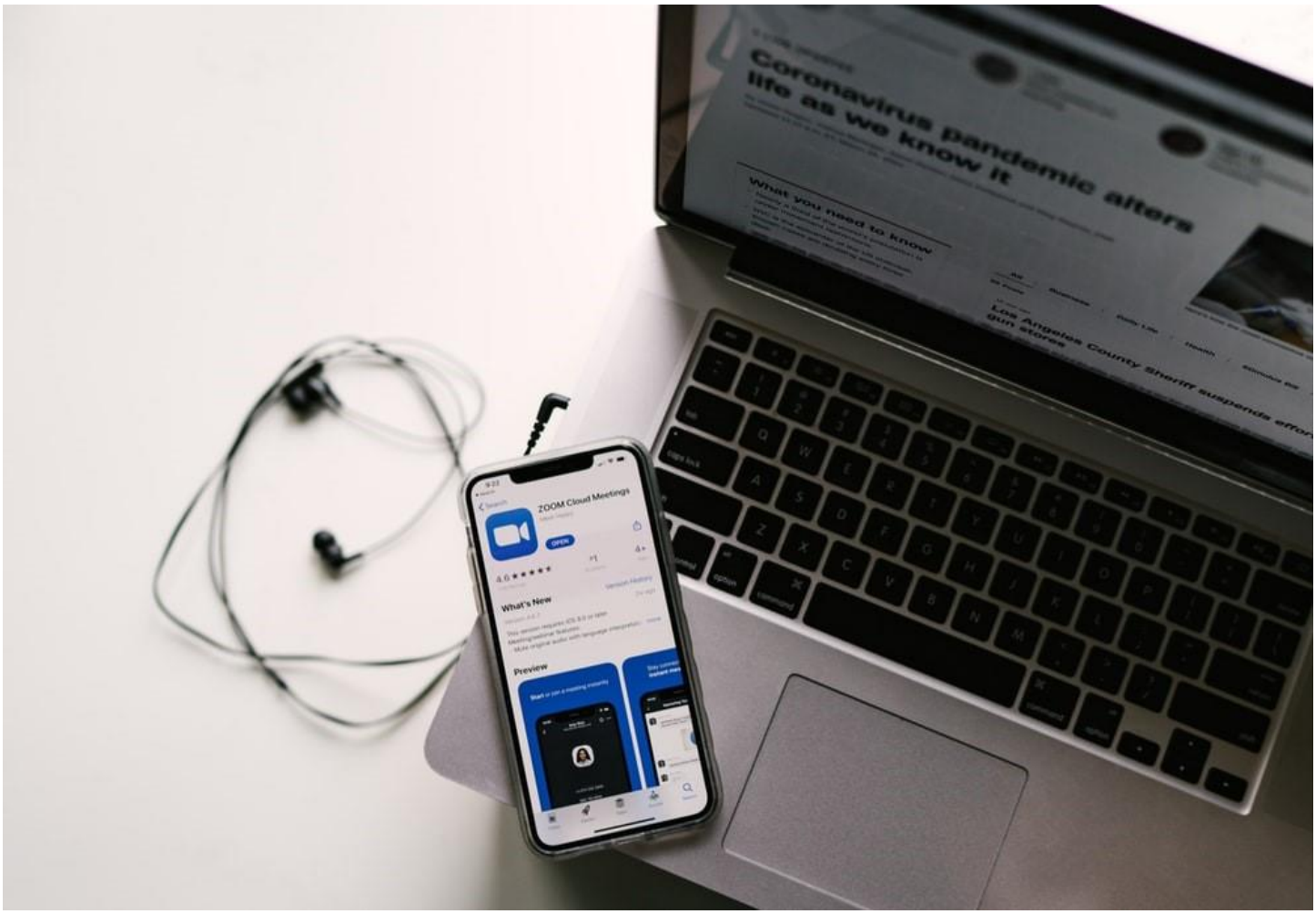
4-19-2020

Zooming in on Big Tech's Deceptive Privacy Practices and Why We Should All Be Paying More Attention

Samuel Friedman
Cardozo Arts & Entertainment Law Journal

Zooming in on Big Tech's Deceptive Privacy Practices and Why We Should All Be Paying More Attention

BY SAMUEL FRIEDMAN/ ON APRIL 19, 2020



Join With Computer Audio.

Send Personal Information to Facebook.

By now, you're more than likely familiar with the first prompt—it's the text that appears when you first open Zoom, and by enabling this function you can join a meeting using your computer's microphone. Zoom is the video conferencing app that has recently surged in popularity due to the coronavirus pandemic. [1] Zoom allows users to work or learn remotely, all from a safe social distance in the relative privacy of their own homes. While the company responsible for the app, Zoom Video Communications, hasn't given concrete numbers regarding the size of its userbase,[2] Zoom's mobile platform was so popular towards the end of March that it was second only to TikTok as the most downloaded app globally.[3]

And yet, despite this ubiquity, you are probably not familiar with the second prompt. Of course, that's because it wasn't a prompt at all. Recent reporting revealed that Zoom was silently sending personal information to Facebook's servers each time the Zoom app was accessed, and it was doing so without first seeking user approval.[4] Details delivered to Facebook included when the user opened the app, their location, their phone carrier and model, as well as an advertising identifier uniquely generated by the user's device that helps companies to target the user with personalized advertisements.[5] Moreover, even if users had read the company's privacy policy (which a majority of people do not[6]), they would not have been aware that Zoom was disclosing this information because Zoom's privacy policy did not even detail this practice![7]

Shortly after the Motherboard story broke, Zoom released an update to its iOS app that halted it from sending undisclosed data to Facebook.[8] This swift software patch, however, was not enough to prevent a Zoom user from filing a class action lawsuit against the company for the illicit disclosures.[9] The plaintiff's complaint seeks relief under the California Consumer Privacy Act of 2018 ("CCPA"), as well as other related statutes.[10] Effective as of January 1, 2020, the CCPA imposes data regulation requirements on businesses of a certain size that store the personal information of Californians.[11] Given the expansiveness of the Internet, however, the CCPA's requirements effectively cover most companies that traffic in user data nationwide. Indeed, in the class action against Zoom, the complaint's putative class includes "[a]ll persons and businesses in the United States whose personal or private information was collected and/or disclosed by Zoom to a third party upon installation or opening of the Zoom video conferencing application."[12]

The Zoom class action is important in that it presents an early opportunity to gauge the effectiveness of the new CCPA in promoting privacy rights for users across the United States. Nonetheless, there are some concerns that this all-encompassing scope will expose the statute to constitutional challenges.[13] And yet at the same time, the CCPA reflects a growing trend, both within the United States and internationally, for safeguarding privacy rights.[14] For example, Republican Senator Jerry Moran of Kansas recently proposed the Consumer Data Privacy and Security Act of 2020, which would create a national rubric for the safeguarding of consumer data, while also exempting small business from the more onerous compliance provisions required under the CCPA.[15]

Data privacy has arguably never been more important. As the coronavirus forces citizens across the world into self-isolation, people have become increasingly more reliant on technology that can provide connections.[16] And yet, time and again, the companies responsible for safeguarding user data have repeatedly shown themselves to be irresponsible stewards of this information. Notwithstanding the fact that Zoom was disclosing your data without notice or consent, rumors have circulated regarded the company's other privacy problems. This may be because Zoom's increased userbase has brought with it an increased degree of public scrutiny, causing a litany of security concerns to come to light. For instance,

Zoom's marketing materials asserted that the service was end-to-end encrypted, yet a spokesperson later conceded that "it is not possible to enable [end-to-end] encryption for Zoom."[17] The company also admitted to accidentally routing some calls through China, a country notorious for overzealously monitoring the Internet.[18] And then there's the practice of "Zoombombing" – because Zoom's meetings are organized through the use of randomly generated access codes and do not require passwords, there have been several instances where people have intruded into video calls, often sharing offensive material in the process.[19] Indeed, the security concerns have risen to such a level that U.S. senators have been advised against using the platform.[20]

Zoom's privacy problems, however, are only the latest example of Big Tech's nonchalant approach to safeguarding user data. On the contrary, Big Tech companies, such as Zoom and Facebook, actively profit off the proliferation of such data. Despite the overt shortcomings of Zoom's app security, many apps regularly disclose user information to third parties.[21] As part of their design, apps are often built using software-development kits ("SDKs"), which facilitate the integration of certain key features and functions.[22] Using an existing SDK makes it easier for app developers to build their own apps, but it also likely results in user information input into these new apps being sent to the third party creator of the SDK.[23] Facebook's SDK, for example, is extremely popular and is used in thousands of apps.[24] A 2019 report done by The Wall Street Journal found that 11 out of more than 70 apps tested, all of which were among the most popular in Apple's App Store, were discovered to send personal information to Facebook.[25] The end result is that these third parties, such as Facebook, can then make money by assisting advertisers by directly targeting users with certain advertisements.[26]

As Americans become more reliant on these apps and services, we need to be more vigilant about what we are giving up and what these companies are taking in return. Zoom's unauthorized data disclosure is just the latest example of Big Tech companies partaking in what Harvard Business School professor Shoshana Zuboff calls "surveillance capitalism" – the exploitation of personal user data in pursuit of billions in profits.[27] Zuboff's thesis posits a fundamental misunderstanding in the way that users look at their relationship with Big Tech: users think that the *platforms* these companies provide are free, when in reality it's the *users* that are free.[28] After all, only one party to this transaction is taking away billions in profits.

The more users come to rely on Big Tech companies for their services—whether due to a pandemic or otherwise—the harder it will be to critique and object to their deceptive and duplicitous practices. Time and again, Big Tech companies have sought forgiveness after the fact rather than first seeking permission. To illustrate, one needs only look as far as the complaint in the Zoom class action, which asserts that while the company did release a corrective software update, it did not require users to install the update to continue using the service.[29] In other words, unless Zoom users took it upon themselves to install the update,

the app would "continue to unknowingly send unauthorized personal information to Facebook, and perhaps other third parties. Zoom could have forced all iOS users to update to the new Zoom App to continue using Zoom but appears to have chosen not to."[30] Zoom, like every other Big Tech company, is counting on us not paying attention when it comes to how they exploit our personal information. As users, we need to start asserting our rights, whether or not we're first prompted to do so.

Sam Friedman is a Second Year Law Student at the Benjamin N. Cardozo School of Law and the rising Executive Editor of the Cardozo Arts & Entertainment Law Journal. Sam's past experience includes work as a student law clerk for Hon. Julie Manning, Chief Bankruptcy Judge for the District of Connecticut, as well as a paralegal at Gibson Dunn & Crutcher LLP in their Real Estate practice.

---

[1] Ben Gilbert, *All your friends are using Zoom, the chat app that is suddenly dominating competition from Google and Microsoft*, Business Insider (Mar. 24, 2020, 4:12 PM), https://www.businessinsider.com/zoom-video-everywhere-google-hangouts-skype-2020-3.

[2] *Id.*

[3] *Id.*

[4] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account*, Motherboard (Mar. 26, 2020, 9:00 AM), https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.

[5] *Id.*

[6] Jessica Guynn, *What you need to know before clicking 'I agree' on that terms of service agreement or privacy policy*, USA Today (Jan. 29, 2020, 2:21 PM), https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/.

[7] Cox, *supra* note 4.

[8] Joseph Cox, *Zoom Removes Code That Sends Data to Facebook*, Motherboard (Mar. 27, 2020, 6:38 PM), https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook.

[9] Joseph Cox, *Zoom Faces Class Action Lawsuit for Sharing Data with Facebook*, Motherboard (Mar. 30, 2020, 10:00 PM), https://www.vice.com/en_us/article/pke4vb/zoom-faces-class-action-lawsuit-for-sharing-data-with-facebook.

[10] Complaint for Damages and Equitable Relief at 10, Cullen v. Zoom Video Communications, Inc., No. 5:20-cv-02155-SVK (N.D. Cal. Mar. 30, 2020).

[11] Associated Press, *California Vastly Expands Digital Privacy. Will People Use It?*, NBC Los Angeles (Jan. 2, 2020, 1:56 AM), https://www.nbclosangeles.com/news/california-news/california-vastly-expands-digital-privacy-will-people-use-it/2282516/.

[12] Complaint for Damages and Equitable Relief at 7, Cullen v. Zoom Video Communications, Inc., No. 5:20-cv-02155-SVK (N.D. Cal. Mar. 30, 2020).

[13] Associated Press, *supra* note 11.

[14] *See* Gregory M. Kratofil, Jr. & Elizabeth Harding, *Federal Privacy Legislation Update: Consumer Data Privacy and Security Act of 2020*, Nat'l L. Rev. (Mar. 14, 2020), https://www.natlawreview.com/article/federal-privacy-legislation-update-consumer-data-privacy-and-security-act-2020.

[15] *Id.*

[16] *See* Geoffrey A. Fowler & Heather Kelly, *'Screen time' has gone from sin to survival tool*, Wash. Post. (Apr. 9, 2020, 8:00 AM), https://www.washingtonpost.com/technology/2020/04/09/screen-time-rethink-coronavirus/.

[17] Micah Lee & Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, The Intercept (Mar. 31, 2020, 4:00 AM), https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

[18] Zack Whittaker, *Zoom admits some calls were routed through China by mistake*, Tech Crunch (Apr. 3, 2020, 8:12 PM), https://techcrunch.com/2020/04/03/zoom-calls-routed-china/.

[19] Ashley Carman, *Why Zoom became so popular*, The Verge (Apr. 3, 2020, 4:38 PM), https://www.theverge.com/2020/4/3/21207053/zoom-video-conferencing-security-privacy-risk-popularity.

[20] Kiran Stacey & Hannah Murphy, *US Senate tells members not to use Zoom*, Fin. Times (Apr. 9, 2020), https://www.ft.com/content/dac7d60b-54fa-402b-8469-70f85aaace76.

[21] Sam Schechner, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.*, Wall St. J. (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] Ben Gilbert, *How Facebook makes money from your data, in Mark Zuckerberg's Own Words*, Business Insider (Apr. 11, 2018, 10:25 AM), https://www.businessinsider.com/how-facebook-makes-money-according-to-mark-zuckerberg-2018-4.

[27] Frank Bajak, Meet the scholar who diagnosed 'surveillance capitalism', AP (Dec. 11, 2019), https://apnews.com/68e73fe9c328fc4548d051e0d56b1b7f.

[28] *Id.*

[29] Complaint for Damages and Equitable Relief at 6, Cullen v. Zoom Video Communications, Inc., No. 5:20-cv-02155-SVK (N.D. Cal. Mar. 30, 2020).

[30] *Id.*