visited July 28, 2020).

[5] Eric S. Yuan, *Zoom's Use of Facebook's SDK in iOS Client* (March 27, 2020), available at <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/> (Last Visited July 28, 2020).

parties harmed Plaintiffs by, among other things, consuming data for which Plaintiffs as part of their carrier's plan[6] and diminishing the value of their personal information. Perhaps worst of all, Plaintiffs are harmed when their extracted data is used to target and profile them with unwanted and/or harmful content.

7. On March 31, 2020, an article in The Intercept revealed as false Zoom's claims that it implemented end-to-end encryption ("E2E")—widely understood as the most private form of internet communication—to protect the confidentiality of users' video conferences.[7] In fact, Zoom was using its own definition of the term, one that failed to recognize Zoom's ability to access unencrypted video and audio from meetings. The definition of end-to-end encryption is not up for interpretation in the industry. Zoom's misrepresentations are a stark contrast to other videoconferencing services, such as Apple's FaceTime, which have undertaken the more challenging task of implementing true E2E encryption for a multiple party call.

8. On April 2, 2020, the New York Times published an article disclosing "a data-mining feature" related to a LinkedIn application that could be used to snoop on participants during Zoom meetings without their knowledge.[8]

9. Finally, reports continue to the present day of security breaches by unauthorized bad actors who hijack Zoom videoconferences. This practice has become so commonplace on the Zoom platform that it is referred to as "Zoombombing." Bad actors have disrupted private moments ranging from Alcoholics Anonymous meetings to

---

[6] Jeffrey Fowler, *In the middle of the night. Do you know who your iPhone is talking to?* (May 28, 2019), available at <https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/> (Last Visited July 30, 2020).

[7] Micah Lee and Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading* (March 31, 2020), available at <https://theintercept.com/2020/03/31/zoom-meeting-encryption/> (Last Visited July 28, 2020).

[8] Aaron Krolik and Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*, New York Times (April 2, 2020), available at <https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html> (Last Visited July 28, 2020).

Holocaust memorial services.[9] School classes and religious services all over the world have been affected. Recordings of these incidents and others end up on YouTube and TikTok. Concerns regarding Zoombombing led many organizations to ban employees' use of Zoom, including Google, SpaceX, NASA, the Australian Defence Force, the Taiwanese and Canadian governments, the New York Department of Education, and the Clark County School District in Nevada.[10]

10. The gravity of these data privacy violations cannot be overstated, including the data points leaked through the Facebook SDK. A growing and insidious practice in the "AdTech" industry to collect unique device data from consumers in order to build a profile, sometimes referred to as a "fingerprint," is used to allow third parties and data brokers to follow users' activities across their devices with essentially no limit. The practice of fingerprinting is unique and more damaging than the practice of tracking consumers' browsing activity with cookies.

11. Zoom had the affirmative duty to safeguard consumers' device information and, at the very minimum, to disclose the access, collection, and dissemination of consumers' data. Zoom failed to fulfill such duties.

12. Zoom users have an expectation of privacy in their videoconference communications, just as they do during telephone calls, irrespective of the substance of those communications. With social distancing and quarantine orders in place during the COVID-19 pandemic, videoconference platforms like Zoom have replaced conference rooms, churches and temples, AA meeting rooms, schools, and healthcare professionals' offices. The need for proper security with respect to private video conferences during which people discuss their religious views, struggle with addiction, where children are educated, and where healthcare professionals provide counsel, is paramount.

---

[9] Sebastien Meineck, *'Zoom Bombers' Are Still Blasting Private Meetings With Disturbing and Graphic Content* (June 10, 2020), available at <https://www.vice.com/en_us/article/m7je5y/zoom-bombers-private-calls-disturbing-content> (Last Visited July 28, 2020).

[10] *Id.*

13. Zoom has issued mea culpas after the reports exposing its privacy inadequacies, admitting to the problems and vowing to change its ways.[11] Nonetheless, independent ratings organizations consider Zoom's commitment to security on par with some of the worst of today's tech giants.[12] Nonetheless, Zoom continues to exploit the ever-greater market share of the video conferencing that has become a daily necessity with state stay-at-home orders for attending class, practicing our faith, engaging with loved ones, and getting the advice of medical professionals. Ensuring privacy and safety during the use of Zoom's popular platform is a matter of public interest.

14. Each of these security lapses presents an independently actionable event. Data sharing relating to Facebook, Google Analytics, other third parties' SDKs used by Zoom, and third-party applications with which the Zoom platform works are breaches of common law, contract, and statutory duties to refrain from sharing and collecting users' valuable data without proper disclosures. Similarly, although they arise from the same freewheeling security practices, Zoom's misrepresentations regarding of E2E encryption and its security protocols to prevent Zoombombings, are independently actionable.

15. Zoom's popularity is such that it has become ubiquitous despite its security shortcomings. Despite knowledge of Zoom's shortcomings and a desire to maintain one's privacy, many people including Plaintiffs nonetheless are required to use Zoom for work, school, or other purposes, including. For instance, this Court has been using Zoom to conduct hearings remotely during the pandemic.[13]

---

[11] CEO Eric Yuan himself admitted that Zoom fell "short of our community's—and our own—privacy and security expectations." Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[12] As of May 2020, PrivacySpy gave Zoom a privacy score of 3.5 out of 10, similar to that of Facebook (3.2) and Amazon (3.5). *See* <https://privacyspy.org/product/zoom/> (Last Visited July 28, 2020).

[13] *See* Northern District of California, *Preparing to Participate in a Zoom Video Conference*, available at <https://www.cand.uscourts.gov/zoom/> ("Participants: If you do not

16. Accordingly Plaintiffs, on behalf of themselves and all others similarly situated, bring this action to ensure that Zoom vastly improves its security practices going forward and to recover for past privacy violations.

PARTIES

17. **Plaintiff Kristen Hartmann** is, and at all times relevant was, a citizen of the State of Maryland residing in Rockville, Maryland. On March 25, 2019, Ms. Hartmann registered to use Zoom through her personal iPhone. Ms. Hartmann accessed Zoom's video conferencing services at least once prior to the creation of her personal Zoom account on March 25, 2019 using an iOS device. Ms. Hartmann purchased a "Zoom Pro" account for her own personal use and accessed Zoom's video conferencing services. Ms. Hartmann accesses Zoom's video conferencing services through her iPhone running the iOS operating system, and her Apple computers' macOS operating system. Ms. Hartmann hosted or attended the majority of her Zoom meetings at or near her home residence.

18. Ms. Hartmann regularly used her Zoom account as a "safe place" to host meetings for a professional women's group; the topics discussed in these meetings included encounters with sexual harassment in the workplace, sensitive and private discussions about workplace conflicts, and confidential insider information about the employers and work environments of the participants. Since March 2020, Ms. Hartmann also used Zoom to stay in touch with her friends and family. Many of these Zoom meetings included conversations discussing the mental and physical health of the participants in coping with illness, identification by name and medical diagnoses of people who became ill, the resulting impact on their families, and discussion of private financial information. Several of her Zoom meetings were deeply private and emotional as family and friends became ill.

19. Ms. Hartmann was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook and Google. Nor

---

already have a Zoom account, set one up at https://zoom.us.") (Last Visited July 30, 2020).

was she aware that Zoom would allow third parties, like Facebook and Google, 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 advertising and behavior influencing purposes. Rather, Ms. Hartmann 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. Likewise, Ms. Hartmann did not give Zoom permission to access, take or use her personally identifiable information.

20. Ms. Hartmann purchased her account having seen advertising that Zoom Meetings were equipped with end-to-end encryption technology, which was a feature that she valued and for which she was willing to pay a premium. After comparing Zoom against GoToMeeting and Webex, Ms. Hartmann selected Zoom over other options largely due to Zoom's representations of its end-to-end encryption. Further, because of the confidential nature of the Zoom meetings she hosted, Ms. Hartmann would periodically check to ensure the calls were end-to-end encrypted by hovering her cursor over the green lock icon in the application during Zoom meetings. The icon would then show text indicating active end-to-end encryption. Had Ms. Hartmann known that Zoom meetings were not actually end-to-end encrypted, she would not have paid for a Zoom Pro subscription, or she would have paid less for it.

21. **Plaintiff Isabelle Gmerek** is, and at all times relevant has, resided in the State of California. She currently lives in Carlsbad, California.

22. Ms. Gmerek does not possess a registered account with Zoom. She accessed Zoom's video conferencing services through the Zoom links that she received without creating an account. Ms. Gmerek accesses Zoom's video conferencing services mainly through her Android phone but also on occasion through her Amazon Fire 7 tablet. Ms. Gmerek attended the majority of her Zoom meetings from her home residence.

23. Ms. Gmerek uses Zoom for telehealth. She began using Zoom's services on March 14, 2020 for meetings with her psychologist in reliance on representations by Zoom that it was a secure method of videoconferencing, that it was in full compliance with the Health Insurance Portability and Accountability Act ("HIPAA"), and that it had not misrepresented the security features available to users. Ms. Gmerek also attended her doctors' appointments and mindfulness classes through Zoom. In particular, Ms. Gmerek attended two such classes on March 14, 2020 and March 22, 2020 where she discussed personal and private issues concerning her mental health.

24. Ms. Gmerek uses Zoom at least twice a week as an attendee, but she has no way of determining whether Zoom's representations that her personal information will be secure are, in fact, correct.

25. Ms. Gmerek was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook and Google. Nor was she aware that Zoom would allow third parties, like Facebook and Google, 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 advertising and behavior influencing purposes. Rather, Ms. Gmerek 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. Likewise, Ms. Gmerek did not give Zoom permission to access, take or use her personally identifiable information.

26. **Plaintiff Lisa T. Johnston** is, and at all times relevant was, a resident of the State of California and the State of Colorado residing in Santa Monica, California and Colorado Springs, Colorado, respectively. In July 2019, Ms. Johnston registered to use Zoom through her Apple laptop. Ms. Johnston accesses Zoom's videoconferencing services through her Apple laptop running the macOS operating system and iPhone, running the iOS

operating system. Ms. Johnston attended the majority of her Zoom meetings from her home residences in Santa Monica, California and Colorado Springs.

27. Ms. Johnston used her Zoom account to attend meetings involving confidential information of real estate buyers and sellers, details of client transactions, and proprietary business information.

28. Ms. Johnston was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook and Google. Nor was she aware that Zoom would allow third parties, like Facebook and Google, 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 advertising and behavior influencing purposes. Rather, 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. Likewise, Ms. Johnston did not give Zoom permission to access, take or use her personally identifiable information.

29. **Plaintiff M.F.** is, and at all times relevant was, a citizen of the State of California residing in Culver City, California. M.F. accessed Zoom's video conferencing services without first creating a Zoom account. M.F. is, and at all relevant times was, under the age of 13. M.F. accesses Zoom's video conferencing services through iPads running the iOS operating system, a Windows laptop, and an Android phone. M.F. began using Zoom on an iPad to attend online classes on March 19, 2020. M.F. attended the majority of his Zoom meetings from his home residence.

30. M.F. was not aware, and did not understand, that Zoom would collect and share his personal information with third parties, including Facebook and Google. Nor was he aware that Zoom would allow third parties, like Facebook and Google, to access his personal information and combine it with content and information from other sources to create a unique identifier or profile of his for advertising and behavior influencing purposes.

Rather, M.F. 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. Likewise, M.F. did not give Zoom permission to access, take or use his personally identifiable information.

31. **Plaintiff Therese Jimenez** is, and at all times relevant was, a citizen of the State of California residing in Culver City, California. Plaintiff Jimenez is the mother and natural guardian of Plaintiff M.F. Ms. Jimenez accesses Zoom's video conferencing services through her iPad, running the iOS operating system, Windows laptop, and Android phone. On March 19, 2020, Ms. Jimenez registered to use Zoom through her personal Android Galaxy Note 8 phone. Ms. Jimenez accessed Zoom's video conferencing services at least once prior to the creation of her personal account on March 17, 2020. Ms. Jimenez attended the majority of her Zoom meetings from her home residence.

32. Ms. Jimenez used Zoom to attend parent-teacher conferences at M.F.'s school, among other school-related events. Ms. Jimenez also used Zoom to stay in touch with her friends and family. Many of these Zoom meetings included conversations discussing the mental and physical health of the participants in coping with illness, identification by name and medical diagnoses of people who became ill, the resulting impact on their families, and discussion of private financial information.

33. When Ms. Jimenez registered with Zoom as a user, Ms. Jimenez was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook and Google. Nor was she aware that Zoom would allow third parties, like Facebook and Google, 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 advertising and behavior influencing purposes. Rather, Ms. Jimenez 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. Likewise, Ms. Jimenez did not give Zoom permission to access, take or use her personally identifiable information.

34. **Plaintiff Saint Paulus Lutheran Church** is, and at all times relevant was, a citizen of the State of California. Saint Paulus Lutheran Church accesses Zoom's video conferencing services through an Apple computer, running macOS operating system, commencing on March 17, 2020.

35. Saint Paulus Lutheran Church is an Evangelical Lutheran church located at 1541 Polk Street, San Francisco, California. Founded in 1867, Saint Paulus has been serving countless congregants, including the homeless, the marginalized, and the underserved, in San Francisco for over 150 years. The Reverend Daniel Solberg is currently serving as the eighth Pastor of Saint Paulus Lutheran Church, a position he has held since November of 1999. Saint Paulus is a citizen of California. In Saint Paulus's long history, it survived the Great Earthquake and Fire of 1906, the social and cultural turmoil of the 1960s–70s, and a 1995 fire that destroyed its 103 year-old cathedral building.

36. **Plaintiff Heddi N. Cundle** is, and at all times relevant was, a citizen of the State of California residing in San Francisco, California. She is the administrator at Saint Paulus. She organizes Saint Paulus's weekly bible-study classes. Ms. Cundle registered an account with Zoom on behalf of Saint Paulus, and accessed Zoom's videoconferencing on behalf of Saint Paulus. Ms. Cundle also registered a separate account with Zoom for personal use, and accessed Zoom's videoconferencing for personal purposes on April 2, 2020. Ms. Cundle used Zoom at least once in March 2020 before registering for her personal account. Ms. Cundle accesses Zoom's video conferencing services through her iPhone running the iOS operating system and Windows laptop.

37. Ms. Cundle used Zoom to attend religious events, including a Passover Seder where a select few were invited to dine virtually with the rabbi. The topics at these meetings include the mental and physical health of meeting participants, the death of family members,

and religious discussions. Ms. Cundle attended the majority of her Zoom meetings from her home.

38. Ms. Cundle was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook and Google. Nor was she aware that Zoom would allow third parties, like Facebook and Google, 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 advertising and behavior influencing purposes. Rather, Ms. Cundle 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. Likewise, Ms. Cundle did not give Zoom permission to access, take or use her personally identifiable information.

39. Further, Ms. Cundle on behalf of Saint Paulus was not aware, and did not understand, that Zoom would collect and share Saint Paulus's private information with third parties, including Facebook and Google. Nor was she aware that Zoom would allow third parties, like Facebook and Google, to access Saint Paulus's private information and combine it with content and information from other sources to create a unique identifier or profile of Saint Paulus for advertising purposes. In fact, Ms. Cundle on behalf of Saint Paulus 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. Likewise, Ms. Cundle on behalf of Saint Paulus did not give Zoom permission to access, take or use its personally identifiable information.

40. To conduct Saint Paulus's weekly Bible-study class in compliance with the State's stay-at-home order, Saint Paulus decided to transition its gatherings online. Prior to registering for Zoom, Ms. Cundle on behalf of Saint Paulus researched video-conferencing

services such as Webex and GoToMeeting. A few days before March 17, 2020, Ms. Cundle on behalf of Saint Paulus reviewed Zoom's website and relied on Zoom's representations that Zoom valued the safety and security of its users in selecting Zoom's services.

41. Ms. Cundle registered an account with Zoom on behalf of Saint Paulus. Saint Paulus paid the fee to use a "Zoom Pro" account. Through Ms. Cundle and congregants, Saint Paulus has continued to use and access Zoom videoconferencing services.

42. For the May 6, 2020 Saint Paulus Bible-study class, Ms. Cundle followed Zoom's instructions to set up a password-protected meeting. Despite her efforts, an intruder hacked into the Bible-study meeting and hijacked the meeting, displaying child pornography images and video to the participants. During the Zoombombing incident, Ms. Cundle and the other participants were unable to minimize or close the video screen. Despite Ms. Cundle's efforts to use the tools Zoom made available to her, she could not stop the graphic display or eject the intruder and, thus, closed the meeting and instructed the participants to rejoin. As soon as participants rejoined, the intruder again hijacked the Bible study with further displays of child pornography. Despite Ms. Cundle's efforts to use the tools Zoom made available to her, she could not stop the graphic display or eject the intruder and, thus, after attempting, unsuccessfully, to block the intruder or close the meeting, she finally closed the meeting. The depravity of the video footages was beyond description here. Ms. Cundle and the other participants were traumatized and deeply disturbed.

43. Immediately following the May 6, 2020 Zoombombing incident, Ms. Cundle reported the incident to Zoom. In response, Zoom admitted that the intruder was "a known serial offender who disrupts open meetings by showing the same video" and, shockingly, had "been reported multiple times to the authorities." Despite this, it was not until Ms. Cundle reported the May 6, 2020 Zoombombing incident that Zoom finally blocked the intruder "from joining future meetings using the same Zoom software."

44. **Plaintiff Oak Life Church** is, and at all relevant times was, a citizen of the State of California. Oak Life Church is located at 337 17th Street, Oakland, California. Founded in 2014, Oak Life Church is a decentralized, non-denominational Christian church

serving the marginalized and the underserved in the community. Christopher Scott is the lead pastor at Oak Life Church. Beginning on March 17, 2020, Oak Life Church registered an account with Zoom, which it subsequently converted to a paid "Zoom Pro" account. Thereafter, Oak Life Church accessed Zoom's videoconferencing services for team meetings, Bible studies, prayer meetings, and church services. Oak Life Church accesses Zoom's video conferencing services through an iPhone running the iOS operating system and Apple computers, running the macOS operating system.

45. Oak Life Church used Zoom to conduct "check-ins" with its congregants, engage in pastoring counseling and community care, hold board meetings where sensitive financial information and the mental, physical, or financial health of the Oak Life Church's congregants were discussed. Many of the congregants relied on Oak Life Church as their spiritual support system. On the Zoom meetings, congregants discussed very private issues such as loss of job, illnesses in their families, and their mental and physical health.

46. Prior to signing up for Zoom's services, Oak Life Church reviewed Zoom's website and concluded from Zoom's online representations, on or shortly before March 17, 2020, it would be a safe and secure platform to use. Oak Life Church was not aware, and did not understand, that Zoom would collect and share its private information with third parties, including Facebook and Google. Nor was Oak Life Church aware that Zoom would allow third parties, like Facebook and Google, to access its private information and combine it with content and information from other sources to create a unique identifier or profile of Oak Life Church for advertising purposes. In fact, Oak Life Church 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. Likewise, Oak Life Church did not give Zoom permission to access, take or use its personally identifiable information.

47. On April 19, 2020, Oak Life Church and its members were subjected to a Zoombombing incident during a regularly-scheduled Sunday church service. Following

protocols provided by Zoom, the meeting on April 19, 2020 was set up with a waiting room, mute on entry, and no ability for users to share their screens. Thirty minutes into the service, while the host was using Zoom's screen-sharing feature, the host's dedicated screen started to experience issues, whereby a "black box" appeared on the host's screen, covering the image being projected to other meeting participants. When efforts to fix the issue were unsuccessful, the host stopped the screen sharing. Shortly thereafter, the Zoombombing incident took place, whereby child pornography images and video were displayed to the participants. After attempting, unsuccessfully, to block the intruder, the host shut down the meeting as quickly as possible. But the damage was done. The participants from that meeting, many of whom were trauma survivors to begin with, were left traumatized and devastated. Oak Life Church was required to hire trauma counsellors and establish support groups to assist its congregation in dealing with the resulting trauma.

48. Immediately following the April 19, 2020 Zoombombing incident, Oak Life Church reported the incident to Zoom. In response, Zoom admitted that the intruder was a "known offender" and that the intruder had used the same IP address to attack Zoom's network before. Despite this, it was not until Oak Life Church reported the April 19, 2020 Zoombombing incident that Zoom finally "blocked the offender from joining future meetings using the same Zoom software."

49. **Plaintiff Stacey Simins** is, and at all times relevant was, a citizen of the State of Texas residing in Austin, Texas. Ms. Simins purchased a "Zoom Pro" account and accessed Zoom's videoconferencing services in March 2020. Ms. Simins accesses Zoom's video conferencing services through her iPhone, running the iOS operating system, Apple laptop, running the macOS operating system, and Apple desktop, running the macOS operating system.

50. Ms. Simins was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook and Google. Nor was she aware that Zoom would allow third parties, like Facebook and Google, 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 advertising and behavior influencing purposes. Rather, Ms. Simins 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. Likewise, Ms. Simins did not give Zoom permission to access, take or use her personally identifiable information.

51. Ms. Simins is the operator of a burlesque dance studio and uses her Zoom Pro account for teaching classes. On multiple occasions, uninvited men showed up in dance classes taught by her studio. These men were present in the dance classes for several minutes before Ms. Simins shut down the meeting. As a result, Ms. Simins lost a significant portion of her clientele; 10-15 full time members and any new clients who were present for the incidents will no longer participate in online classes.

52. **Plaintiff Caitlin Brice** is, and at all times relevant was, a citizen of the State of Illinois residing in Chicago, Illinois. Ms. Brice registered for an account with Zoom for personal use, and accessed Zoom's videoconferencing services on January 17, 2019. Ms. Brice also accesses Zoom's videoconferencing services through a paid account maintained by her employer for work purposes commencing on August 16, 2018. Ms. Brice accesses Zoom's video conferencing services through her Android phone, tablet, and Windows laptop.

53. Ms. Brice was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook and Google. Nor was she aware that Zoom would allow third parties, like Facebook and Google, 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 advertising and behavior influencing purposes. Rather, Ms. Brice 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. Likewise, Ms. Brice did not give Zoom permission to access, take or use her personally identifiable information.

54. Ms. Brice used Zoom for speech therapy meetings with her students in reliance on representations by Zoom that it was a secure method of videoconferencing, that it was in full compliance with HIPAA, and that it had not misrepresented the security features available to users. Had Ms. Brice known that Zoom meetings were not actually end-to-end encrypted, she would have requested permission to use a different platform for her school contract clients.

55. In April or May 2020, Ms. Brice attended a Zoom event during which the participants were subjected to intentional pornographic material when unknown men dropped into the meeting with the intention of disrupting it.

56. **Plaintiff Peter Hirshberg** is, and at all times relevant was, a citizen of the State of California residing in San Francisco, California. Mr. Hirshberg purchased a "Zoom Pro" account for his own personal use and accessed Zoom's video conferencing services on March 17, 2020. Mr. Hirshberg had been using Zoom without an account since at least June 4, 2015. Mr. Hirshberg accesses Zoom's video conferencing services through his iPhone and iPads, running the iOS operating systems, and his Apple computer, running the macOS operating system.

57. Mr. Hirshberg used Zoom for both work and in his personal life. Mr. Hirshberg conducted business calls through Zoom, including private investment meetings discussing sensitive financial information, conference with clients and partners discussing highly private business strategies, and calls with his accountant. Mr. Hirshberg also used Zoom to stay in touch with his friends and family. Several of these Zoom meetings included conversations discussing the mental and physical health of the participants in coping with illness, identification by name and medical diagnoses of people who became ill, the resulting impact on their families, and discussion of private financial information.

58. Mr. Hirshberg was not aware, and did not understand, that Zoom would collect and share his personal information with third parties, including Facebook and Google. Nor was he aware that Zoom would allow third parties, like Facebook and Google, to access his personal information and combine it with content and information from other sources to create a unique identifier or profile of him for advertising and behavior influencing purposes. Rather, Mr. Hirshberg 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. Likewise, Mr. Hirshberg did not give Zoom permission to access, take or use his personally identifiable information.

59. On May 30, 2020, Mr. Hirshberg attended a Zoom event during which the participants were subjected to intentional anti-semetic material when uninvited intruders dropped into the meeting with the intention of disrupting it.

60. **Plaintiff Angela Doyle** is, and at all times relevant was, a citizen of the State of California residing in San Diego, California. Ms. Doyle registered for a Zoom account on or around March 13, 2020 for her own personal use and accessed Zoom's video conferencing services. Ms. Doyle converted her free Zoom account into a "Zoom Pro" account on March 28, 2020. Ms. Doyle accessed Zoom's video conferencing services at least once prior to the creation of her personal account. Ms. Doyle accesses Zoom's videoconferencing through her iPhone running the iOS operating system, and Windows computer.

