Alert

April 22, 2020

COZEN O'CONNOR

Demand for Information-Sharing Platforms Has Soared, Raising Privacy Concerns With Regulators

Amid the havoc wreaked by COVID-19 on individuals, businesses, and economies, technology companies offering information-sharing platforms have enjoyed an unexpected upside as demand for their services has skyrocketed. But with great opportunity comes new responsibilities. The COVID-19 pandemic has exposed potential vulnerabilities of platforms — such as those that provide video and teleconferencing services, e-learning, and telemedicine — to data security and privacy threats. While these tools have diminished the risk of COVID-19 exposure by providing alternatives to in-person meetings, users may be exposed to new risks online, prompting state attorneys general (AGs) to question whether consumers are being protected with adequate security and data privacy practices.

Zoom: A Case Study

Videoconferencing platform Zoom Video Communications, Inc. (Zoom) has become the test case for those seeking to protect consumer privacy in this new remote environment. Zoom has seen a steady rise in the number of users on its platform since it launched in 2011. As millions transitioned to working from home, Zoom reported that demand for its service had grown exponentially from 10 million daily users in December 2019 to more than 200 million daily users in March 2020.

Along with the millions of new subscribers came more frequent instances of "Zoombombing," in which uninvited and unauthorized participants disrupt teleconferences with lewd, offensive, or even threatening conduct and content.

Recent reports point to other Zoom security vulnerabilities. *The Washington Post* reported that videos containing personally identifiable information and private conversations from one-on-one therapy sessions and a training orientation for workers performing telehealth calls were openly viewable online. Among thousands of accessible recordings were small-business meetings that included private company financial statements, and elementary school classes in which children's faces, voices, and personal details were exposed. Furthermore, the naming convention Zoom uses to label recordings resulted in certain Zoom recordings that were saved outside of Zoom becoming searchable and accessible to anyone.

Several AGs, including New York AG James, Florida AG Moody, and Connecticut AG Tong — himself a witness to Zoombombing — have announced that their respective offices are investigating whether Zoom's security measures and disclosures are accurate and sufficient. In many cases, the Federal Trade Commission (FTC) undertakes its own investigation concurrently with AG investigations. That is likely to happen in Zoom's case, given the growing chorus of Democratic lawmakers calling on the FTC to open an investigation of Zoom's data privacy and security practices. Moreover, a recently filed investor class action suit alleges that investors were misled about the robustness of Zoom's digital defenses.

In response to these concerns, Zoom has updated its privacy policy, emphasizing that it does not, and has never, sold users' personal data. In a recent blog post, Founder and CEO Eric Yuan promised that Zoom will focus on addressing privacy issues for the next 90 days, and that it will release a transparency report similar to those put out by Facebook, Google, and Twitter.

Steps Platforms Should Consider Taking Now

Zoom's situation is instructive and should serve as a warning for information-sharing platforms, especially those providing conferencing services, e-learning, telehealth, or supporting other synchronous electronic communications.

Ann-Marie Luciano

Member

aluciano@cozen.com
Phone: (202) 471-3420
Fax: (202) 861-1905

Related Practice Areas

- State Attorneys General

Information-sharing platforms should consider adopting the following privacy best practices in the current environment:

- Review and, if necessary, update privacy policies and security settings to ensure they are sufficient for demand levels, accurate, and in compliance with applicable law.
    - Platforms should consider actively promoting privacy-enhancing features, such as password-protection for virtual meetings and administrator controls over participants.
    - Platforms should prominently warn conference participants that a meeting is being recorded.
    - If the platform is marketed to and/or used by students or patients of health care providers, the provider should evaluate additional opt-in requirements to ensure adequate disclosure and consent.
    - If the platform now needs to disclose patient or consumer data to local, state, or federal entities addressing COVID-19, it should update its privacy policies to communicate this new requirement.
- Review the privacy infrastructure, such as locations for storing consumer personal information, including whether search engines can easily uncover recordings of meetings, and whether private messages can be accessed by third parties.
- Apply the most stringent privacy settings as the default from which users can opt-out, rather than making them an opt-in feature.
- Deploy easy-to-use privacy settings (as a toggle, for example) to require users to make an explicit choice each time they take a privacy-implicating action.

Often overlooked by companies in the first instance, consumer complaints and online reviews can provide a useful barometer of consumer satisfaction and should be monitored to help providers identify areas of weakness or vulnerability. AGs frequently take action in response to consumer complaints and even social media commentary, a form of corporate shaming that has taken criticism of companies' actions into public forums as never before. AGs themselves are issuing guidelines to help the public stay safe on video conferences, demonstrating their concern with these issues and providing useful insights into the areas they are most focused on. Due to the privacy and security issues at stake in videoconferencing, the FTC has released its own suggestions for best practices: Video conferencing: 10 privacy tips for your business.

At a minimum, these steps will reduce the chance of encountering a situation that would prompt an AG or an FTC investigation, and demonstrate a responsible attitude by platforms in response to the demand explosion and revenue windfall.