Frankfurt Kurnit Klein + Selz PC

Focus on the Data

Unique Insights and Practical Guidance on Privacy and Data Security Issues Worldwide

A Big Zooming Mess: A Cautionary Tale

By Tanya Forsheit on April 6, 2020

Over the last several weeks, while Americans have grown accustomed to working from home, home schooling, and life in lockdown during the COVID-19 pandemic, the Zoom videoconferencing service has surged in popularity for every imaginable form of gathering, professional and personal. Zoom has become the service of choice – from team meetings to kids' story times; from

religious services to happy hours; from corporate onboarding to every manner of more "intimate" get-togethers for individuals who are following government-mandated social distancing guidelines.

The media and then, in quick succession, regulators, plaintiffs' lawyers, and even Congress, began to scrutinize, publicize, and take legal action with respect to what were perceived as privacy or data security flaws from the latest technology darling. The result is a still-evolving case study in the classic reactionary American response to privacy and data security concerns, a phenomenon we have seen again and again in this practice space.

What sins has Zoom actually committed? Are they really so "shocking" from a privacy and data security perspective? In violation of law? Just not best practice? Creepy? And has Zoom's iterative response served as a wet blanket or fuel for the inferno?

In this post, I explore the who, what, why, when, and how of this, at least as much as we can say as we sit here today. And because I am a hopeless nerd, I have chosen the format required by California's data breach notification law, California Civil Code § 1798.82(d)(1), as the very best way to tell this story. We are going to use this blog post as a jumping off point for a free live and recorded roundtable discussion webinar (using WebEx [insert winking emoji here]) on April 14, 2020, at 12:30 pm Eastern/9:30 am Pacific. You can register **here**.

What Happened?

- The Privacy Issues

On March 24, 2020, **Consumer Reports published an article suggesting "Zoom Calls Aren't as Private as You May Think,"** questioning provisions of Zoom's privacy policy that appeared to indicate that any and all meeting information, including video and other content, could be used by Zoom for targeted advertising. Two days later, on March 26, Motherboard published an article entitled **"Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account."** In fact, the Motherboard author did not accuse Zoom of doing something unusual in sending analytics information such as device model, time zone, city, phone carrier, and unique advertising identifiers, through the Facebook SDK. The Facebook SDK is just another form of tracking technology used by many apps (think of it as the app equivalent of trackers like cookies used in a browser environment).

Despite the title, the real issue identified in the Motherboard article was Zoom's purported failure to sufficiently disclose its use of the Facebook SDK, and with that the fact that the SDK sends data to Facebook, in its privacy policy.

If you are lawyer, this leads to the obvious question – was Zoom required to disclose the use of the Facebook SDK in its privacy policy? And for all the lawyers out there, the answer is that it depends. Some think the California Consumer Privacy Act ("CCPA"), which took effect on January 1, 2020, will require the treatment of unique advertising identifiers as personal information. The answer is more apparent under contract. As correctly pointed out in the article, section 3.b.ii. of the **Facebook's business terms** require the specific disclosure of the Facebook SDK.

On March 30 and 31, **Plaintiff's lawyers threw together and filed class action complaints** accusing Zoom of all manner of wrongdoing and violating several laws, even claiming that the disclosure of information to Facebook gives rise to a private right of action under the CCPA. Such a claim, if valid, would entitle the plaintiffs to statutory damages of $100 to $750 per consumer per violation, without any showing of harm.

- The Security Issues

It turns out the Facebook SDK and privacy concerns were only the tip of the iceberg. On Monday, March 30, as reported by the New York Times, the New York Attorney General sent a letter to Zoom reportedly inquiring about privacy issues (such as the Facebook data sharing) and also what, if any, new security measures Zoom had put in place to handle increased traffic on its network and to detect hackers. The regulator reportedly expressed concern regarding the amount of time Zoom had taken to address vulnerabilities "that could enable malicious third parties to, among other things, gain surreptitious access to consumer webcams."

Apart from the more recent phenomenon of **Zoombombing (about which the FBI issued a warning on March 30)**, where bad actors use open and/or poorly secured Zoom meetings to post malicious content, the New York AG asked about changes the company put in place after **a security researcher exposed a number of security vulnerabilities starting as far back as March 2019** (the linked article includes the researcher's timeline). According to the researcher, it took Zoom months to address

flaws in 2019. Per the New York Times article, the New York AG's letter noted that Zoom did not address the problem until after **the Electronic Privacy Information Center filed a complaint with the Federal Trade Commission in July 2019** alleging that Zoom exposed users to the risk of remote surveillance, unwanted videocalls, and denial-of-service attacks.

On Tuesday, March 31, **the Intercept published an article claiming that, despite public statements to the contrary, Zoom meetings are not encrypted "end to end".** Instead, according to Zoom's statements to the reporters, Zoom video meetings use transport encryption – in this case, a combination of TCP using TLS and UDP with AES encryption. The fact that Zoom is using transport encryption is again not so unusual – not unlike the use of the Facebook SDK described above. The Intercept article took issue with a perceived misrepresentation by Zoom about a technical structure that could theoretically allow Zoom itself to spy on meetings.

It did not take long for other state regulators to start asking questions. By April 3, POLITICO reported on a coordinated effort among **multiple state attorneys general looking at Zoom's privacy and security practices**, including Connecticut Attorney General William Tong and Florida Attorney General Ashley Moody. In a piece published on Saturday, **April 4, the Wall Street Journal reported that 27 attorney general's offices have raised questions**.

Also on April 3, Congress jumped into the fray when **19 House Democrats sent Zoom a letter** seeking details on Zoom's data practices and Ohio Senator Sherrod Brown, the ranking member of the Committee on Banking, Housing and Urban Affairs, sent a **letter to the Federal Trade Commission** asking the Commission to investigate Zoom for deceptive practices.

Perhaps most concerning of all, **the same day, the Washington Post published a piece** stating that thousands of Zoom videos "have been left viewable on the open Web", including therapy sessions, training for workers doing telehealth calls including names and phone numbers, business meetings including private company financial statements, elementary school classes in which children's faces, voices and personal details were exposed, and demonstrations of personal care techniques that included nudity.

While this initially sounds alarming, the Post story clarifies that these are all meetings that participants chose to record and saved onto separate online storage space, including Amazon buckets, without a password, and that "[i]t does not affect videos that

remain with Zoom's own system." Nonetheless, the Post article claims 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."

What Information Was Involved?

- The Facebook SDK Thing

As mentioned above, the information Zoom sent to Facebook through the Facebook SDK was just device information, not the kind of information that gives rise to breach notification obligations in California (or any other state), or to a private right of action for statutory damages under the CCPA. That subset of information is limited to (A) an individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) social security number; (ii) driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; or (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual; or (B) a username or email address in combination with a password or security question and answer that would permit access to an online account. Cal. Civil Code §1798.81.5 (cross-referenced in Cal. Civil Code §1798.150, the CCPA's private right of action). Note also that, for purposes of the CCPA, unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

- The Reported Security Vulnerabilities

The security researcher findings dating back to last year, the New York Attorney General's letter, the Congressional inquiries, and the Washington Post's article raise the question of whether poor naming conventions or other security vulnerabilities have allowed unauthorized third parties access to Zoom video or other content even if users take advantage of passwords and other features

designed to help secure the meetings. To the extent these videos and other content include sensitive information such as the data elements described above from California's law (which are comparable to those identified in other state data breach notification laws), or other extremely personal information such as nudity, there are clearly larger issues that call for further exploration.

What Zoom Is Doing.

Zoom reacted immediately to the Motherboard article the day after it ran, March 27, by **removing the Facebook SDK**. Since Zoom could have simply updated its privacy policy to disclose the use of the Facebook SDK, the speed with which Zoom removed the SDK is curious (particularly since it is a tool that is used by thousands of apps).

Two days later, over a weekend, **on March 29, Zoom did in fact update its privacy policy** in apparent reaction to the Consumer Reports March 24 allegations that Zoom was able to use the contents of meetings for targeted advertising. The updated privacy policy boldly declares at the top of the document that "[w]e do not sell your personal data," but makes the legally required disclosure in the fine print far below that "Zoom does use certain standard advertising tools on our marketing sites which … sends personal data to the tool providers, such as Google. …California's CCPA law has a very broad definition of "sale". Under that definition, when Zoom uses the tools to send the personal data to the third-party tool providers, it may be considered a "sale". It is important to know that advertising programs have always worked this way and we have not changed the way we use these tools. It is only with the recent developments in data privacy laws that such activities may fall within the definition of a 'sale.'"

On April 1, **Zoom's Co-Founder and CEO Eric Yuen published a blog post** apologizing for having "fallen short of the community's – and our own – privacy and security expectations" and enumerating the changes already made and that Zoom was continuing to make.

The April 1 apology was not the last of what has the outward appearance (whether or not accurate) of hasty clean-up activity. On April 2, **Zoom made additional changes, removing an attendee attention tracker feature** that **reportedly let meeting hosts track whether participants have their Zoom app in view on a PC or in the background**.

On April 3, **TechCrunch and others reported that Zoom would change its default settings** to require a password for meetings and enable the waiting room functionality, which blocks meeting participants from joining until they are admitted by the host.

Eric Yuen told the Wall Street Journal, for its article published April 4, that he "messed up."

What You Can Do.

Zoom's conduct has received so much attention that even those who typically pay no attention to privacy and data security news are well aware of the drama. Some organizations have already taken steps to help mitigate the risks associated with using Zoom (or any online service). During our **April 14 webinar**, we will discuss things that organizations concerned with the accusations leveled against Zoom can do. These include, but are not limited to, the following:

- Don't use Zoom to share especially sensitive information or content;
- Don't publicly circulate Zoom meeting links; and/or
- Don't record Zoom meetings

Organizations can also choose to use one of the other commercially available videoconferencing solutions.

Other Important Information

As a privacy and data security lawyer, what is most striking about the Zoom story to me, based on the information made publicly available to date, is not that Zoom has engaged in particularly egregious privacy and data security practices. That's not at all clear as we sit here today. What is more concerning from the outside is the emerging pattern of revising statements and apologies, with new issues arising on a daily basis. It's a pattern we have seen before, most dramatically with organizations like Facebook. Whenever any organization rises to prominence so quickly, it emerges from obscurity and can no longer treat privacy and data security as anything other than a top priority. For the Facebooks of the world, they grew large enough that even a Cambridge

Analytica, being called before Congress, and being subject to fines in the billions of dollars, are not enough to bring them down. For a company like Zoom, where the timeline to explosive growth and scrutiny is so much more condensed, its fate is less certain.

Of course, the whole situation takes on a new tone in light of the considerable contribution Zoom is making to the greater good by scaling its operations so quickly to allow millions of Americans to communicate with each other during a public health crisis. There are really difficult questions:

- What weight should be given to privacy and security concerns in a time of such seismic societal change and crisis?
- Should our attention be focused on the more significant concerns (like poor naming conventions that might make video content more easily accessible) as opposed to noise about practices that are extremely common and don't implicate sensitive information (like the Facebook SDK)?

I do have one immediate takeaway that I don't think is likely to change as this tale continues to unfold. It is the same thing all the best privacy and security lawyers I know have been saying for years. Privacy and security cannot be an after-thought. It should not be a nice-to-have budget line item. It is a must-have. And once the spotlight shines the light on your practices, it is often too late.

For More Information.

We are going to keep talking about this and exploring different angles and perspectives. You can register **here** for our roundtable discussion webinar on April 14, at 12:30 pm Eastern. You can submit questions through chat and we will try to address a number of audience questions in real-time.

Klein+Selz

Copyright © 2021, Frankfurt Kurnit Klein & Selz PC. All Rights Reserved.