61. Ms. Doyle used Zoom to stay in touch with her friends and family. Many of these Zoom meetings included conversations discussing the mental and physical health of the participants in coping with illness, identification by name and medical diagnoses of people who became ill, the resulting impact on their families, and discussion of private financial information.

62. Ms. Doyle was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook and Google. Nor

was she aware that Zoom would allow third parties, like Facebook and Google, 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 advertising and behavior influencing purposes. Rather, Ms. Doyle 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. Likewise, Ms. Doyle did not give Zoom permission to access, take or use her personally identifiable information.

63. **Defendant Zoom Video Communications, Inc.** is a Delaware corporation with its principal place of business and headquarters in San Jose, California.

JURISDICTION AND VENUE

64. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000 (exclusive of interests and costs), because there are more than 100 members in each of the proposed classes, and because at least one member of each of the proposed classes is a citizen of a State different from Defendant.

65. This Court has personal jurisdiction over Defendant because it is headquartered in California, and regularly conducts business in California.

66. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

STATEMENT OF FACTS

ZOOM AND ITS SERVICES

67. Zoom provides a cloud-based communications platform for video and audio conferencing to both business and individual consumers throughout California and the United States. Zoom's products and services can be used across mobile devices, desktops, telephones, and room systems.

68. Zoom purports to provide "[s]implified video conferencing and messaging across any device."[14]

69. Zoom offers different tiers of services for its registered users: Basic, Pro, Business, and Enterprise. Subscription fees range from free for the Basic version, to $19.99 per month per user for the Enterprise version.[15] While users receive additional features under more expensive subscriptions, Zoom's representations regarding the security of its video conferences and its published privacy policy with its representations regarding data sharing are common to all subscription levels.

70. In March 2019, Zoom boasted that its platform "has been used to conduct tens of billions of meeting minutes" since its founding in 2011.[16]

71. Zoom has developed mobile apps to access its most popular service, Zoom meetings, for both the iPhone and Android. Zoom provides software to access Zoom meetings on a desktop computer for both Windows and Mac operating systems. Further add-ons, add-ins, plugins, and extensions are available for Microsoft Office 360, Outlook, Gmail, Firefox, Chrome, and Safari.

72. Parties who host a Zoom meeting invite participants in one of two ways. First, a host may utilize a Zoom feature whereby Zoom will link to the host's email account directly and provide a form email containing the URL for participants of the Zoom meeting to use, or by otherwise providing that URL for participants to enter into their web browser.

73. Alternatively, Zoom provides a telephone number and access code for participants who wish to call with a telephone as a voice-only participant.

74. Users who have a Zoom app on their computer or cellphone are directed to that app after clicking on the URL. User who do not have the Zoom app are directed to a Zoom webpage where the meeting is hosted. Voice-only telephone users participate in the

[14] <https://zoom.us/meetings> (Last Visited July 28, 2020).

[15] <https://zoom.us/pricing> (Last Visited July 28, 2020).

[16] *Id.*

meeting as one would with a normal telephone conference call, *i.e.* without employing any app or webpage.

75. In early 2020, usage of video conferencing increased even more dramatically in response to the coronavirus pandemic, and Zoom's usage surged higher. As of the end of December 2019, Zoom had a maximum number of 10 million daily meeting participants, both free and paid. In March 2020, Zoom reached more than 200 million daily meeting participants, both free and paid.[17]

DATA SHARING, BEHAVIOR TRACKING, USER PROFILING, AND ZOOM'S PRIVACY POLICY

Facebook Data Sharing

76. On March 26, 2020, Joseph Cox posted an article on Vice Media Group's website Motherboard revealing that the Zoom iPhone app sends data to Facebook even if the Zoom user does not have a Facebook account.[18] The article states "The Zoom app notifies Facebook when the user opens the app, details on the user's device such as the model, the time zone and city they are connecting from, which phone carrier they are using, and a unique advertiser identifier created by the user's device which companies can use to target a user with advertisements." The article continues that Zoom confirmed the data collection several days after it was asked for comment and a day after the publication of the article.

77. On March 27, 2020, Zoom's Founder and Chief Executive Officer, Eric Yuan, published a statement asserting that Zoom was unaware until two days prior that its Zoom iPhone app was providing any of its users' personal data to Facebook. Nevertheless, Mr.

[17] Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[18] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account* (March 26, 2020), available at <https://www.vice.com/en_us/ article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account> (Last Visited July 28, 2020).

Yuan represented that Zoom "takes its users' privacy extremely seriously" and that its "customers' privacy is incredibly important to us."[19]

78. Mr. Yuan stated that the data sharing was the result of Zoom's use of the Facebook software developer kit ("SDK").[20]

79. An SDK is a collection of software development tools in one installable package. The Facebook SDK allows mobile app developers to integrate Facebook tools (like "Login with Facebook" and Facebook Analytics Tools) within the mobile app. They ease creation of applications, because the code has already been written and debugged by the provider of the SDK (in this case Facebook). Due to the nature of how Facebook's SDKs are implemented by parties such as Zoom, any data collected via the SDK is, by default, automatically passed to Facebook, allowing Facebook to keep a log of app usage.

80. Use of the Facebook SDK is voluntary for the convenience of app developers. It is used not only to offer the "Log in with Facebook" feature, but also to track user activity and behavior within the application, as well as traffic to and within the application. In exchange for this built and packaged software, Facebook receives the same data Zoom collected using Facebook's SDK.

81. Mr. Yuan confirmed that users' personal data released to Facebook included: Application Bundle Identifier; Application Instance ID; Application Version; Device Carrier; iOS Advertiser ID; iOS Device CPU Cores; iOS Device Disk Space Available; iOS Device Disk Space Remaining; iOS Device Display Dimensions; iOS Device Model; iOS Language; iOS Timezone; iOS Version; and IP Address.[21] An updated version of the Zoom app was released which would prevent the release of information to Facebook. Users were encouraged, but not required, to update to this newer version of the Zoom app.

---

[19] Eric S. Yuan, *Zoom's Use of Facebook's SDK in iOS Client* (March 27, 2020), available at <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/> (Last Visited July 28, 2020).

[20] *Id.*

[21] *Id.*

82. While Zoom's public statements referred only to iOS, reports from Privacy International and The Wall Street Journal confirm that apps sending data to Facebook without a user's consent and without proper disclosure is a problem that is universal across both iOS *and Android.*[22]

83. The bulleted list on Zoom's March 27, 2020 blog was not a complete disclosure of all information that was passed to Facebook. Mr. Yuan stated that the list was only "examples" of data shared with Facebook without explaining why the entire list of shared data was not provided. Facebook's online handbook for developers states that the Facebook SDK is not limited to information reported by Zoom, but also includes "explicit events, implicit events, and automatically logged events, Facebook app ID," and potentially even more information.[23] The range of information this description could include is staggering. Facebook's SDK allows app developers to integrate their apps with Facebook's platform and contains a number of core components: Analytics, Ads, Login, Account Kit, Share, Graph API, App Events and App Links. For example: Facebook's SDK also offers Analytics (data, trends, and aggregated audience insights about the people interacting with the app), as well as Ads and reading and writing to Facebook's Graph API.

84. Additionally, "Analytics" SDKs, like the one implemented by Zoom, allow developers to collect "events," i.e. additional data points and types of data. Developers can register any event that they want to track even if it's not part of the events reported by the SDK by default (events that come pre-packaged in the SDK). The developer of a communications app like Zoom might want to monitor in their analytics dashboard, the types of meetings users are attending and what plugins are being used in a particular geographical area. In addition to Facebook, Firebase (also used by Zoom) is known to

[22] *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, The Wall Street Journal (February 22, 2019), available at <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636> (Last Visited October 28, 2020).

[23] <https://www.facebook.com/business/m/one-sheeters/gdpr-developer-faqs> (Last Visited July 29, 2020).

collect this customized information.

85. This level of detail gives SDKs provided by third parties like Facebook and Google the ability to track users' every move and constitutes a danger to their privacy, especially when analytics services collect information that can identify users uniquely.

86. According to "Built With," an online service that provides a profile of all the software implemented by a given company, Zoom uses several Facebook products. This is significant because the type of data collected by default from Facebook depends on the kind of Facebook product app and web developers choose to implement. Just the Facebook SDK itself "contains a number of core components: Analytics, Ads, Login, Account Kit, Share, Graph API, App Events and App Links." In addition to the Facebook SDK, Zoom has implemented: Facebook Domain Insights, Facebook Pixel, Facebook Conversion Tracking, Facebook Signal, Facebook for Websites, and Facebook Custom Audiences. The profile says nothing about the software being limited only to iOS devices.[24]

87. Following the adoption of the European Union's Data Protection Regulation ("GDPR") in 2018, Facebook SDK started to allow developers to disable automatically logged events like app installation and login. However, developers must manually and deliberately go into the code and change the default settings. Based on public statements made by Zoom, Plaintiffs are informed and believe that Zoom did not change this default setting. Thus, Facebook was receiving this information before users ever had access to any terms and conditions or privacy disclosures.

88. For every app implementing the Facebook SDK, Facebook starts receiving data on its servers the second the installation process begins on the device by default. From the very first install and launch of an app (such as Zoom) that utilizes Facebook's SDK, data is sent to Facebook. This happens regardless of whether the user has created a Zoom or Facebook account, and, even worse, before the user would have even encountered

[24] Zoom.us Detailed Technology Profile, available at <https://builtwith.com/detailed/zoom.us> (Last Visited July 29, 2020).

Zoom's terms and conditions or any privacy disclosures. Furthermore, the data sharing occurs even if someone has "opted out" of social media and advertising for that particular app.

89. When initially starting an application, the Facebook SDK gets invoked several times, but one particular invocation sends an "Application Install" as an "event" to the Facebook Graph API (Application Programming Interface) detailing:

- the user's IP Address, allowing Facebook to Geo-Reference your location and correlate your device with other devices using the same IP Address;
- Advertiser_id, a unique identifier shared across all applications installed on the user's device, which allows advertisers to link data about the user and to correlate most of that data;
- device model, screen resolution, and system language;
- carrier name and timezone, allowing Facebook not only to know your location through IP Address, but also if you are traveling or roaming; and
- the origin of the application (or the App Store), allowing Facebook to learn whether the user installed this app from the Manufacturer's store or elsewhere.

90. All these data points create a fingerprint of the user's identity.

Device Fingerprinting, Tracking, and User Profiling

91. Zoom attempted to downplay the personal-identifying nature of the information released to Facebook. Mr. Yuan stated that the data sent to Facebook's servers was not related to Zoom conference attendees but, "rather, included information about devices . . . ." This is misleading because not only is the shared information used to "fingerprint" the user's identity as explained below but, when combined with information regarding other apps used on the same device, this information is used to build precise and detailed profiles on individuals, ultimately identifying characteristics such as race, age, sexual orientation, relationship status, socioeconomic status, parental status, and much more. Facebook's longstanding indirect data collection practices rely on apps to autonomously

collect and send information about app usage to the social network without telling users about the arrangement. This third party tracking amounts to total surveillance.

92. Third party tracking can be broadly defined as any transfer of personally identifying data from an online service, to an entity other than the provider of that service. Third party tracking allows companies like Facebook and Google to identify users and track their behavior across multiple digital services. Such networks link activity across multiple apps to a single user, and also link to their activities on other devices or mediums like the web. This enables construction of detailed profiles about individuals, which could include inferences about shopping habits, socio-economic class or likely political opinions. These profiles can then be used for a variety of purposes, from targeted advertising to credit scoring and targeted political campaign messages.

93. To create these detailed profiles, identifying information is required from the device. The Facebook SDK collects different types of persistent unique identifiers, but even just the Advertiser_ID (AAID for Android and IDFA for iOS) is a unique identifier, persistent personal identifier used for long term tracking – no other phone on the planet has this number. In addition to the Advertiser ID, Zoom listed other identifiers such as Application Bundle Identifier; Application Instance ID that are used to specifically narrow who is doing what on a specific device, when they are doing that activity, and where.

94. In fact the primary purpose of Google advertising ID, "AAID" or Apple's iOS equivalent, "IDFA" is to allow advertisers to link data about user behavior from different apps and web browsing into a comprehensive profile. The process of linking different browsers and mobile apps is referred to in the industry as "ID syncing."

95. Mobile devices contain many different types of identifiers, such as information relating to the device, as well applications, tools or protocols that, when used, allow the identification of the individual to whom the information may relate. However, even in the absence of such identifiers, researchers have found that knowledge of any four apps installed on users' smartphones is enough to successfully track 95% of users.

96. While Apple and Google claim that device owners can "opt-out" of targeted

advertising, network traffic tests show that when a phone is set to opt out of targeted advertising, even *more* information is sent to Facebook than when the device owner allowed targeted advertising.[25]

97. The data that apps send to Facebook typically include information such as the fact that a specific app was opened or closed. This sounds fairly basic, but it really isn't. Since behavior and activity in each app is sent with a unique identifier, specific to each device, (the Advertising ID) this data detailing user behavior is linked into a profile resulting in broad surveillance of practically all of someone's interests, identities and daily routines.

98. Facebook (and other third parties to whom user behavior and activity is sent) combines data from different apps to create a fine-grained and intimate picture of people's activities, interests, behaviors and routines, some of which can reveal special category data, including information about people's health or religion. Facebook then combines this data with data brokers to place people in categories like, "heavy alcohol spender at home."

99. Furhermore, third parties like Facebook also perform cross-device tracking, the practice of linking multiple devices, such as smartphones, television sets, smart TVs, and personal computers, to a single user. The more granular a user profile, the more intimate inferences can be derived about people's likely attributes, identities, habits and opinions.

100. Obtaining data on and from a device, including the transmission of data linked to a unique identifier from an app to Facebook via the Facebook SDK, constitutes the processing of personal data. Data relating to the use of specific apps, including usage logs, from which an individual is directly or indirectly identifiable is also personal data.

101. Users of Zoom were completely unaware that their entire Zoom usage history,

[25] Privacy International, *How Apps on Android Share Data with Facebook (even if you don't have a Facebook Account),* December 2018, available at <https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf> (Last Visited October 27, 2020).

activity, and behavior patterns, and potentially with whome they were connecting with on Zoom or other "customized events" were being shared with Facebook.

102. Even for individuals without a Facebook account, a shadow profile is built based on a compilation of app usage on the specific individual's device. Every interaction someone has through apps installed on their device (that utilize Facebook's SDKs) is logged and sent to Facebook. The more complete the profile, the more monetary value it holds on the personal data market.

103. Facebook's Cookies Policy describes two ways in which people who do not have a Facebook account can control Facebook's use of cookies to show them ads. However, Privacy International has tested both opt-outs and found that they had no discernible impact on data sharing.

104. In the worst cases, "Fingerprinting" is a process by which websites and applications can discern that a device belongs to a particular user based on system configurations. Fingerprinting completely circumvents user choice because it can detect the identity of a device, which makes the ability to reset the Advertising ID completely futile. It is effectively impossible for individuals to give informed consent about the way their data is collected and used when these circumventing tactics are used because information that sounds benign is aggregated to uniquely and specifically identify someone. Promises made by companies not to share personally identifiable information are meaningless.

105. SDKs like those used by Zoom are like the mobile equivalent of cookies, but with more power because the apps are installed on the device itself unlike a website that is opened and closed. Cookies are data sent to third party servers to obtain information about the consumer's browsing activity. Consumers can remove the cookies cached in their browser through various options built into their browsers. Many browsers also give consumers the ability to block all cookies—so first party publishers and third-party data brokers are not able to place cookies in the consumers' browsers or retrieve data from them.

106. Device fingerprinting using mobile apps (in contrast to web pages) is

nefarious because the practice gives consumers no choice about whether the websites they visit, or third parties, can observe their internet activity. A device fingerprint is created with the exact types of data that Zoom provided to Facebook via integration of the Facebook SDK into the Zoom app for Android and iOS operating systems.

107. Consumer device data, such as that leaked by Zoom, is especially valuable because consumers increasingly block cookies and take precautions against cookie tracking. The device data enables fingerprinting, an even more powerful tracking tool than cookies.

108. Even tech giants admit that device fingerprinting is wrong. Indeed, the director of Chrome Engineering at Google stated regarding fingerprinting in an August 2019 blog post:

> With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites. Unlike cookies, users cannot clear their fingerprint, and therefore cannot control how their information is collected. We think this subverts user choice and is wrong.[26]

Data Sharing With Google

109. Facebook isn't the only third party receiving detailed user data from Zoom. Even though Zoom reports it removed the Facebook SDK, the application is still sharing data with Google according to a July 13, 2020 Exodus report. Zoom shares information with Google via the Google Firebase Analytics tracker. This is confirmed by recent network traffic tests on the Zoom app for Android. A tracker is a piece of software that gathers information on the person using the application or on the smartphone being used. A tracker typically is distributed as an SDK, just as discussed in the Facebook context.[27]

110. According to Zoom's Technology Profile from BuiltWith, Zoom continues

[26] Justin Schuh, *Building a More Private Web* (Aug. 22, 2019), available at <https://www.blog.google/products/chrome/building-a-more-private-web/> (Last Visited July 29, 2020).

[27] *See* <https://reports.exodus- privacy.eu.org/en/reports/us.zoom.videomeetings/latest/> (Last Visited July 30, 2020).

to implement Google's software including but not limited to: Google Optimize 360, Google Analytics Event Tracking, Google Universal Analytics, Google Analytics with Ad Tracking Google Converstion Tracking, Google Conversion Linker, DoubleClick Floodlight, Google Analytics Ecommerce, and Google Analytics 360 Suite.

111. Zoom allows Google the following permissions and access (among many things):

- GPS (precise) and network-based (approximate) location
- "Do Not Disturb" setting
- Available wi-fi connections
- Bluetooth settings
- Read your Calendar and Details
- Read your Contacts
- Read contents of SD card
- Read phone status and identity

112. Network traffic tests were performed on the Zoom app in June of 2020, and much of the data sent was obfuscated, concealing the nature of what data was sent to Google. Other network traffic tests have confirmed that Zoom shares the Android AAID with Google.

113. Depending on the smartphone and operating system, it is sometimes possible for users to restrain some of these permissions, but the vast majority of users have no idea which specific permissions are allowed by default.

114. By integrating the Facebook SDK and Google Firebase Analytics SDK into the Zoom app, Zoom shared Plaintiffs' personal information with third parties including at a minimum, Facebook and Google.

Data Is the New Oil

115. Data harvesting is the fastest growing industry in the entire country. As software, data mining, and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

116. Consumer data is so valuable that some have proclaimed that data is the new oil.[28] Between 2016 and 2018, the value of information mined from Americans increased by 85% for Facebook and 40% for Google. Overall, the value internet companies derive from Americans' personal data increased almost 54%. Conservative estimates suggest that in 2018, internet companies earned $202 per American user. In 2022, that value is expected to be $200 billion industry wide, or $434 per user, also a conservative estimate.[29]

117. The behavioral data within apps described above is particularly valuable because behavioral advertising in its currently dominant form is driven by a range of invisible tracking technologies, like cookies, device fingerprinting and SDKs, using a variety of techniques, including cross- device tracking and identity matching. Privacy International is greatly concerned about the manifold ways in which people's data is exploited in these hidden back-end systems.[30] Both Google and Facebook are like other ad companies that try to collect a lot of data about what consumers do online. The crucial difference, however, is that their purview is especially broad. The fact that they are able to know the details and entire extent of a user's activity on Zoom clearly demonstrates this.

118. Location data is also extremely valuable. Not only is it typical for Google and Facebook to receive precise location data from apps, Zoom itself has collected location

---

[28] *The World's Most Valuable Resource Is No Longer Oil, But Data*, The Economist (May 6, 2017), available at <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (Last Visited July 29, 2020).

[29] R Shapiro, *What Your Data Is Really Worth to Facebook*, Washington Monthly (July/Aug. 2019), available at <https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-facebook/> (Last Visited July 29, 2020); *see also* R Shapiro & A Siddhartha, *Who owns American's Personal Information and What is it Worth?*, available at <https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf> (Last Visited July 29, 2020).

[30] Privacy International, *How Apps on Android Share Data with Facebook (even if you don't have a Facebook Account),* December 2018, available at <https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20 Data%20 with%20Facebook%20-%20Privacy%20International%202018.pdf> (Last Visited October 27, 2020).

data and saved it on its own servers. Companies that collect user location data are able to sell, use or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior. It's a hot market, with sales of location-targeted advertising reaching an estimated $21 billion this year.[31] The mobile location industry began as a way to customize apps and target ads for nearby businesses, but it has morphed into a data collection and analysis machine.

119. The value of data is probably most evident from the transaction that occurs on millions of apps in the mobile internet environment. The availability of Facebook and Google's software is not a community service. Google and Facebook provide their perfected software packages that have required immense capital to develop in exchange for data extracted from implementation of their SDKs in apps. The ability to reuse this well-tested and well-maintained code in Facebook and Google's software allows developers to reduce development costs and time. The ubiquitous nature of smartphones and their capacity to access sensitive and behavioral data, along with the innovations enabled by the Big Data revolution, gives SDK providers easy access to an unprecedented volume of high-quality data thanks to developers like Zoom integrating their components in millions of apps.

120. Both Facebook and Google are established personal data brokers. Data is monetized through targeted advertising. Facebook's ability to sell targeted messaging to its user population now drives its revenues and share price. But beyond profiting from direct advertising, both Facebook and Google also enter into data sharing/selling partnerships with various companies and apps where the entire basis of the deal is around the value of data extracted from apps like Zoom. Facebook in particular engineered its SDKs and APIs to facilitate the collection of data for app developers and for its business partners like Apple, Samsung, Amazon and other third parties.

[31] *See* <https://shop.biakelsey.com/product/2018-u-s-local-mobile-local-social-ad-forecast> (Last Visited October 27, 2020).

121. Facebook's partnerships with third parties, including device makers and its app developers, have formed a large part of its data-brokerage strategy. These partnerships allow Facebook to pool and aggregate information about billions of people for the purpose of targeting them with content. By engaging in partnerships with third party app developers, mobile devices makers, software makers, security firms, and even the chip designer Qualcomm, Facebook leveraged its position as a curator of user content and information.

122. For example, data sharing partners of Facebook such as cellular network carriers and device designers use this data to assess their standing against competitors, including customers lost to and won from those competitors.

123. In 2018, Facebook introduced "Actionable Insights," a corporate data sharing program including operators, carriers, internet service providers, and device makers to "enable better business decisions" through "analytics tools." It's exactly this sort of quasi-transactional data access that has become a hallmark of Facebook's business, allowing the company to plausibly deny that it ever sells data while still leveraging it for revenue.

124. Facebook itself also has an interest in technical information collected about devices that goes beyond social media. Since 2013, Facebook has been working towards establishing itself as a network service provider through efforts such as Facebook Connectivity and Fiber. Facebook now offers high capacity fiber-optic routes to sell unused capacity between its data centers to third parties.

125. It's no secret that Facebook also seeks to become a frontrunner in the videoconferencing sector. On July 23, 2020, Facebook announced that it is "launching its own Zoom competitor."[32] Technical device and performance information collected by the SDK is quite valuable to Facebook's efforts in this regard. "The Video Engineering team at Facebook is responsible for the end-to-end video experience, including upload, encoding, playback, and distribution across mobile and web. From backend infrastructure like

[32] Alison Durkee, *Facebook Is Launching Its Own Zoom Competitor*, Forbes (July 23, 2020), available at <https://www.forbes.com/sites/alisondurkee/2020/07/23/facebook-is-launching-its-own-zoom-competitor/#4be9bdfe2495> (Last Visited July 29, 2020).

networking and storage to the software that supports product development, our work focuses on developing systems to deliver a world-class video experience at scale on all platforms."[33]

Data Mining Through Third Party Applications

126. Zoom cooperates with developers of third-party applications to allow those applications to work with the Zoom platform. *See, e.g.*, <https://marketplace.zoom.us> (last visited May 12, 2021). In many instances, the Zoom app will share users' data with these applications.

127. Zoom explicitly misleads customers and consumers into believing their information is secure on Zoom's platform. As described by one Zoom developer in a July 2019 Medium post, "more importantly, users needed to trust these apps. Because our customers use these apps, we developed a rigorous process around security-focused testing and validation. For example, we prevent apps from pulling customer or end-user data without explicit consent and approval."[34] This was not the case.

128. As with the data gathered through the Facebook SDK, the names and email address of meeting participants is valuable in and of itself. However, when paired with other profiles, *e.g.*, those maintained by LinkedIn, the data has extraordinary value for all sorts of commercial and illegitimate purposes.

129. Zoom's data sharing is not limited to Facebook and Google. According to BuiltWith, upon information and belief, Zoom also sends personal data about their users to hotjar, Zendesk, AdRoll, Bing, and others.

130. Zoom maintains what it describes as "marketing" websites, *e.g.*, zoom.us and zoom.com, where its Privacy Policy is available. Zoom's privacy policies have had three

[33] *See* <https://engineering.fb.com/category/video-engineering/> (Last Visited July 29, 2020).

[34] Tim Sagle, *Zoom App Marketplace — What We Learned and Where We're Going* (July 23, 2019), available at <https://medium.com/zoom-developer-blog/zoom-app-marketplace-what-we-learned-and-where-were-going-9e15882794ca> (Last Visited July 28, 2020).

iterations that were complete overhauls of its previous versions: pre-March 29, 2020 policy, post-March 29, 2020 policy, and post July 2020 policy.

131. Prior to March 29, 2020, Zoom's Privacy Policy stated:

> **Collection of your Personal Data**
>
> Whether you have Zoom account or not, we may collect Personal Data from or about you when you use or otherwise interact with our Products. We may gather the following categories of Personal Data about you:
>
> - Information commonly used to identify you, such as your name, user name, physical address, email address, phone numbers, and other similar identifiers
> - Information about your job, such as your title and employer
> - Credit/debit card or other payment information
> - Facebook profile information (when you use Facebook to log-in to our Products or to create an account for our Products)
> - General information about your product and service preferences
> - Information about your device, network, and internet connection, such as your IP address(es), MAC address, other device ID (UDID), device type, operating system type and version, and client version
> - Information about your usage of or other interaction with our Products ("Usage Information")
> - Other information you upload, provide, or create while using the service ("Customer Content"), as further detailed in the "Customer Content" section below[35]

132. Zoom's pre-March 29, 2020 Privacy Policy continues:[36]

> Mostly, we gather Personal Data directly from you, directly from your devices, or directly from someone who communicates with you using Zoom services, such as a meeting host, participant, or caller. Some of our collection happens on an automated basis – that is, it's automatically collected when you interact with our Products.

[35] Zoom Privacy Policy (February 23, 2020) accessed via the Internet Archive Wayback Machine, available at <https://web.archive.org/web/20200311205042/https://zoom.us/privacy?zcid=1231> (Last Visited July 28, 2020) ("Zoom Privacy Policy (February 23, 2020)").

[36] *Id.*

133. Finally, Zoom's pre-March 29, 2020 Privacy Policy states: "We may also obtain information about you from a user who uses Zoom."[37]

134. On March 29, 2020, Zoom's Chief Legal Officer, Aparna Bawa, released a statement that: "We are not changing any of our practices. We are updating our privacy policy to be more clear, explicit, and transparent."[38] This statement linked to a broadly revised Zoom Privacy Policy that included both more and less clarity but it still asserted that "[t]he categories of data we obtain when you use Zoom include data you provide to us as well as data that our system collects from you" and that "'You' or 'user' or 'participant' is anyone who uses Zoom" regardless of whether they have an account.[39]

135. In July 2020, Zoom again completely revised its privacy policy to include a chart of data usage which would be indecipherable to the average Zoom user. Language used to describe the type of data, and Zoom's intended use of that data, only raises more questions. For instance Zoom states that, "Automatically through use of the Service," it collects "Operation Data" which includes:[40]

- Configuration Data: information about the deployment of Zoom Services and related environment information.
- Meeting metadata: metrics about when and how meetings were conducted.
- Feature Usage Data: information about if and how Service features were used.
- Performance Data: metrics related to how the Services perform.
- Service Logs: information on system events and states.

---

[37] *Id.*

[38] Aparna Bawa, *Zoom's Privacy Policy* (March 29, 2020), available at <https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/> (Last Visited July 28, 2020).

[39] Zoom Privacy Policy (March 29, 2020) accessed via the Internet Archive Wayback Machine, available at <https://web.archive.org/web/20200331032821/ https://zoom.us/privacy?zcid=1231> (Last Visited July 28, 2020) ("Zoom Privacy Policy (March 29, 2020)").

[40] Zoom Privacy Policy (July 2020), available at <https://zoom.us/privacy> (Last Visited July 28, 2020) ("Zoom Privacy Policy (July 2020)").

136. Zoom's July 2020 privacy policy chart continues that any of these broad categories of "Operation Data" can be used to, among other things, "Create anonymized and/or aggregated data to improve our products and *for other lawful business purposes*"[41] (emphasis added). There is no further explanation of what Zoom considers a "lawful business purpose" or how a user is to understand this exception that swallows the preceding limitations to data usage Zoom outlines.

137. Zoom's March 29, 2020 privacy policy revealed that personal data collected from users included, but was not limited to: information that identifies you (name, username and email address, or phone number); technical information about your devices, network, and internet connection (IP address, MAC address, other device ID (UDID), device type, operating system type and version, client version, type of camera, microphone or speakers, connection type); approximate location; and other forms of metadata.[42] The July 2020 privacy policy chart both removed much of these details and revealed that Zoom has access to an additional range of information that includes billing information, employer information, and marketing data.[43]

138. The July 2020 included a disclosure at the bottom asserting that in revising Zoom's privacy policy on March 29, 2020, and again in July 2020: "We did not change or add any data practices, only how we described them."[44]

139. Accordingly, Zoom stands by its prior representation in its March 29, 2020 privacy policy that: "We do not allow marketing companies, advertisers or similar companies to access personal data in exchange for payment. We do not allow third parties to use any

[41] *Id.*

[42] Zoom Privacy Policy (March 29, 2020).

[43] Zoom Privacy Policy (July 2020).

[44] *Id.*

personal data obtained from us for their own purposes, unless you consent (e.g., when you download an app from the Marketplace)."[45]

140. Zoom's revised July 2020 privacy policy also states that: "Zoom is committed to protecting your personal data. We use reasonable and appropriate technical and organizational measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data."[46]

141. Plaintiffs are informed and believe that Zoom has not complied with its own Privacy Policy by, among other things, sharing personal data from people engaging with its products to third parties, including but not limited to Facebook.

142. Zoom users who have not been notified by Zoom's March 27, 2020 statement that its iPhone app was providing users' personal data to Facebook, and have thus not updated to the newer version of the Zoom iPhone app, continue to have their information released to Facebook.

143. Furthermore, many Zoom users would never have known of Zoom's policies on collection and dissemination of users' personal data. Zoom's disclosure of its Privacy Policy—and its collection and dissemination to third parties of users' personal data—is only available through a small link on Zoom's marketing page. Zoom users who opened an account prior to July 2020 would not have encountered the updated Privacy Policy by simply opening the Zoom app on their desktop or mobile device. Zoom users who have not opened a Zoom account have never been provided the Zoom Privacy Policy, nor is it likely they have ever even seen the Zoom marketing page since these users are automatically placed in a Zoom meeting after clicking the provided URL.

144. While Zoom continues to represent that it "takes its users' privacy extremely seriously" and that its "customers' privacy is incredibly important to" it, Zoom's actions

[45] Zoom Privacy Policy (March 29, 2020).

[46] Zoom Privacy Policy (July 2020).

demonstrate otherwise.[47] Zoom has attempted to sidestep liability by offering an update to its Zoom iPhone app through a blog post on its website without affirmatively contacting current users, or requiring users to update their Zoom iPhone app, and by revising its Privacy Policy to further obscure that users without accounts are having their data collected by Zoom and shared with third parties.

145. Had Zoom informed its accountholders that it would not engage in a thorough review of the third parties with whom its Zoom iPhone app shared personal data, *e.g.*, Facebook, Google, and other Zoom users, it is likely that customers—like Plaintiffs and Class members—would not have been willing to purchase its services at the price charged, or even to have used those services at all, regardless of price.

146. Furthermore, it has been well documented by privacy researchers that when people are fully informed on collection of their information, people dislike these practices, and would stop using these services if they were full informed and understood the extent of the data collection. If invasive surveillance is the price of using free services, people would rather pay or at least be completely informed as to the extent, with whom, and how their personal information and granular details of their behavior and activity is used. Companies understand consumers' distaste for being tracked, and use a form of coercion to ensure participation. This is especially true in the case of Zoom where most users are required to use the service by virtue of where they attend school, volunteer, or are employed. Zoom uses this to its advantage and the customer has no free choice or negotiating power in the exchange.

147. Zoom's failure to implement adequate security protocols or app review procedures jeopardized millions of consumers' privacy, fell well short of its promises, and diminished the value of the products and services provided. In other words, because Defendant failed to disclose its gross security inadequacies, and affirmatively shared users'

[47] Eric S. Yuan, *Zoom's Use of Facebook's SDK in iOS Client* (March 27, 2020), available at <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/> (Last Visited July 28, 2020).

information with third parties without their informed consent, it delivered fundamentally less useful and less valuable products and services than those for which consumers like Plaintiffs paid and/or expected when they chose to use them.[48]

148. While Zoom's wrongful conduct constitutes invasion of privacy in and of itself, entitling consumers to damages, Plaintiffs and Class members also now are placed at an increased risk of further imminent harm as a direct result of Zoom's wrongful acts and omissions. Indeed, a recent report revealed that account information belonging to over half a million Zoom users was published, exchanged and, in some cases, sold online without their knowledge or consent.[49] No doubt this is a result of the aforementioned wrongful conduct by Zoom.

149. Finally, the unauthorized access to Plaintiffs' and Class members' private and personal data also has diminished the value of that information resulting in the above described harm to its users.

Unauthorized Interception and Use of Video Sessions, Chats, and Transcripts

150. Zoom's pre-March 29, 2020 privacy policy provides that, regardless of whether the consumer has a "Zoom account or not, we may collect Personal Data from or about you when you use or otherwise interact with our Products," including "information you upload, provide, or create while using the service ('Customer Content'), as further

[48] Zoom has admitted to further security issues related to its products including: "Zoombombing"—incidents of harassment by unauthorized participants in a Zoom meeting; failure of Zoom to implement promised end-to-end encryption; privacy issues related to attendee tracking features; data disclosures to LinkedIn; etc. *See* Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[49] Lawrence Abrams, *Over 500,000 Zoom Accounts Sold On Hacker Forums, the Dark Web* (April 13, 2020), available at <https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/> (Last Visited July 28, 2020).

detailed in the 'Customer Content' section below."[50] In the later section, the policy provides "Customer Content is information provided by the customer to Zoom through the usage of the service. Customer Content includes the content contained in **cloud recordings, and instant messages, files, whiteboards, and shared while using the service**."[51] Under a heading entitled "More about meeting recordings" the policy states: "If you participate in a Recorded Meeting or you subscribe to Zoom cloud recording services, we collect information from you in connection with and through such Recordings. This information may include Personal Data."[52]

151. As of April 2, 2020, Zoom "removed the attendee attention tracker feature as part of our commitment to the security and privacy of our customers."[53] Prior to its removal, this surreptitious tracking feature gave presenters the ability to "track if participants . . . clicked away from the active Zoom window for more than half a minute."[54]

152. Consumer Reports has pointed out that Zoom provides meeting hosts with the ability "make a recording of the conference, have it transcribed automatically, and share the information with people who aren't at the meeting."[55] Under Zoom's privacy policy,

---

[50] Zoom Privacy Policy (February 23, 2020) accessed via the Internet Archive Wayback Machine, available at <https://web.archive.org/web/20200311205042/ https://zoom.us/privacy?zcid=1231> (Last Visited July 28, 2020) ("Zoom Privacy Policy (February 23, 2020)").

[51] *Id.*

[52] *Id.*

[53] <https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking> (last visited July 30, 2020); *see also* Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[54] Karl Bode, *Working From Home? Zoom Tells Your Boss If You're Not Paying Attention*, available at <https://www.vice.com/en_us/article/qjdnmm/working-from-home-zoom-tells-your-boss-if-youre-not-paying-attention> (Last Visited July 30, 2020).

[55] Allen St. John, *Zoom Calls Aren't as Private as You May Think*, CONSUMER REPORTS (March 30, 2020), available at <https://www.consumerreports.org/video-conferencing-services/zoom-teleconferencing-privacy-concerns/> (Last Visited July 29, 2020).

Zoom collects those video recordings and transcripts, as well as documents shared on the screen, and the name of everyone on a call.[56] Like other tech giants with access to large troves of live video recordings, Zoom has incredible incentive to access and view that video and audio content.[57]

153. There are reports of Zoom sending presenters meeting transcripts that include transcriptions of supposedly private chats conducted between meeting participants, sometimes without the presenter's participation, and sometimes including embarrassing, personal content that those participating in the chats surely would not have included had they known the chats would be recorded.[58]

154. Such video conference recordings are extremely helpful in the development of highly capable artificial intelligence ("AI"). AI systems are highly valuable to businesses because they automate away the need for human workers. Virtual assistants or "chatbots" are one example of an AI that has immense monetary value. One firm estimated that the chatbot market was valued at USD 17.17 billion in 2019 and is projected to reach 102.29 billion by 2025.[59] "A chatbot is basically an artificial intelligence-powered application that converses with a human being to solve a problem or to answer a certain query... According to Salesforce, 69% of consumers prefer to use chatbots for the speed at which they can communicate with a brand. [60]

155. The catch: to build an effective AI model, companies need vast amounts of

[56] *See id.*

[57] Thomas Germain and Daniel Wroclawski, *Do Tech Companies Watch Your Home Security Camera Footage?*, Consumer Reports (October 22, 2019), available at <https://www.consumerreports.org/home-security-cameras/do-tech-companies-watch-your-home-security-camera-footage/?EXTKEY=AFLIP> (Last Visited July 29, 2020).

[58] *See, e.g.*, Danny M. Lavery, *I Saw My Co-Workers' Private DMs Mocking My Weight*, SLATE (April 25, 2020), available at <https://slate.com/human-interest/2020/04/dear-prudence-coworkers-private-dm-zoom-mocking-weight.html> (Last Visited July 30, 2020).

[59] *See* <https://www.mordorintelligence.com/industry-reports/chatbot-market> (Last Visited July 29, 2020).

[60] *Id.*

data. The more data, the better and more "human-like" the AI.[61] OpenAI recently released GPT-3, currently a language AI so advanced, that it was able to code basic HTML script to produce a simple website:

> Others have found that GPT-3 can generate any kind of text, including guitar tabs or computer code. For example, by tweaking GPT-3 so that it produced HTML rather than natural language, web developer Sharif Shameem showed that he could make it create web-page layouts by giving it prompts like "a button that looks like a watermelon" or "large text in red that says WELCOME TO MY NEWSLETTER and a blue button that says Subscribe." Even legendary coder John Carmack, who pioneered 3D computer graphics in early video games like Doom and is now consulting CTO at Oculus VR, was unnerved: "The recent, almost accidental, discovery that GPT-3 can sort of write code does generate a slight shiver."[62]

156. The key to effective AI models is access to large data sets. Indeed, MIT Technology Review points out that GPT-3 "is the largest language model ever created."[63] "The model has 175 billion parameters (the values that a neural network tries to optimize during training), compared with GPT-2's already vast 1.5 billion. And with language models, size really does matter."[64] For example, Google used 341GB of social media

---

[61] Karen Hao, Facebook Claims Its New Chatbot Beats Google's As The Best In The World (April 29, 2020), available at <https://www.technologyreview.com/2020/04/29/1000795/facebook-ai-chatbot-blender-beats-google-meena/> (Last Visited July 29, 2020); Chris Knight, *How Much Data Do You Need To Train A Chatbot and Where To Find It?*, available at <https://chatbotslife.com/how-much-data-do-you-need-to-train-a-chatbot-and-where-to-find-it-d25a7b930e> (Last Visited July 29, 2020).

[62] Will Douglas Heaven, *OpenAI's New Language Generator GPT-3 Is Shockingly Good—And Completely Mindless,* MIT Technology Review (July 20, 2020), available at < https://www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/> (Last Visited July 29, 2020).

[63] *Id.*

[64] *Id.*

conversation data to train its chatbot "Meena," which has only 2.6 billion parameters.[65]

157. "The requirement for upgrading AI systems is more and more data, and more and more diverse data," according to Anil Jain, a professor at Michigan State University.[66] Zoom has access to the authentic and unscripted dialogue of millions of humans around the world, speaking in various languages, on diverse topics, with various levels of intimacy and formality—a veritable goldmine. A chatbot trained on transcripts of conversation between travel agents can be used to answer the questions of consumers who visit a travel website. A chatbot trained on conversations between students and teachers can become a more natural language sounding teaching tool.

158. The problem: training AI using Zoom's recorded content would invade the privacy of Zoom users. To train AI systems, according to Professor Jain, "human workers have to manually review and annotate recordings or other information. There's always a human touch involved at some point."[67] And not just humans—the AI itself will read the consumer data while being trained, and can be prompted to share that private consumer information with others. A collaboration between researchers at Google Brain, Berkeley, and the University of Singapore showed that the AI can spit back the personally identifiable information of a single data point which was intentionally placed in a large database:

---

[65] Daniel Adiwardana et al., Towards a Human-like Open-Domain Chatbot, available at <https://arxiv.org/pdf/2001.09977.pdf> (Last Visited July 29, 2020); Chris Knight, *How Much Data Do You Need To Train A Chatbot and Where To Find It?*, available at <https://chatbotslife.com/how-much-data-do-you-need-to-train-a-chatbot-and-where-to-find-it-d25a7b930e> (Last Visited July 29, 2020).

[66] Thomas Germain and Daniel Wroclawski, *Do Tech Companies Watch Your Home Security Camera Footage?*, Consumer Reports (October 22, 2019), available at < https://www.consumerreports.org/home-security-cameras/do-tech-companies-watch-your-home-security-camera-footage/?EXTKEY=AFLIP> (Last Visited July 29, 2020).

[67] Thomas Germain and Daniel Wroclawski, *Do Tech Companies Watch Your Home Security Camera Footage?*, Consumer Reports (October 22, 2019), available at < https://www.consumerreports.org/home-security-cameras/do-tech-companies-watch-your-home-security-camera-footage/?EXTKEY=AFLIP (Last Visited July 29, 2020).

> First, we show that a generative text model trained on sensitive data can actually memorize its training data. For example, we show that given access to a language model trained on the Penn Treebank with *one* credit card number inserted, it is possible to **completely extract** this credit card number from the model.[68]

159. Both the audio and visual content of zoom users' recordings are extremely valuable in the creation of AI, and Zoom may be accessing and viewing consumers' video recordings without the users' consent or knowledge for such purposes.[69]

Misrepresentations Regarding End-to-End Encryption

160. End-to-end encryption ("E2E") is a system of communication where only the communicating users can read the messages.

161. Increasingly, E2E encryption is becoming an industry standard expectation for communication technology. Facebook announced in March 2019 that it would move all three of its messaging platforms (including WhatsApp) to E2E encryption. Similarly, Apple says of its data security: "iCloud is built with industry-standard security technologies, employs strict policies to protect your information, and is leading the industry by adopting privacy-preserving technologies like end-to-end encryption for your data."

162. Competitor platforms Webex and GoToMeeting both either automatically utilize E2E encryption or offer hosts the option of E2E encryption as part of their standard

---

[68] Nicholas Carlini, *Evaluating and Testing Unintended Memorization in Neural Networks* (Aug. 13, 2019), available at <https://bair.berkeley.edu/blog/2019/08/13/memorization/> (Last Visited July 29, 2020); Nicholas Carlini, *The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks* (July 16, 2019), available at <https://arxiv.org/pdf/1802.08232.pdf> (Last Visited July 29, 2020).

[69] Blair Hanley Frank, *Zoom Uses AI to ADD Automatic Transcription to Its Videoconferencing Service* (Sept. 26, 2017), available at <https://venturebeat.com/2017/09/26/zoom-uses-ai-to-add-automatic-transcription-to-its-videoconferencing-service/> (Last Visited July 30, 2020); John Porter, *This Tool Automatically Transcribes Your Zoom Meetings as They Happen* (April 23, 2020), available at <https://www.theverge.com/2020/4/23/21232385/otter-ai-live-video-meeting-notes-zoom-transcription-annotation-teams> (Last Visited July 30, 2020).

platform.

163. As a result, Zoom is and has been aware that E2E encryption is a valuable service that consumers will both pay for and have increasingly come to expect as part of their online communication choices. In a recent blog post announcing that Zoom will begin testing E2E encryption, Zoom's chief information security officer Jason Lee said end-to-end encryption was a "highly requested feature from our customers, and we're excited to make this a reality."[70]

164. With this in mind, Zoom has explicitly represented that it had E2E encryption functionality at least as early as 2019. For example, Zoom made representations that it "exceeds a high standard for data privacy and protection," "is certified and compliant with the EU-U.S. Privacy Shield Framework," as well as utilizing "end-to-end-encryption for desktop and mobile devices."[71]

165. Similarly, Zoom's own website prominently featured, on the "Security at Zoom" page, the statement that:

> We take security seriously and we are proud to exceed industry standards when it comes to your organization's communications
> . . . .
> The following in-meeting security capabilities are available to the meeting host:
> - Secure a meeting with end-to-end encryption
>
> . . .
> Zoom's solution and security architecture provides end-to-end encryption and meeting access controls so data in transit cannot be intercepted.[72]

166. Zoom also prominently linked to a "Security Whitepaper" on its "Security at

---

[70] *See* <https://techcrunch.com/2020/10/27/zoom-launches-end-to-end-encryption-for-free-meetings-with-a-catch/> (Last Visited October 28, 2020).

[71] *Zoom Executive Summary*, available at <https://www.neha.org/sites/default/files/Zoom%20Executive%20Summary%202019.pdf >, at 10 (Last Visited July 28, 2020).

[72] Security at Zoom, (March 22, 2020), accessed via the Internet Archive Wayback Machine, available at <http://web.archive.org/web/20200322145328/ https://zoom.us/security> (Last Visited July 28, 2020).

Zoom" page which repeated these false claims regarding E2E encryption.[73]

167. Additionally, during Zoom videoconferences, hovering your cursor over the green lock at the top left corner of the application would show the text "Zoom is using an end to end encrypted connection." Zoom has since changed this text to simply say that the session is encrypted.

168. On March 31, 2020, The Intercept published an article revealing that Zoom video conferences, and Zoom's other audio and video functionality, did not in fact support E2E encryption.[74]

169. Zoom thereafter updated its encryption to the industry-standard AES-GCM with 256-bit keys. But the encryption keys for each meeting are generated by Zoom's servers, not by the client devices. 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 a web browser and a website 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. In a Zoom meeting utilizing this encryption technology, the video and audio content will stay private from anyone spying on Wi-Fi, but will not stay private from the company or, presumably, anyone with whom the company shares its access voluntarily, by compulsion of law (*e.g.*, at the request of law enforcement), or involuntarily (*e.g.*, a hacker who can infiltrate the company's systems). With true E2E encryption, the encryption keys are generated by the client (customer) devices, and only the participants in the meeting have the ability to decrypt it.[75]

170. Matthew Green, a cryptographer and computer science professor at Johns

[73] Zoom Security Guide, (March 31, 2020), accessed via the Internet Archive Wayback Machine, available at <http://web.archive.org/web/20200331082306/https://zoom.us/docs/doc/Zoom-Security-WhitePaper.pdf> (Last Visited July 28, 2020).

[74] Micah Lee and Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading* (March 31, 2020), <https://theintercept.com/2020/03/31/zoom-meeting-encryption/> (Last Visited July 28, 2020).

[75] *Id.*

Hopkins University, points out that group video conferencing is difficult to encrypt end-to-end. That's because the service provider—in this case Zoom—needs to detect who is talking to act like a switchboard, in order to send a high-resolution videostream from the person who is talking at the moment, and low-resolution videostreams of other participants. This type of optimization is much easier if the service provider can see everything because it's unencrypted, but it is possible. Apple FaceTime, for example, utilizes E2E encryption.[76]

171. Zoom's own response on April 1, 2020 (the day after The Intercept's article) made it clear that Zoom both knew that it did not use the industry-accepted definition of E2E encryption and had made a conscious decision to use the term "end-to-end" anyway.[77]

172. This is particularly egregious in light of Zoom's representations regarding compliance with the Health Insurance Portability and Accountability Act ("HIPAA"). Zoom has encouraged patients and health care professionals to use its videoconferencing services for private and sensitive medical appointments.[78] Any person doing so would assume that no-one but the doctor and patient were capable of viewing such a conversation. As is apparent from the above explanation, however, Zoom itself (and anyone who knowingly or unknowingly gained access to Zoom's system) can view those videoconferences.

173. This misrepresentation is a particularly egregious violation of public trust because of the very high level of privacy people have in their personal, private, and intimate communications.

"Zoombombing"

174. Further failures of Zoom's security procedures have arisen with a troubling

[76] *Id.*

[77] Oded Gal, *The Facts Around Zoom and Encryption for Meetings/Webinars* (Apr. 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/> (Last Visited July 28, 2020).

[78] *See, e.g.*, Zoom, *HIPAA Compliance Guide*, available at <https://zoom.us/ docs/doc/ Zoom-hipaa.pdf> (Last Visited July 28, 2020); <https://marketplace.zoom.us/ apps?category=health_care> (describing healthcare app partners) (Last Visited July 28, 2020).

phenomenon referred to as "Zoombombing." Zoombombing involves unauthorized participants entering Zoom meetings to disrupt them. Following the issuance of local and state stay-at-home orders, schools, churches, synagogues, mosques, support groups, and medical providers have all moved their meetings online using Zoom's video conferencing service to connect students, teachers, parishioners, participants and patients.

175. Just as schools, businesses, support groups, and religious institutions and millions of individuals have adopted Zoom as a meeting platform in an increasingly remote world, reports of Zoombombing by uninvited participants have become frequent.[79]

176. On April 3, 2020, the New York Times reported that "While those incidents may have initially been regarded as pranks or trolling, they have since risen to the level of hate speech and harassment, and even commanded the attention of the F.B.I."[80]

177. An analysis by The New York Times found "153 Instagram accounts, dozens of Twitter accounts and private chats, and several active message boards on Reddit and 4Chan where thousands of people had gathered to organize Zoom harassment campaigns, sharing meeting passwords and plans for sowing chaos in public and private meetings."[81]

178. As early as March 20, 2020, Zoom admitted its product had an issue with Zoombombing.[82] Rather than change security protocols and default features, however, Zoom turned its back on its users, asserting they were to blame through their inability to properly use the program.

---

[79] Taylor Lorenz and Davey Alba, *'Zoombombing' Becomes a Dangerous Organized Effort,* New York Times (April 3, 2020), available at <https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html> (Last Visited July 28, 2020).

[80] *Id.*

[81] *Id.*

[82] *How to Keep Uninvited Guests Out of Your Zoom Event* (March 20, 2020), available at <https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/> (Last Visited July 28, 2020).

179. Nevertheless, bad actors have disrupted private moments as diverse as Alcoholics Anonymous meetings to Holocaust memorial services.[83] School classes and religious services all over the world have been affected. Recordings of these incidents and others end up on YouTube and TikTok.[84] Concerns regarding Zoombombing led many organizations to ban employee use, including Google, SpaceX, NASA, the Australian Defence Force, the Taiwanese and Canadian governments, the New York Department of Education, and the Clark County School District in Nevada.[85]

180. The Zoombombing incidents experienced by Saint Paulus and Oak Life Church and their church members were consistent with those experienced by others across the country. Both incidents involved offenders that were "known" to Zoom but as to whom Zoom failed to take any action. Both incidents caused irreparable harm to already-vulnerable communities, requiring trauma counselling and emotional support groups in case of Oak Life Church, and were so severe as to require them to be reported to law enforcement, including the FBI.

181. Zoom could have, but did not provide adequate meeting security to limit or prevent altogether such Zoombombing instances or unauthorized meeting access and intrusions.

182. While the experiences of Zoombombing were in many cases horrific, Zoom's failure to provide a safe and private platform is serious and disruptive regardless of content.

183. Zoom also could have implemented various other relatively simple technical solutions to limit or prevent altogether such Zoombombing attacks, for instance making it easier to allow hosts to cancel a meeting and/or eject a Zoombomber with the push of a single button, screen sharing control defaults, or implementing stronger meeting security

---

[83] Sebastien Meineck, *'Zoom Bombers' Are Still Blasting Private Meetings With Disturbing and Graphic Content* (June 10, 2020), available at <https://www.vice.com/en_us/article/ m7je5y /zoom-bombers-private-calls-disturbing-content> (Last Visited July 28, 2020).

[84] *Id.*

[85] *Id.*

(attendee admission) protocols such as identity verification or unique meeting passcodes.

184. Given these incidents, Zoom's representations that it "takes its users' privacy extremely seriously" and that its "customers' privacy is incredibly important to" it cannot be taken at face value. To date Zoom has marketed itself to institutions and to the pubic under the false premise that its Zoom meetings are secure. If they were secure, Zoom participants would not be subjected to racial slurs and other abusive behavior by Zoombombers.

185. Had Zoom informed its users that it would not engage in a thorough review of its security protocols, or that it would create default settings or other security holes that could be exploited by malicious actors, customers—like Plaintiffs and Class members—would not have been willing to purchase its services at the price charged, or even to use those services at all, regardless of price.

186. Zoom's failure to implement adequate security protocols jeopardized millions of consumers' privacy, fell well short of its promises, and diminished the value of the products and services provided. In other words, because Defendant failed to disclose its gross security inadequacies, and exposed users to malicious third parties' harassment, without their informed consent, it delivered fundamentally less useful and less valuable products and services than those for which consumers like Plaintiffs paid and/or expected when they chose to use Zoom's services.

187. While Zoom's wrongful conduct constitutes invasion of privacy in and of itself, entitling consumers to damages, Plaintiffs and Class members are also now placed at an increased risk of further imminent harm as a direct result of Zoom's wrongful acts and omissions.

THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT RULE

188. Congress enacted the Children's Online Privacy and Protection Act ("COPPA") in 1998 to protect the safety and privacy of children online by prohibiting the unauthorized or unnecessary collection of children's personal information online by operators of Internet Web sites and online services. COPPA directed the Federal Trade

Commission to promulgate a rule implementing COPPA, 16 C.F.R. Part 312 ("COPPA Rule").

189. The COPPA Rule applies to any operator of a commercial Web site or online service directed to children that collects, uses, and/or discloses personal information from children, or on whose behalf such information is collected or maintained, and to any operator of a commercial website or online service that has actual knowledge that it collects, uses, and/or discloses personal information from children. Defendant Zoom specifically advertises its video conferencing service to schools and children.

190. The COPPA Rule defines "personal information" to include, among other things, a first and last name; a home or other physical address including street name and name of a city or town; online contact information (*i.e.*, an email address or other substantially similar identifier that permits direct contact with a person online, such as an instant messaging user identifiers, screen name, or user name); a persistent identifier such as an IP address that can be used to recognize a user over time and across different Web sites or online services; a photograph, video, or audio file where such file contains a child's image or voice; or information concerning the child or parents of that child that the operator collects online from the child and combines with an identifier described in this definition. Through its video conferencing services, Defendant collected personal information as defined in the COPPA Rule, including children's names, addresses, IP addresses, and photographs and audio files containing a child's image or voice. Defendant also collected information from the child concerning the child that was combined with other identifiers, such as the name or photograph of the child.

191. Because Defendant collects and maintains personal information from its users through its video conferencing services, Defendant is an operator as defined by the COPPA Rule, 16 C.F.R. § 312 *et seq.*.

192. Among other things, the Rule requires that an operator of a child-directed website or online service meet specific requirements prior to collecting online, using, or disclosing personal information from children, including but not limited to:

a. posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what information it collects from children, how it uses such information, and its disclosure practices for such information, and other specific disclosures set forth in the Rule;

b. providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents;

c. obtaining verifiable parental consent prior to collecting, using, and/or disclosing personal information from children; and

d. establishing and maintaining reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

193. Defendant has failed to comply with each of these requirements as outlined in the failures and events described above, including but not limited to, Defendant's failure to properly post its privacy policy, failing to properly provide its information practices, failing to properly obtain parental consent, and failing to establish and maintain reasonable practices to protect personal information and prevent unauthorized access to video conferences.

CLASS ALLEGATIONS

194. Plaintiffs bring this class action lawsuit individually and on behalf of the proposed Class under Rule 23 of the Federal Rules of Civil Procedure.

195. Plaintiffs seek certification of a Nationwide Class and an Under 13 Sub-Class (collectively, the "Classes") defined as follows:

> Nationwide Class: All persons in the United States who used Zoom.

196. In the alternative, Plaintiffs seek certification of the following nationwide class of children under the age of 13:

> Under 13 Sub-Class: All persons under the age of 13 in the United States who used Zoom.

197. Specifically excluded from the Classes are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, members of the judge's staff, and the judge's immediate family.

198. The Classes meet the requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the following reasons.

199. **Numerosity:** Although the exact number of Class members is uncertain, and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable, believed to amount to many thousands or millions of persons. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and the Court. Information concerning the exact size of the putative class is within the possession of Defendant. The parties will be able to identify each member of the Classes after Defendant's document production and/or related discovery.

200. **Commonality:** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant collected Plaintiffs' and Class members' personal data;

c. Whether Defendant provided Plaintiffs' personal data to third parties;

d. Whether Defendant adequately disclosed its policy of providing personal data to third parties;

e. Whether Defendant's collection and storage of Plaintiffs' and Class and members' personal data in the manner alleged violated federal, state and local laws, or industry standards;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by providing personal data to third parties;

g. Whether Defendant violated the consumer protection and privacy statutes applicable to Plaintiffs and members of the Class;

h. Whether Defendant acted negligently in failing to properly safeguard Plaintiffs' and Class members' personal data;

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

j. The nature of the relief, including equitable relief, to which Plaintiffs and Class members are entitled.

201. **Typicality:** Plaintiffs' claims are typical of the claims of other Class members. Plaintiffs and other Class members were injured through Defendant's uniform misconduct and their legal claims arise from the same core practices of Defendant.

202. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Classes, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Classes, and there are no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

203. **Risks:** The proposed action meets the requirements of Fed. R. Civ. P. 23 because prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant or would be dispositive of the interests of members of the proposed Classes. Furthermore, Defendant's database still exists, and Defendant may still be intentionally or inadvertently providing data to third parties – one standard of conduct is needed to ensure the future handling of Defendant's database.

204. **Injunctive Relief:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

205. **Predominance:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the Classes predominate over any questions that may affect only individual Class members in the proposed Classes.

206. **Superiority:** The proposed action also meets the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendant. Even if it were economically feasible, requiring thousands of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Plaintiffs anticipate no unusual difficulties in managing this class action.

207. **Certification of Particular Issues:** In the alternative, this action may be maintained as class action with respect to particular issues in accordance with Fed. R. Civ. P. 23(c)(4).

208. Finally, all members of the purposed Classes are readily ascertainable. Defendant has access to addresses and other contact information for members of the Classes, which can be used to identify Class members.

FIRST CAUSE OF ACTION
Invasion of Privacy in
Violation of California Common Law and the California Constitution, Art. 1, § 1
(*On Behalf of Plaintiffs and all Classes*)

209. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

210. Plaintiffs and Class members have a legally protected privacy interest in their private and personal information that is transferred to or recorded by Zoom, and are entitled to the protection of their property and information against unauthorized access.

211. Plaintiffs and Class members reasonably expected that their personal data would be protected and secure from unauthorized parties, and that their private and personal information would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

212. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class members by (a) failing to adequately secure their private and personal information from disclosure to unauthorized parties for improper purposes; (b) disclosing their private, and personal information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their private and personal information to unauthorized parties without the informed and clear consent of Plaintiffs and Class members, including but not limited to Zoom's unauthorized sharing of personal information with Facebook and Google, Zoom's failure to implement E2E encryption, and Zoom's failure to secure users' meetings against Zoombombings. This invasion into the privacy interest of Plaintiffs and Class members is serious and substantial.

213. In failing to adequately secure Plaintiffs' and Class members' personal information, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its substandard security measures would cause its users harm and, would be considered highly offensive to a reasonable person in the same position as Plaintiffs and Class members.

214. Defendant violated Plaintiffs' and Class members' right to privacy under California law, including, but not limited to California common law and Article 1, Section 1 of the California Constitution and the California Consumer Privacy Act.

215. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs' and Class members' private, personal, and confidential information has been accessed or is at imminent risk of being accessed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and proposed Class members have suffered injuries as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

216. Plaintiffs and Class members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(*On Behalf of Plaintiffs and all Classes*)

217. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

218. Defendant provided Zoom meetings to Plaintiffs and members of the Class. In exchange, Defendant received benefits in the form of monetary payments and/or other valuable consideration, *e.g.*, access to their private and personal data.

219. Defendant acknowledged these benefits and accepted or retained them.

220. In using Zoom meetings, Plaintiffs and Class members continually provide Defendant with their valuable private and personal information.

221. By providing that information, and upon Defendant's acceptance of that information, Plaintiffs and Class members, on the one hand, and Defendant, on the other, entered into implied contracts, separate and apart from Zoom's terms of service, under which Defendant agreed to and was obligated to take reasonable steps to secure and safeguard that sensitive information.

222. All parties understood that such security was integral and essential to Defendant's entire line of business—secure video conferencing services.

223. Under those implied contracts, Defendant was obligated to provide Plaintiffs and Class members with Zoom meetings that were suitable for their intended purpose of providing secure video conferencing services, rather than other video conferencing services vulnerable to unauthorized access, incapable of providing safety and security, and instead actually utilized to track its users' personal data for commercial purposes.

224. Without such implied contracts, Plaintiffs and Class members would not have used Zoom meetings and would not have conferred benefits on Defendant, but rather would have chosen alternative video conferencing services that did not present these privacy and safety risks.

225. Plaintiffs and Class members fully performed their obligations under these implied contracts.

226. As described throughout, Defendant did not take reasonable steps to

safeguard Plaintiffs' and Class members' private information. In fact, Defendant willfully violated those privacy interests by tracking and disclosing its customers' personal data to third parties without consent.

227. Because Defendant failed to take reasonable steps to safeguard Plaintiffs' private information, Defendant breached its implied contracts with Plaintiffs and Class members.

228. Defendant's failure to fulfill its obligation to safeguard Plaintiffs' and Class members' private information resulted in Plaintiffs and Class members receiving video conferencing services that were of less value than they provided consideration for (*i.e.*, unsecure video conferencing services without adequate security).

229. Stated otherwise, because Plaintiffs and Class members provided valuable consideration for secure video conferences and privacy protections they did not receive—even though such protections were a material part, if not the very essence, of their contracts with Defendant—the full benefit of their bargain.

230. As a result of Defendant's conduct, Plaintiffs and members of the Class have suffered actual damages in an amount equal to the difference in the value of the video conferencing services they provided valuable consideration for and the unsecure video conferences they received.

231. Accordingly, Plaintiffs, on behalf of themselves and Class members, seeks an order declaring that Defendant's conduct constitutes breach of implied contract, and awarding them damages in an amount to be determined at trial.

THIRD CAUSE OF ACTION
Breach of Implied Covenant of Good Faith and Fair Dealing
(*On Behalf of Plaintiffs and all Classes*)

232. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

233. 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.

234. 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 Plaintiffs and other Class members; (b) refrain from disclosing, without authorization or consent, the personal information of Plaintiffs and other Class members to any third parties; (c) promptly and accurately notify Plaintiffs 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.

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

- disclosing Plaintiffs' and other Class members' personal information to unauthorized third parties, including Facebook and Google;
- allowing third parties to access the personal information of Plaintiffs and other Class members;
- failing to implement and maintain adequate security measures to safeguard users' personal information;
- failing to timely notify Plaintiffs 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.

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

FOURTH CAUSE OF ACTION
Unjust Enrichment/Quasi-Contract
(*On Behalf of Plaintiffs and all Classes*)

237. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

238. Defendant received a benefit from Plaintiffs and Class members in the form of payments and/or other valuable consideration including access to their private and personal data, in exchange for videoconferencing services.

239. Those benefits received by Defendant were at the expense of Plaintiffs and Class members.

240. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class members.

241. The circumstances alleged herein are such that it would be unjust for Defendant to retain the portion (if not the entirety) of Plaintiffs' and Class members' payments, or the value of other consideration, that should have been earmarked to provide secure and reliable videoconferencing services, and adequate privacy and security procedures and safeguards for Plaintiffs' and the Class' private information, including only third-party sharing as authorized by its customers.

242. Plaintiffs seek an order directing Zoom to disgorge these benefits and profits and pay restitution to Plaintiffs and other Class members.

FIFTH CAUSE OF ACTION
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.*
(*On Behalf of Plaintiffs and all Classes*)

243. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

244. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

245. Defendant engaged in unfair and unlawful business practices in connection with its provision of Zoom meetings, in violation of the UCL.

246. As alleged herein, Defendant expressly represented to consumers such as Plaintiffs and Class members, among other things: that Zoom meetings were secure, including by use of E2E encryption; and that Defendant would maintain adequate security practices and procedures to protect Plaintiffs' and Class members' private information from

unauthorized access. Defendant also omitted or concealed the material fact of its inadequate privacy and security measures, and thus failed to disclose to Plaintiffs and Class members that it failed to meet legal and industry standards for the protection of Zoom meetings and consequently, its customers' private property and information. Defendant also concealed its commercial tracking and sharing of customers' personal data with third parties.

247. The acts, omissions, and conduct of Defendant as alleged herein constitute "business practices" within the meaning of the UCL.

248. Defendant violated the "unlawful" prong of the UCL by violating, *inter alia*, Plaintiffs' and Class members' constitutional rights to privacy, state and federal privacy statutes, and state consumer protection statutes, such as The Children's Online Privacy Protection Act, 16 C.F.R. § 312.5 ("COPPA"), The Online Privacy Protection Act, California Business and Professions Code §§ 22575-22579 ("CalOPPA"), the California Invasion of Privacy Act ("CIPA"), California Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA"), and The Health Insurance Portability and Accountability Act ("HIPAA").

249. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy (including the aforementioned federal privacy statutes, and state consumer protection statutes, such as COPPA, CalOPPA, CIPA, CDAFA, and HIPAA) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and Class members.

250. The harm caused by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

251. As a result of Defendant's violations of the UCL, Plaintiffs and Class members are entitled to injunctive relief.

252. As a result of Defendant's violations of the UCL, Plaintiffs and Class

members have suffered injury in fact and lost money or property, including but not limited to payments to Defendant and/or other valuable consideration, e.g. access to their private and personal data. The unauthorized access to Plaintiffs' and Class members' private and personal data also has diminished the value of that information.

253. In the alternative to those claims seeking remedies at law, Plaintiffs and Class members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair practices. Further, no legal remedy exists under COPPA, CalOPPA, and HIPAA. Therefore, Plaintiffs and members of the proposed Class are entitled to equitable relief to restore Plaintiffs and Class members to the position they would have been in had Defendant not engaged in unfair competition, including an order enjoining Defendant's wrongful conduct, restitution, and disgorgement of all profits paid to Defendant as a result of its unfair, deceptive, and fraudulent practices.

SIXTH CAUSE OF ACTION
Violation of the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*
(*On Behalf of Plaintiffs and all Classes*)

254. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

255. California's Consumers Legal Remedies Act ("CLRA") has adopted a comprehensive statutory scheme prohibiting various deceptive practices in connection with the conduct of a business providing goods, property, or services to consumers primarily for personal, family, or household purposes. The self-declared purposes of the CLRA are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection.

256. Defendant is a "person" as defined by Civil Code Section 1761(c), because it is a corporation, as set forth above.

257. Plaintiffs and Class members are "consumers" within the meaning of Civil Code Section 1761(d).

258. Zoom meeting software purchased by Plaintiffs and the Class constitute "goods" and within the meaning of Cal. Civ. Code § 1761(a).

259. Zoom meeting services purchased by Plaintiffs and the Class constitute "services" within the meaning of Cal. Civ. Code § 1761(b).

260. Defendant's sale of Zoom meeting software to Plaintiffs and the Class constitute "transactions," as defined by Cal. Civ. Code § 1761(e).

261. Plaintiffs and Class members purchased Zoom meetings software and services from Defendant stores for personal, family, and household purposes, as defined by Cal. Civ. Code § 1761(d).

262. Venue is proper under Cal. Civ. Code § 1780(d) because a substantial portion of the conduct at issue occurred in this District. An affidavit establishing that this Court is the proper venue for this action is attached below.

263. As described herein, Defendant's practices constitute violations of California Civil Code Section 1770 in at least the following respects:

a. In violation of Section 1770(a)(5), Defendant misrepresented that Zoom meeting software and services had characteristics, benefits, or uses that they do not have (being E2E encrypted and private and secure from unauthorized third-party access when in fact they are not);

b. In violation of Section 1770(a)(7), Defendant misrepresented that Zoom meeting software and services were of a particular standard, quality, and/or grade when they were of another (being E2E encrypted and private and secure from unauthorized third-party access when in fact they are not);

c. In violation of Section 1770(a)(9), Defendant advertised Zoom meeting software and services with an intent not to sell them as advertised (advertising them as being E2E encrypted and private and secure from unauthorized third-party access when in fact they are not);

d. In violation of Section 1770(a)(16), Defendant misrepresented that Zoom meeting software and services were supplied in accordance with previous representations when they were not (that they are E2E encrypted and private and secure from unauthorized third-party access when in fact they are not).

264. Defendant's misrepresentations regarding Zoom meeting software and services were material to Plaintiffs and Class members because a reasonable person would have considered them important in deciding whether or not to purchase Zoom meeting software and services.

265. Plaintiffs and Class members relied upon Defendant's material misrepresentations and would have acted differently had they known the truth.

266. As a direct and proximate result of Defendant's material misrepresentations, Plaintiffs and Class members have been irreparably harmed.

267. In accordance with Cal. Civ. Code § 1782(a), prior to the filing of this Complaint, Plaintiffs' counsel served Defendant with notice of these CLRA violations by certified mail, return receipt requested. Defendant has responded and refused to fully rectify the violations detailed above and give notice to all affected consumers.

268. On behalf of Class members, Plaintiffs seek injunctive relief in the form of an order enjoining Defendant from making such material misrepresentations and to engage in a corrective advertising to alert consumers of these misrepresentations.

269. Since Defendant refused to agree to rectify the violations detailed above and give notice to all affected consumers within 30 days of the date of written notice, Plaintiffs also seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CLRA violations.

PRAYER FOR RELIEF

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

A. Determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure and appointing and his Counsel to represent the Class;

B. Finding Defendant's conduct was unlawful as alleged herein;

C. Enjoining Defendant from engaging in the wrongful conduct complained of

herein;

D. Requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Awarding Plaintiffs and Class members actual damages, compensatory damages, punitive damages, statutory damages, and statutory penalties, in an amount to be determined;

F. Awarding Plaintiffs and Class members costs of suit and attorneys' fees, as allowable by law; and

G. Granting such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiffs demands a trial by jury on all issues so triable.

Respectfully submitted,

Dated: May 12, 2021

/s/ Tina Wolfson
Tina Wolfson
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111; Fax: (310) 474-8585

/s/ Mark C. Molumphy
Mark C. Molumphy
mmolumphy@cpmlegal.com
COTCHETT, PITRE & MCCARTHY, LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577
Interim Co-Lead Counsel for Plaintiffs

Rachele R. Byrd
byrd@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
Symphony Towers

750 B Street, Suite 1820
San Diego, CA 92101
Tel: (619) 239-4599
Fax: (619) 234-4599

Albert Y. Chang
achang@bottinilaw.com
BOTTINI & BOTTINI, INC.
7817 Ivanhoe Avenue, Suite 102
La Jolla, CA 92037
Tel: (858) 914-2001
Fax: (858) 914-2002

Eric H. Gibbs
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, California 94612
Telephone: (510) 350-9700
Fax: (510) 350-9701
ehg@classlawgroup.com
Plaintiffs' Steering Committee

FILER ATTESTATION

I, Tina Wolfson, am the ECF user whose identification and password are being used to file this Second Amended Consolidated Class Action Complaint. I hereby attest that Mark C. Molumphy has concurred in this filing.

DATED: May 12, 2021

/s/ Tina Wolfson
Tina Wolfson

AFFIDAVIT OF TINA WOLFSON

I, Tina Wolfson, declare as follows:

1. I am an attorney with the law firm of Ahdoot & Wolfson, PC, counsel for Plaintiffs in this action. I am admitted to practice law in California and before this Court, and am a member in good standing of the State Bar of California. This declaration is made pursuant to California Civil Code section 1780(d). I make this declaration based on my research of public records and upon personal knowledge and, if called upon to do so, could and would testify competently thereto.

2. Venue is proper in this Court because many of the acts and transactions giving rise to this action occurred in this District, and Defendant (1) is authorized and registered to conduct business in this District, (2) has intentionally availed itself of the laws and markets of this District through the distribution and sale of its merchandise in this District, and (3) is subject to personal jurisdiction in this District.

3. Plaintiff Heddi Cundle is a resident of California.

4. Plaintiff Angela Doyle is a resident of California.

5. Plaintiff M.F. is a resident of California.

6. Plaintiff Isabelle Gmerek resides in California.

7. Plaintiff Peter Hirshberg is a resident of California.

8. Plaintiff Therese Jimenez is a resident of California.

9. Plaintiff Lisa Johnston is a resident of California.

10. Plaintiff Saint Paulus Lutheran Church is a citizen of the State of California.

11. Plaintiff Oak Life Church is a citizen of the State of California.

12. Defendant Zoom Video Communications, Inc. is a Delaware corporation with its principal place of business at 55 Almaden Blvd, San Jose, California 95113. Defendant is registered and authorized to conduct business and regularly conducts business in the State of California.

I declare under penalty of perjury under the laws of the United States and the State of California this 12th day of May, 2021 in Los Angeles, California that the foregoing is true and correct.

/s/ Tina Wolfson
Tina Wolfson