Videoconferencing privacy and security are far from perfect

April 13 2020, by Elizabeth Stoycheff

Videoconferencing software mapped in terms of security and privacy protections. Credit: Elizabeth Stoycheff, CC BY-ND

If, before COVID-19, you were concerned about all the data that

technology companies had about you, just wait. As stay-at-home orders push more professional and social activities online, it's becoming harder to remain in control.

Look no further than Zoom, which suffered dual security and privacy crises in the past few weeks. Lawsuits alleging data sharing violations and hackers have descended on the software, which has led Google and school districts to ban Zoom for professional use.

I'm a researcher who investigates how these concerns affect the use of online platforms. The first thing to understand is that privacy and security are two different things, and they have different consequences for using videoconferencing platforms.

Privacy versus security

Privacy refers to individuals' universal rights to control their data. Security is how that data is protected. One or both can be compromised when using popular videoconferencing tools, leaving personal information vulnerable.

For example, say someone signs up for a new videoconferencing platform using full name, email address and phone number. Ideally, the platform company would maintain both privacy and security, meaning the company wouldn't share that person's information outside the company, and would keep their system protected from hackers and viruses. The most private platforms, like Signal and FaceTime, use end-to-end encryption to ensure that even the companies themselves do not have access to the contents of anyone's communication. When such systems are kept secure, they are the best communication tools to use.

Alternatively, a company could compromise privacy but maintain security, meaning it would collect information about video calls and sell

that data to a third party for marketing purposes. Many companies will include such conditions in their terms of service, which users rarely read. However, companies have incentive to maintain security; they don't want to be overrun with criminals or pranksters, which could damage their reputations.

Worst case is when a company surrenders both privacy and security, meaning they share personal information with third parties, and they fail to prevent data breaches. Offerings from these companies are the riskiest of all digital tools, and unfortunately, they're all too common.

Here's how some of the most popular video conferencing services stack up.

Videoconferencing options

Zoom's most updated privacy policy states that the company "do[es] not allow third parties to use any personal data obtained from users for their own purposes, unless you consent." However, Zoom is currently facing a lawsuit alleging that it violated this agreement and shared user data with Facebook. The company claims that this was a security, not a privacy, breach and that it was not compensated for data sharing.

Zoom has also come under fire for security flaws that have allowed "Zoom-bombers" to intrude on personal calls, often using profane or obnoxious content. The company admitted that it has fallen short on protecting users' privacy and security and is working to fix the problems.

Microsoft Teams' privacy policy leaves no questions. It explicitly states that it "collects data from you, through our interactions with you and through our products." It is upfront about using this information to market to users, personalize their experiences and even participate in legal investigations. In other words, make no presumptions of privacy

here—all personal data on the platform is fair game.

To differentiate its security from Zoom, Microsoft's Teams has implemented dual-factor authentication, meaning passwords are not enough. Users need to also enter email or text codes to log in. The Microsoft family of software—though not Teams specifically—confronted a number of security problems this year, including a breach of its customer service center that exposed 14 years of information. The jury is still out on whether it's a more secure alternative to Zoom.

Unlike Zoom and Teams, Webex offers hosts the option of end-to-end encryption, meaning only the sender of a message and its recipient have access to the data within. This is a strong privacy feature, but it's elective and tends to limit the usefulness of the tool.

Webex is not immune to security breaches, but the difference between this company and their competitors is their transparency and quick patches. The platform actively maintains a public list of vulnerabilities, which documents how the company has resolved them.

Skype has a privacy problem. It shares user data with third parties, across the entire Microsoft family, and even with law enforcement when asked. In a benign effort to improve customer service, it allowed employees to access recordings of Skype conversations from their personal computers over a period of several years. Such tasks have since been transferred to a secure facility, but it doesn't change the fact that if you've used Skype lately, your privacy has been compromised.

Like Teams, Skype uses dual-factor authentication but it was also likely compromised in the massive Microsoft customer service breach earlier this year.

Long before Facebook acquired WhatsApp, the video chat service provided end-to-end encryption on calls and messages. The privacy of chats here are, and always have been, protected.

However, WhatsApp suffered a very public security breach when Jeff Bezos' personal messages were compromised by spyware and leaked. That was one of 12 vulnerabilities the platform faced last year.

Apple's FaceTime also boasts end-to-end protections, and the company has upheld its commitment to privacy by refusing requests from the FBI to access user devices. It's positioning itself as a steward of user privacy.

Like other services, FaceTime has been susceptible to occasional security hacks. In early 2019, users reported a security glitch in its group calls where recipients could hear and see callers before answering. The feature was disabled and patched, and the service has been without a major incident since.

Settings and choices

Across all these platforms, people should use complex passwords, turn on enhanced security features, like the use of waiting rooms and channel moderation, and make sure conferences are restricted to intended guests. It's also important to consider what can be seen on camera, like a loan statement pinned to a bulletin board or an envelope with a home address visible. Try videoconferencing in front of a neutral wall or using blurred or customized backdrops to keep the home environment off camera.

There's still room in the market for more reliably secure, private videoconferencing systems. But in the meantime, not all communication requires the same levels of privacy and security. People might not care much if marketers or even pranksters crash their G-rated happy hours. But confidential client meetings and remote health care consultations are

another matter. The companies' offerings and track records, outlined here, should help people choose the videoconferencing tool that best balances usefulness with privacy and security.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation