Eric H. Gibbs (SBN 178658)
Andre Mura (SBN 298541)
Amanda M. Karl (SBN 301088)
Jeffrey Kosbie (SBN 305424)
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, California 94612
Telephone: (510) 350-9700
Fax: (510) 350-9701
ehg@classlawgroup.com
amm@classlawgroup.com
amk@classlawgroup.com
jbk@classlawgroup.com

Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

STACEY SIMINS, on behalf of herself and all others similarly situated,

Plaintiff,

v.

ZOOM VIDEO COMMUNICATIONS, INC.,

Defendant.

Case No. 5:20-cv-2893

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and all others similarly situated, alleges the following:

SUMMARY OF THE CASE

1. Zoom provides a video-conferencing service called Zoom Meetings. The video meetings ostensibly allow users to engage in video and audio conversations with only those specified people with whom they have chosen to communicate. Users reasonably expect these conversations to be private and secure, and these expectations are heightened by the very nature of Zoom Meetings, where users can not only be heard, but also seen.

2. Zoom has long cultivated the expectation that its service is both secure and private, and Zoom has grown its business and revenues based on that expectation. Among other things, Zoom has long marketed the service as being protected with end-to-end, 256-bit encryption, and has emphasized that it takes concrete steps to ensure privacy and security for its users.

3. But in reality, Zoom has failed to deliver private and secure video conferencing. The level of encryption Zoom provides is far less robust than what it promised. And a wide variety of security failings have jeopardized Zoom-users' privacy. These failings have enabled bad actors to join meetings without permission, to access web cameras surreptitiously, and to access many thousands of recorded Zoom meetings stored online. All the while, Zoom has actively shared information about its users with Facebook, despite failing to disclose that practice in its privacy policy.

4. Zoom's conduct violates various state laws and has led to Zoom profiting unfairly at the expense of its customers. Plaintiff, as a paying customer, has brought suit on behalf of herself and all others similarly impacted, to force Zoom to deliver appropriate injunctive relief and remuneration.

PARTIES

5. Plaintiff Stacey Simins is a citizen and resident of Texas.

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

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interest and costs, and at

least one class member is a citizen of a different state than Defendant Zoom. This Court has jurisdiction over supplemental state law claims pursuant to 28 U.S.C. § 1367.

8. This Court may exercise jurisdiction over Defendant because they are registered to conduct business in California; have sufficient minimum contacts in California; and intentionally avail themselves of the markets within California through the promotion, sale, marketing, and distribution of their products, thus rendering the exercise of jurisdiction by this Court just and proper.

9. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant is headquartered in this district, Defendant conducts substantial business in this district, and a substantial part of the events giving rise to Plaintiff's claims occurred in this District.

INTRADISTRICT ASSIGNMENT

10. Assignment to the San Jose Division would be proper because Zoom is headquartered in San Jose, California, and a substantial part of the events or omissions which give rise to the claims alleged herein occurred there.

FACTUAL ALLEGATIONS

Background

11. Zoom was launched in 2011. The company provides video-conferencing capabilities to businesses and individuals.

12. The cornerstone of Zoom's product line-up is Zoom Meetings.[1] Zoom Meetings provide video, voice, chat, and content sharing across mobile devices, desktops, laptops, telephones, and conference room systems. The Zoom Meetings are effectively calls made online, most commonly with video as well as audio. The meetings can have two participants or far more.[2]

13. Zoom Meetings integrates with numerous other widely used software tools, including Dropbox, Google, LinkedIn, Microsoft, Salesforce, and Slack. Zoom advertises unparalleled usability, making it "easy to start, join, and collaborate across any device" with "streamlined enterprise-grade video conferencing."[3]

[1] https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa
[2] https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa
[3] https://web.archive.org/web/20200208202315/https://zoom.us/meetings

14. Zoom customers include global Fortune 50 companies and span industry sectors, including education, entertainment/media, enterprise infrastructure, finance, government, health care, manufacturing, non-profit/not for profit and social impact, retail/consumer products, and software/internet.[4] As of January 31, 2020, approximately 81,900 Zoom customers had more than 10 employees.

15. As of December 2019, Zoom had about 10 million peak daily Zoom Meeting participants. Following the rapid adoption of Zoom due to COVID-19 related closures, in March 2020 Zoom reported daily meeting participants topped 200 million.[5]

16. Zoom users can access Zoom Meetings by creating an account. Zoom offers a basic account level for free, and it charges between $14.99 and $19.99 per month, per host, for accounts that come with additional features, including the ability to host more participants and to conduct meetings lasting longer than 40 minutes. Zoom users can pay for additional add-on features, including additional cloud storage and support for conference rooms. In addition, Zoom offers education and healthcare plans with their own pricing.

Users Reasonably Expect Security and Privacy When Using Zoom

17. Because of the very nature of Zoom Meetings, users expect and understand that the service comes with privacy and security features. Like talking on the phone, communicating by video conference is generally understood to be a private matter. Users reasonably expect that their communications will only be heard and seen by those that the users know they are communicating with in the meeting.

18. Zoom understands that user privacy and security are important for its customers. As Zoom put it in a June 2019 security guide, "Zoom places security as the highest priority in the operations of its suite of products and services."[6] At least as far back as November 2019, Zoom's security webpage acknowledged that "millions of people and organizations trust us with their communications."[7]

[4] https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa
[5] https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
[6] https://web.archive.org/web/20200331082306/https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
[7] https://web.archive.org/web/20191104094251/https://zoom.us/security

19. Not only does Zoom know its users expect privacy and security, Zoom actively cultivates that expectation. Zoom's June 2019 security guide tells users it "strives to continually provide a robust set of security features and practices to meet the requirements of businesses for safe and secure collaboration.[8] Since November 2019, its security webpage told users that Zoom is "proud to exceed industry standards when it comes to your organizations communications."[9] And since at least October 2018, the product webpage for Zoom Meetings promised that it was "built for modern teams" and allowed users to "meet securely" with end-to-end encryption and other security features and settings.[10]

20. Zoom's blog includes numerous entries regarding Zoom's security features, stating, for example, "ensuring the privacy and security of our users and their data is our top priority"[11] and "Zoom is able to give hosts and attendees the security they need to communicate confidently and securely over any device."[12]

21. In addition to these statements acknowledging the importance of privacy and security, Zoom tells users "how Zoom secures your data and protects your privacy."[13] Of particular emphasis, Zoom tells potential and current users that Zoom uses "encryption for all meetings."[14] And in particular, beginning at least in July 2017, Zoom claimed to provide "industry-standard end-to-end Advanced Encryption Standard (AES) encryption using 256-bit keys to protect meetings."[15]

22. Zoom has emphasized the end-to-end and 256-bit AES encryption both generally and in the context of meetings involving entities in the fields of education, finance, government, and healthcare—all of which require privacy and security. On July 12, 2019, in a blog post titled "The Rise of Cloud Video Conferencing in Financial Services," Zoom identified compliance and security, including encryption and security certifications, as one of the capabilities that financial services looked for in evaluating video conferencing services.[16] So, on its finance webpage, Zoom advertises "multi-

[8] https://web.archive.org/web/20200331082306/https:/zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
[9] https://web.archive.org/web/20191104094251/https://zoom.us/security
[10] https://web.archive.org/web/20181028201834/https://www.zoom.us/meetings
[11] https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/
[12] https://blog.zoom.us/wordpress/2019/12/04/hosts-admins-secure-zoom-meeting-experience/
[13] https://zoom.us/docs/en-us/privacy-and-security.html
[14] https://zoom.us/meetings
[15] https://web.archive.org/web/20200406001952/https://zoom.us/meetings
[16] https://blog.zoom.us/wordpress/2019/07/12/rise-of-cloud-video-conferencing-in-financial-services/

layer security with 256-bit AES encryption, data sovereignty, and role-based access control;"[17] its government and education pages explain that "Zoom enables FERPA/HIPAA compliance and provides 256-bit encryption;"[18] and its healthcare page claims "HIPAA (signed BAA) and PIPEDA/PHIPA compliance with 256-bit AES encryption."[19] Prior to April 2020, going back at least to March 2019, these webpages all advertised "end-to-end 256-bit AES encryption."[20]

23. Zoom also advertises security and encryption features on its plans and pricing page. Prior to April 2020, and at least as far back as July 2017, the Security listing on this page included "AES 256 bits encryption: [e]nd to end security is an added layer of application security. Zoom can encrypt all presentation content at the application layer using the Advanced Encryption Standard (AES) 256-bit algorithm."[21]

Zoom Broke Its Promises and Failed to Protect Security and Privacy

24. Despite its promises, and its knowledge of its users' expectations, Zoom has consistently failed to protect its users' security and privacy.

Zoom Failed to Provide the Encryption It Promised

25. Despite its unequivocal representations, Zoom never provided end-to-end encryption for Zoom meetings.

26. A Zoom spokesperson recently acknowledged that Zoom did not actually have the ability "to enable [end-to-end] encryption for Zoom video meetings."[22]

27. Instead, what Zoom was claiming to be end-to-end encryption is commonly referred to as transport encryption. With end-to-end encryption, only the participants in a Zoom meeting would have the keys required to decrypt meeting content. With transport encryption, data is encrypted as it travels over the Internet, but Zoom itself has access to the encryption keys.

[17] https://zoom.us/finance
[18] https://zoom.us/education, https://zoom.us/government
[19] https://zoom.us/healthcare
[20] https://web.archive.org/web/20190211182832/https://www.zoom.us/finance, https://web.archive.org/web/20181028201833/https://zoom.us/education, https://web.archive.org/web/20190314004506/https://zoom.us/government, https://web.archive.org/web/20181205050841/https://www.zoom.us/healthcare
[21] https://web.archive.org/web/20170703052830/https://zoom.us/pricing
[22] https://theintercept.com/2020/03/31/zoom-meeting-encryption/

28. Providing end-to-end encryption is possible in video meetings. In fact, despite any technical challenges in implementing end-to-end encryption, Apple's FaceTime does so.[23]

29. And in the period during which Zoom was telling customers its meetings were end-to-end encrypted, Zoom never presented them with the caveat that what Zoom was claiming to be end-to-end encryption was what the rest of the industry called transport encryption. As Zoom's chief product officer Odel Gal recently admitted, the company had instead "incorrectly suggest[ed] that Zoom meetings were capable of using end-to-end encryption."[24]

30. Not only did the lack of end-to-end encryption raise the concern that Zoom or its employees would access meeting content, it also raised the concern that other third parties, including governments might do so. The Intercept reported that Zoom has failed to publish transparency reports, which enumerate the government requests for data they receive, from which countries, and which of those they comply with.[25]

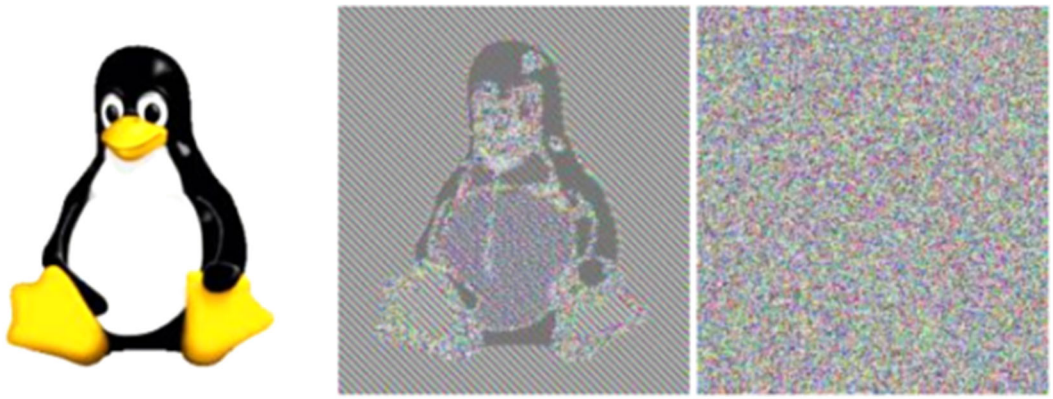
31. For example, a Citizen Lab report found that some Zoom Meetings with participants in North America were routed through servers in China, as were the encryption keys used to secure those calls.[26] Due to Zoom's failure to implement true end-to-end encryption, state operators in China could have had access to the unencrypted meeting data. Shortly after the Citizen Lab report, Zoom acknowledged "it is possible certain meetings were allowed to connect to systems in China, where they should not have been able to connect."[27] Although Zoom software typically connects to datacenters near a user's region, during heavy network traffic, Zoom uses servers in other regions too, and as Zoom began rapidly expanding capacity in February 2020, it included servers in China on the whitelist of potential servers for clients outside of China. Zoom admitted that these servers should have never been on the whitelist for backup servers available to clients outside of China.

32. The lack of end-to-end encryption was not Zoom's only broken promise relating to encryption. On April 3, 2020, the Citizen Lab at the University of Toronto revealed that Zoom did not

[23] https://theintercept.com/2020/03/31/zoom-meeting-encryption/
[24] https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/
[25] https://theintercept.com/2020/03/31/zoom-meeting-encryption/
[26] *See also* https://techcrunch.com/2020/04/03/zoom-calls-routed-china/
[27] https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/

use AES-256 encryption as it had advertised.[28] Instead, Citizen Lab discovered, Zoom used an AES-128 key for its encryption. AES-256 vs. 128 refers to the length of the encryption key, and a 256-bit key is exponentially stronger than a 128-bit key.[29]

33. Even worse, Citizen Lab explained, Zoom used an in-house implementation of the algorithm in ECB mode. ECB mode encrypts data in blocks, which preserves patterns from the original file in the encrypted version, as illustrated below:[30]



34. In response to the concerns raised by Citizen Lab, Zoom CEO Eric Yuan admitted "we can do better with our encryption design."[31]

Zoom Failed to Provide Private and Secure Meetings

35. Beyond its broken promises regarding encryption, there have been many indications that Zoom's meetings were not as private and secure as reasonable users would have expected.

Zoom's Waiting Room Has Not Been Secure

36. Citizen Lab issued reports on April 3 and April 8, 2020, concerning "a security issue with Zoom's Waiting Room feature."

37. Zoom advertises Waiting Rooms as an additional security feature. In a February 2020 blog post, Zoom explained that waiting rooms are "a virtual staging area that prevents people from joining a meeting until the host is ready."[32] With the waiting room feature enabled, the meeting host

[28] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
[29] https://www.rapidsslonline.com/blog/encryption-strength-128-bit-ssl-vs-256-ssl/
[30] https://securityboulevard.com/2020/04/simple-illustration-of-zoom-encryption-failure/
[31] https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/
[32] https://blog.zoom.us/wordpress/2020/02/14/secure-your-meetings-zoom-waiting-rooms/

must "admit" all users to the meeting before they gain access to the video chat. Meeting hosts can also kick people out of the video chat, sending them back to the waiting room.

38. Citizen Lab reported that when a user joined a Zoom Meeting waiting room, Zoom sent the video data stream and decryption key to the user's computer.[33] This could allow the user to extract and decrypt the video data stream, allowing them to view the meeting video without being admitted to the meeting.

Zoom Bypasses Mac Security

39. Zoom has also recently admitted to several security vulnerabilities.

40. For instance, a security researcher named Jonathan Leitschuh pointed out that a security flaw enabled third-parties to both enable and access the webcam in Zoom meetings on Mac computers.[34] This could trigger a computer to automatically launch a Zoom meeting with no notification to the computer's user.[35] Zoom's video-on preferences increased the danger. Unless a user disabled that default setting, a third party could set Zoom to launch with video on. As a result, Mr. Leitschuh explained, an attacker exploiting this vulnerability could use Zoom to access a user's video feed without the user's knowledge.

41. Further, Mr. Leistchuh disclosed, this same vulnerability would have allowed an attacker to engage in a denial-of-service attack by repeatedly joining a user to an invalid call.[36] If an attacker initiated a denial-of-service attack exploiting this vulnerability, the Zoom app would constantly request "focus" from the OS, disrupting the user's ability to continue using their computer.

42. This security flaw resulted from the way in which Zoom is installed on a Mac computer. The installation creates a local web server that is undocumented and undisclosed. This web server can not only launch a Zoom meeting, but also can re-install the Zoom app even after a user had uninstalled it. With the web server installed, the Zoom app could be used to bypass the web browser's security prompt to launch a Zoom meeting.

---

[33] https://citizenlab.ca/2020/04/zooms-waiting-room-vulnerability/

[34] https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5

[35] https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5

[36] https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5

43. In a July 8, 2019 blog post, Zoom acknowledged the security flaw and said that it had intentionally created the web server. Zoom claimed the web server could function as "a workaround to a change introduced in Safari 12 [the MacOS web browser] that requires a user to confirm that they want to start the Zoom client prior to joining every meeting."[37]

44. Two days later, Zoom CEO Eric Yuan admitted that "we misjudged the situation" and said Zoom would remove the web server installed on Mac clients.[38] On the same day as Yuan's blog post, Apple released an automatic MacOS update to uninstall the web server.[39] According to security researcher Patrick Wardle, this is the only known instance in which Apple used its Malware Removal Tool against a popular app.[40]

45. A distinct security vulnerability emerged publicly in March 2020, when security researchers Felix Seele and Patrick Wardle revealed problems with the installer for Zoom's Mac client. First, Seele disclosed that Zoom's Mac installer used preinstallation scripts to install Zoom without a user ever clicking install.[41] Once a user opened the Zoom installer on MacOS, preinstallation scripts would unpack and install Zoom without the user intentionally installing the app.

46. Seele described the flaw as "very shady" and said it "definitely leaves a bitter aftertaste." The app is installed without the user consenting via a highly misleading prompt to gain root privileges. Per Seele, "[t]he same tricks that are being used by macOS malware."[42]

47. Zoom's CEO responded to Seele's original post via Twitter, saying, "Your point is well taken and we will continue to improve."[43] Two days later, Zoom issued a new installer that purportedly addressed the security flaws identified by Seele.[44]

48. In response to Seele's disclosure, Wardle further tested the Zoom Mac installer and concluded that the Mac OS installer created a vulnerability that would allow attackers to gain root privileges within MacOS.[45] Wardle also identified a separate vulnerability in the Zoom MacOS app

[37] https://blog.zoom.us/wordpress/2019/07/08/response-to-video-on-concern/
[38] https://blog.zoom.us/wordpress/2019/07/10/security-update-and-our-ongoing-efforts/
[39] https://techcrunch.com/2019/07/10/apple-silent-update-zoom-app/
[40] https://objective-see.com/blog/blog_0x56.html, https://techcrunch.com/2019/07/10/apple-silent-update-zoom-app/
[41] https://twitter.com/c1truz_/status/1244737672930824193, https://objective-see.com/blog/blog_0x56.html
[42] https://objective-see.com/blog/blog_0x56.html
[43] https://twitter.com/ericsyuan/status/1245104758240632832
[44] https://www.theverge.com/2020/4/2/21204648/zoom-macos-installer-update-privacy-security-concerns
[45] https://objective-see.com/blog/blog_0x56.html

that would allow an attacker to piggyback off of Zoom's access to gain access to a user's webcam and microphone.

49. Zoom acknowledged the security flaws identified by Wardle. As part of an April 2, 2020 product update, Zoom said it "Resolved an issue where a malicious party with local access could tamper with the Zoom installer to gain additional privileges to the computer [and] Resolved an issue where a malicious party with local access could gain access to a user's webcam and microphone."[46]

Zoom Bypasses Security on Cisco Endpoints

50. On November 25, 2019, Cisco published a blog post[47] alerting its customers to a vulnerability created by Zoom that provided an access point attackers could use to control a Cisco video endpoint, located inside a corporate firewall, without obtaining authentication.[48] Cisco said the Zoom feature was "not a Cisco supported solution that meets our standards of enterprise-grade security."[49]

51. The security flaw stemmed from how Zoom implemented its connection to the Cisco video endpoint. The Zoom Connector used Cisco video endpoints to join Zoom meetings. A user would install the Zoom Connector on a Windows server located inside an organization's firewall. During the installation, the user entered passwords for the Cisco video endpoint. The credentials were stored in the Zoom Connector so that the Connector could control the Cisco video endpoint.

52. The Zoom Connector also created a unique URL for each Cisco video endpoint. By navigating to one of these URLs on the Zoom cloud, a user could then control the Zoom Connector, and via the Zoom Connector, control the Cisco video endpoint. This URL was unsecured and allowed anyone with the URL to control the Cisco video endpoint. Security analyst Brent Kelly explained, "[t]he Zoom Connector essentially creates a sort of tunnel between the [Cisco] video endpoint browser interface and the Zoom cloud."[50]

53. In a November 26, 2019 blog post, Zoom admitted "If a bad actor were to . . . obtain that URL, for example through an exploit of the administrator's browser, they could access the device

[46] https://support.zoom.us/hc/en-us/articles/201361963-New-Updates-for-macOS
[47] https://blogs.cisco.com/collaboration/our-focus-on-security-in-an-open-collaboration-world
[48] https://www.nojitter.com/video-collaboration-av/zoom-gives-way-video-device-security-breach-again
[49] https://blogs.cisco.com/collaboration/our-focus-on-security-in-an-open-collaboration-world
[50] https://www.nojitter.com/video-collaboration-av/zoom-gives-way-video-device-security-breach-again

administration functions without logging in. The URL would continue to be accessible even after the administrator had logged out or changed their password on the Zoom web portal."[51]

Recorded Zoom Meetings Accessible Online

54. Zoom allows meeting hosts to record videos and save them to their computer or online. Other meeting participants are notified when the host starts to record but are not required to consent to the recording.

55. Due to lax security protocols, Zoom did not password-protect recorded meetings by default and exacerbated the problem by defaulting to nearly identical naming structures for every recording.

56. As a result, thousands of recorded Zoom meetings have been viewable on the Internet. These recorded meetings were stored online without a password.[52] One search for recordings, using Zoom's default naming convention, revealed more than 15,000 results.[53] The Washington Post reported that the accessible recorded meetings included one-on-one therapy sessions; a training orientation for workers doing telehealth calls that included people's names and phone numbers; small-business meetings that included private company financial statements; and elementary school classes, in which children's faces, voices, and personal details were exposed.[54] Per the Washington Post, "Many of the videos include personally identifiable information and deeply intimate conversations, recorded in people's homes. Other videos include nudity, such as one in which an aesthetician teaches students how to give a Brazilian wax." [55]

57. The Washington Post reported that "because Zoom names every video recording in an identical way, a simple online search can reveal a long stream of videos elsewhere that anyone can download and watch."[56] The article reported that several participants in the videos were contacted for comment, and they said they had no idea how their videos became available online.[57]

Zoom Meetings Have Been Frequently Invaded by Malicious Actors

[51] https://blog.zoom.us/wordpress/2019/11/26/zoom-connector-resolved-security-issue/
[52] https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/
[53] https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/
[54] https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/
[55] https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/
[56] https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/
[57] https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

58. Zoom created a default setting that permits all meeting participants to share their screens. As a result, attackers have had the ability to send any image or material to all participants in a meeting.

59. This led to such common abuse that various reports have noted a trend in what is now known as "Zoombombing," a practice in which attackers join Zoom meetings and then broadcast indecent content, hate symbols, or other shocking images.

60. Zoombombers can not only access meetings through publicly shared meeting links, but may also access them by using automated software that attempts possible Zoom Meeting IDs.[58] Each Zoom conference call is assigned a Meeting ID that consists of 9 to 11 digits. Hackers can simply automate the guessing of random IDs within that space of digits. Security experts at Check Point Research found they could predict about four percent of randomly generated Meeting IDs. The Check Point researchers said enabling passwords on each meeting was the only thing that prevented them from randomly finding a meeting. As one security article put it, "a crazy number of meetings . . . are not being protected by a password."[59]

61. Zoom had also failed to block repeated attempts to scan for meeting IDs. And Zoom software automatically indicated whether a meeting ID was valid or invalid, which had the effect of facilitating would-be Zoombombers in their efforts to access meetings.

62. Trent Lo, a security professional, worked with others to demonstrate the ability to access Zoom meeting room information without having to log in. Lo said Zoombombers could thus readily find approximately 100 meetings per hour, and with added resources, would-be Zoombommbers "could probably discover most of the open Zoom meetings on any given day." Per Lo, his success rate of opening a random meeting of 14 percent. Only password-protected meetings could not be accessed. But Zoom had not previously enabled passwords by default in all meetings.

[58] https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/
[59] https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/

Zoom Sent User Data to Facebook

63. On March 26, 2020, an article revealed that the Zoom iOS app shared user data with Facebook—even if a user did not have a Facebook account.[60]

64. Zoom used Facebook's software development kits (SDK), which allow developers to send analytics data to Facebook. After a user downloaded Zoom, Zoom notified Facebook when a user opened Zoom and provided information on the user's cell phone, time zone and city, phone carrier, and a unique advertiser identifier.[61]

65. Following publication of the article, Zoom admitted it was sharing information with Facebook. While Zoom claimed that the practice was for the convenience of users,[62] Facebook's terms required that Zoom "provide[ ] robust and sufficiently prominent notice to [its] users regarding the Customer Data collection, sharing and usage."[63]

66. Zoom's privacy policy, however, did not disclose all of the information Zoom shared with Facebook.[64] While the policy disclose it sent Facebook profile information to Facebook when a user logged into Zoom using their Facebook login, the policy did not disclose the additional data that Zoom sent to Facebook about its users.

Zoom's Acknowledged Security and Privacy Failures

67. Zoom has known about its security and privacy failings for quite some time. For example, DropBox has long been so concerned with Zoom's security flaws that since 2018, DropBox has invested in finding problems with Zoom's software, having its own engineers confirm those problems, and then reporting them to Zoom.[65] Nevertheless, Zoom continued to market its services as secure and private until recently.

[60] https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account
[61] https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account
[62] https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/
[63] https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account
[64] https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account
[65] https://www.nytimes.com/2020/04/20/technology/zoom-security-dropbox-hackers.html

68. Yuan, Zoom's CEO, finally acknowledged on April 1, 2020, "[W]e recognize that we have fallen short of the community's – and our own – privacy and security expectations." In the same blog post, Zoom promised to "enact[] a feature freeze [for the next 90 days], effective[] immediately, and shift[] all our engineering resources to focus on our biggest trust, safety, and privacy issues." Several days later, Yuan reiterated, "I really messed up," adding "we need to slow down and think about privacy and security first."[66]

69. Despite Zoom's sudden interest in upgrading its security and privacy, the public outcry and investigations continue to grow. On March 30, 2020, the FBI issued a warning about videoconferencing hijacking prompted by incidents on Zoom's platform.[67] A group of 19 House Democrats sent Zoom a letter on April 3, 2020, "requesting detailed information on how Zoom safeguards consumer privacy."[68] The letter raised concern that "[a]s consumers turn to Zoom for business meetings, remote consultations with psychologists, or even virtual happy hours with friends, they may not expect Zoom to be collecting and using so much of their information." The letter raised concern with the security and privacy implications of several specific Zoom features. The letter included specific questions as to these functions and how much notice Zoom provides consumers regarding the functions, as well as more general questions regarding Zoom's data collection and use practices. At least 27 U.S. attorney general's offices are also investigating Zoom's privacy and security failures.[69]

70. In response, Google, Tesla, SpaceX, the New York City Department of Education, and the Taiwanese, Australian, and German governments, amongst others, have all banned employees from using Zoom until its security practices improve.[70] The U.S. Senate similarly asked its members to avoid using Zoom.[71]

---

[66] https://www.wsj.com/articles/zoom-ceo-i-really-messed-up-on-security-as-coronavirus-drove-video-tools-appeal-11586031129?st=jmn0xqiy1ea3c63&mod=openfreereg

[67] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

[68] https://mcnerney.house.gov/sites/mcnerney.house.gov/files/Letter%20to%20Zoom_04.03.2020.pdf

[69] https://www.wsj.com/articles/zoom-ceo-i-really-messed-up-on-security-as-coronavirus-drove-video-tools-appeal-11586031129?st=jmn0xqiy1ea3c63&mod=openfreereg

[70] https://www.zdnet.com/article/make-sure-your-zoom-meetings-are-safe-by-doing-these-10-things/; https://www.wsj.com/articles/zoom-ceo-i-really-messed-up-on-security-as-coronavirus-drove-video-tools-appeal-11586031129?st=jmn0xqiy1ea3c63&mod=openfreereg

[71] https://www.businessinsider.com/senate-warns-against-zoom-2020-4

71. Nevertheless, Zoom continues to offer video conferencing services subject to privacy and security concerns. On April 15, 2020, Motherboard reported that hackers are selling information on two unknown Zoom vulnerabilities, one for Windows and one for MacOS.[72] According to a veteran of the cybersecurity industry, the Windows exploit is "[p]erfect for industrial espionage." It was reportedly on the market for $500,000.

PLAINTIFF'S EXPERIENCE

72. Plaintiff Stacey Simins is a resident of Austin, Texas. Ms. Simins own a dance studio, where she teaches burlesque dance and pole dance. Ms. Simins's studio was closed to in-person classes as a result of the state's shelter-in-place order due to COVID-19.

73. Ms. Simins began using Zoom on or about March 18, 2020. Ms. Simins purchased a paid Zoom license in order to provide practice sessions for her clients. Privacy and security are very important to Ms. Simins, and she expected Zoom to be private and secure.

74. Prior to purchasing Zoom, Ms. Simins went to Zoom's plans and pricing webpage, which included a description of Zoom's security features. Specifically, Ms. Simins saw that the plans and pricing webpage listed security features, including encryption. Ms. Simins also saw that the admin feature controls, listed under the Pro license, included enabling cloud recording, which she assumed was secure. After viewing these representations, and believing Zoom to be secure, Ms. Simins purchased a pro account.

75. After Ms. Simins began using Zoom, uninvited men joined some of her classes on Zoom. The attackers were intimidating and harassing to Ms. Simins's clients. On at least one occasion, Ms. Simins had to cancel a session as a result.

76. As a result, several of Ms. Simins's students have refused to join more classes because of their fear over future incidents. Ms. Simins's business has suffered as a result.

77. Ms. Simins continues to pay for Zoom, but she continues to worry about Zoom's security flaws.

78. Had Ms. Simins known about Zoom's security flaws prior to purchasing it, she would not have paid for Zoom.

[72] https://www.vice.com/en_us/article/qjdqgv/hackers-selling-critical-zoom-zero-day-exploit-for-500000

CLASS ACTION ALLEGATIONS

79. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Class and Subclass:

Class

All persons and entities in the United States who have used Zoom Meetings.

Subclass

All persons and entities in the United States who have purchased one or more Zoom Meeting plans.

Excluded from the proposed Class and Subclass are Zoom; any affiliate, parent, or subsidiary of Zoom; any entity in which Zoom has a controlling interest; any officer, director, or employee of Zoom; any successor or assign of Zoom; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse; and any members of the judge's staff.

80. The above proposed class definitions suffice because they use objective characteristics; class membership turns on objective criteria including whether someone used (or purchased a plan to use) Zoom Meetings. Documents and information identifying Class and Subclass members are in Defendant's possession, custody, and control.

81. **Numerosity.** Zoom Meetings has been used by millions of users making the members of the proposed Class and Subclass too numerous to practically join in a single action. Class and Subclass members may be notified of the pendency of the action by mail or email, supplemented by published notice (if deemed necessary or appropriate by the Court).

82. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed members of the Class and Subclass and predominate over questions affecting only individual Class or Subclass members. These common questions include:

a. Whether Zoom in fact made representations about the privacy and security of Zoom Meetings, including with respect to encryption;

b. Whether Zoom's representations about privacy and security of Zoom Meetings, including with respect to encryption, were false or misleading;

c. Whether Zoom knew about privacy and security flaws affecting Zoom Meetings but failed to disclose or actively concealed those flaws from the public;

d. Whether the information Zoom represented, failed to disclose, and concealed was material because it would be important to a reasonable person;

e. Whether Zoom misrepresented or concealed information with the intent to defraud Class and Subclass members;

f. Whether Zoom was unjustly enriched at the expense of Plaintiff and Class and Subclass members;

g. Whether Plaintiff and the Class and Subclass are entitled to injunctive relief; and

h. Whether Plaintiff and the Class and Subclass members are entitled to damages, restitution, or disgorgement.

83. **Typicality.** Plaintiff's claims are typical of the claims of the proposed Class and Subclass. Plaintiff and the members of the proposed Class and Subclass all used or purchased the use of Zoom Meetings with the same flaws impacting security and privacy, giving rise to substantially the same claims.

84. **Adequacy.** Plaintiff is an adequate representative of the proposed Class and Subclass because her interests do not conflict with the interests of the members of the Class and Subclass she seeks to represent. Plaintiff has retained counsel who are competent and experienced in complex class action litigation, and who will prosecute this action vigorously on Class and Subclass members' behalf.

85. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class and Subclass member, while meaningful on an individual basis, is not of such magnitude as to make the prosecution of individual actions against Zoom economically feasible. Even if Class and Subclass members themselves could afford such individualized litigation, the court system could not. In addition to the burden and expense of managing many related actions, individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, a class action presents far fewer

management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

86. In the alternative, the proposed Class and Subclass may be certified because:

a. the prosecution of separate actions by the individual members of the proposed Class and Subclass would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Zoom;

b. the prosecution of individual actions could result in adjudications, which as a practical matter, would be dispositive of the interests of non-party Class and Subclass members or which would substantially impair their ability to protect their interests; and

c. Zoom has acted or refused to act on grounds generally applicable to the proposed Class and Subclass, thereby making appropriate final and injunctive relief with respect to the members of the proposed Class and Subclass as a whole.

FIRST CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW,
Cal. Bus. & Profs. Code § 17200, *et seq*.
(On Behalf of the Class)

87. Plaintiff and the Class incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

88. Zoom has violated and continues to violate California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*, which prohibits unlawful, unfair, and fraudulent business acts and practices.

89. Zoom's acts and practices, as alleged in this complaint, constitute unlawful, unfair, and fraudulent business acts and practices, in violation of the Unfair Competition Law. In particular, Zoom represented and cultivated the expectation among Zoom Meetings users that the video-conferencing service was private and secure (including due to represented levels of encryption), when in reality those representations were false and misleading; Zoom also knew but failed to disclose and concealed that various flaws in Zoom Meetings undermined the security and privacy of the meetings.

90. Zoom's business acts and practices are unlawful in that they violate the California Consumers Legal Remedies Ac, Cal. Civ. Code § 1750, *et seq*., for the reasons set forth below.

91. Zoom's conduct also constitutes unfair business practices for at least the following reasons:

a. The gravity of harm to Plaintiff and Class members from Zoom's acts and practices far outweighs any legitimate utility of that conduct;

b. Zoom's conduct is immoral, unethical, oppressive, unscrupulous, or substantially injurious to Plaintiff and Class members; and

c. Zoom's conduct undermines or violates the stated policies underlying the Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*, namely, to protect consumers against unfair and sharp business practices relating to the sale of goods and services in the marketplace.

92. Zoom's acts and practices also constitute fraudulent practices in that they are likely to deceive a reasonable person. As described above, Zoom made false and misleading representations concerning the security and privacy of Zoom Meetings, including with respect to encryption levels, and also knowingly failed to disclose and actively concealed information about flaws that undermined the security and privacy of Zoom Meetings. As Zoom knew, its knowledge was exclusive to the company and was not generally known to the public or to Zoom users, and had Zoom disclosed what it knew, Plaintiff, Class members, and other reasonable persons would not have used or purchased Zoom Meetings or would have paid significantly less.

93. As a direct and proximate result of Zoom's business practices, Plaintiff suffered injury in fact and lost money or property, because she purchased a Zoom Meetings plan that was worth less than what Plaintiff (and others) paid due to Zoom's material misrepresentations and nondisclosures.

94. Plaintiff and Class members are entitled to restitution and equitable relief, including an order directing Zoom to cease its misrepresentations, cease its unlawful nondisclosures, and to provide improved security and privacy in connection with Zoom Meetings.

SECOND CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, Cal. Civ. Code § 1750, *et seq*.
(On Behalf of the Subclass)

95. Plaintiff and the Subclass incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

96. Zoom is a "person" within the meaning of Civil Code §§ 1761(c) and 1770, and has provided "services" within the meaning of Civil Code §§ 1761(b) and 1770.

97. Plaintiff and identifiable members of the proposed Subclass are "consumers" within the meaning of Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" within the meaning of Civil Code §§ 1761(e) and 1770.

98. Zoom's acts and practices, which were intended to result and which did result in the sale of Zoom Meetings, violate § 1770 of the Consumers Legal Remedies Act for at least the following reasons:

a. Zoom represents that its video-conferencing services had characteristics, uses, or benefits which they do not have;

b. Zoom advertises its goods with intent not to sell them as advertised;

c. Zoom represents that its video-conferencing services are of a particular standard, quality, or grade when they are not;

d. Zoom represents that a transaction conferred or involved rights, remedies, or obligations which they do not;

e. Zoom represents that its goods have been supplied in accordance with a previous representation when they have not; and

f. Zoom fails to disclose material information within its exclusive knowledge and actively conceals material information.

99. As described above, Zoom sold video-conferencing services to Subclass members while misrepresenting the security and privacy of those services and while failing to disclose and concealing known flaws that undermined the security and privacy of the meetings.

100. Had Zoom not made those misrepresentations and concealed information, but instead adequately disclosed what it knew, Plaintiff, members of the proposed Subclass, and reasonable consumers would not have purchased or would have paid less for Zoom Meetings.

101. Pursuant to the provisions of Cal. Civ. Code § 1782(a), Plaintiff will send a notice letter to Zoom to provide it with the opportunity to correct its business practices, and may amend this complaint to add a claim for damages should Zoom not do so.

102. Pursuant to California Civil Code § 1780, Plaintiff seeks appropriate injunctive relief and reasonable attorney's fees and costs.

THIRD CAUSE OF ACTION
FRAUD
(On Behalf of the Subclass)

103. Plaintiff and the Subclass incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

104. As detailed above, Zoom made false and misleading representations concerning the security and privacy of Zoom Meetings, including with respect to encryption levels, and also knowingly failed to disclose and actively concealed information about flaws that undermined the security and privacy of Zoom Meetings. As Zoom knew, its knowledge was exclusive to the company and was not generally known to the public or to Zoom users.

105. Zoom knew that the privacy and security of its video-conferencing service was materially worse than it represented and what Subclass members reasonably expected.

106. Zoom intended that Plaintiff and Subclass members rely on its representations and nondisclosures concerning security and privacy.

107. The information Zoom misrepresented and concealed was material in that it was important to reasonable persons, and Plaintiff and Subclass members relied on the misrepresentations and nondisclosures to their detriment. As a result, Plaintiff and Subclass members purchased Zoom Meetings they would not otherwise have purchased or paid significantly more for Zoom Meetings than they otherwise would have.

108. Plaintiff seeks an award of all available damages.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT,
(On Behalf of the Subclass)

109. Plaintiff and the Subclass incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

110. Plaintiff also seeks restitution in quasi contract.

111. Zoom's misrepresentations and nondisclosures made its video-conferencing service appear more secure and private than it really was—leading Plaintiff and the Subclass to pay more money to Zoom than they otherwise would have paid.

112. Zoom knew about, accepted, and benefited from Plaintiff's and Subclass members' purchase of these video services.

113. Under the circumstances, it would be inequitable for Zoom to benefit from its non-secure and non-private Zoom Meetings.

114. To avoid injustice, Plaintiff and the Subclass accordingly seeks restitution and disgorgement of profits in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Simins, on behalf of herself and the Class and Subclass, seeks the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class and Subclass as requested herein, appointing Gibbs Law Group LLP as Class Counsel, and finding that Plaintiff is a proper representative of the Class and Subclass requested herein.

B. Plaintiff requests injunctive relief. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class and Subclass, including order directing Zoom to cease its misrepresentations, cease its unlawful nondisclosures, and to provide improved security and privacy in connection with Zoom Meetings.

C. Plaintiff also requests damages, restitution, attorneys' fees, statutory costs, and such other and further relief as is just and proper (except that Plaintiff does not currently seek monetary relief under the Consumers Legal Remedies Act). Plaintiff seeks attorneys' fees under California Code of Civil Procedure 1021.5 and the Consumers Legal Remedies Act.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a trial by jury for all issues so triable under the law.

DATED: April 27, 2020

Respectfully submitted,

GIBBS LAW GROUP LLP

By: */s/ Eric H. Gibbs*

Eric H. Gibbs
Andre Mura
Amanda M. Karl
Jeffrey Kosbie
505 14th Street, Suite 1110
Oakland, California 94612
Telephone: (510) 350-9700
Fax: (510) 350-9701
ehg@classlawgroup.com
amm@classlawgroup.com
amk@classlawgroup.com
jbk@classlawgroup.com

Attorneys for Plaintiff and Proposed Class