Zoom’s privacy problems are growing as platform explodes in popularity

Enlarge / Zoom’s San Jose, Calif., headquarters looks like a lovely place to be socially distanced from.

reader comments

45 with 36 posters participating, including story author

Share this story

We have several more weeks, if not several more months, to go in this sudden era of Everything from Home. Work from home, school from home, funerals from home, church from home, happy hour from home—you name it, and we as a society are trying as best as we can to pull it off remotely. Tech use as a result is up all over, but arguably the biggest winner to date of the “Oh, crap, where’s my webcam” age is videoconferencing platform Zoom.

Zoom’s ease of use, feature base, and free service tier have made it a go-to resource not only for all those office meetings that used to happen in conference rooms but also for teachers, religious services, and even governments. The widespread use, in turn, is shining a bright spotlight on Zoom’s privacy and data-collection practices, which apparently leave much to be desired.

The challenge is particularly pronounced in the health care and education sectors: Zoom does offer specific enterprise-level packages—Zoom for Education and Zoom for Healthcare—that have compliance with privacy law (FERPA and HIPAA,

respectively) baked in. Many users in those fields, however, may be on the free tier or using individual or other types of enterprise licenses that don’t take these particular needs into consideration.

Growing (privacy) pains

Zoom’s privacy policy began to draw widespread attention more than a week ago for provisions about its storage and use of customer data. At the time, the platform said it would collect, store, and share with advertisers data potentially including “the content contained in cloud recordings, and instant messages, files, whiteboards” shared on the platform. That included videos and transcripts.

Amid the scrutiny, Zoom this week made some changes to that policy. “Zoom does not sell customer content to anyone or use it for any advertising purposes,” the company now says in bold, italic lettering—a welcome change, to be sure.

The privacy policy itself, though, seems to be only the tip of the iceberg. An investigation Vice Motherboard published Friday found the Zoom iOS app shared usage data with Facebook—even for users who do not have Facebook accounts. According to Motherboard, Zoom was sending Facebook data showing when the user opened the app, details about the device the app was used on, the time zone and city the user connected from, information about the mobile network the user was connected through, and a unique advertiser number used for tracking a device between apps.

Following the report, Zoom updated the app on Friday to cut off the feature, saying, “We originally implemented the ‘Login with Facebook’ feature using the Facebook SDK in order to provide our users with another convenient way to access our platform. However, we were recently made aware that the Facebook SDK was collecting unnecessary device data.”

The company is still facing a lawsuit from a plaintiff in California, however. The suit (PDF), which seeks class-action status, alleges that Zoom violated the California Consumer Privacy Act (CCPA), which went into effect on January 1, arguing Zoom "failed to properly safeguard the personal information of the increasing millions of users of its software application."

Worse, a feature meant to streamline connection for corporate users seems to be leaking some Zoom users' personal contact information. A report today, also by Vice Motherboard, found that users who sign up from the same email domain are automatically being added to each others' contact lists. For a workplace scenario, this makes sense: if two users both sign up using @arstechnica.com email addresses, odds are we work for the same employer and would need to talk to each other for work purposes. Businesses' contacts get populated into Zoom this way regularly.

Users signing up with personal email addresses, however, are *also* having their information shared with other users of the same domain. One user shared with Motherboard a screenshot showing almost 1,000 other users—all strangers to him—listed in a "company directory." Some widely used domains, including gmail.com, yahoo.com, and hotmail.com, are excluded from the company directory. Smaller domains used by individuals, though, appear not to be on the exclusion list.

Broken promises?

Zoom promises a bevy of protections for hosts who create meetings. At the top of that list is a promise that users can "secure a meeting with end-to-end encryption." That sounds pretty great! Unfortunately, it also might not be exactly true.

A report published today by The Intercept finds that the claim might be misleading. Instead of end-to-end encryption for

audio and video, Zoom offers something slightly different, called transport encryption.

When The Intercept asked Zoom about its encryption capabilities, a spokesperson straight-up responded that they can't do it. "Currently, it is not possible to enable E2E encryption for Zoom video meetings," the spokesperson said, adding, "Zoom video meetings use a combination of TCP and UDP. TCP connections are made using TLS and UDP connections are encrypted with AES using a key negotiated over a TLS connection."

If the data were truly encrypted end-to-end, only the users on either end of it would be able to access it. Under the TLS encryption it actually uses, though, Zoom itself could access the content that flows back and forth in meetings.

The company stressed to The Intercept that it does not, saying in a statement:

> *Zoom has layered safeguards in place to protect our users' privacy, which includes preventing anyone, including Zoom employees, from directly accessing any data that users share during meetings, including—but not limited to—the video, audio and chat content of those meetings. Importantly, