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
10728 Lindbrook Drive
Los Angeles, CA 90024
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	Case No. 5:20-CV-02155-LHK
This Document Relates To: All Actions	**FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**
	DEMAND FOR JURY TRIAL

Plaintiffs Caitlin Brice, Heddi N. Cundle, Angela Doyle, Sharon Garcia, Isabelle Gmerek, Cynthia Gormezano, 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

[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).

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.

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 that company's Firebase Analytics. Plaintiffs never granted permission for third parties to extract and use such data—indeed, they were not even aware of the data transmission.

---

[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 28, 2020)> (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).

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 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 during which unauthorized bad actors hijack Zoom videoconferences, displaying pornography, screaming racial epitaphs, or engaging in similarly despicable conduct. This practice has become so

[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).

commonplace on the Zoom platform that it is referred to as "Zoombombing." Bad actors have disrupted private moments ranging from Alcoholics Anonymous meetings to Holocaust memorial services (*e.g.*, in one instance with images of Adolf Hitler).[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 with the horrified reactions of participants being the digital trophies of the Zoombombers. 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.

[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.*

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.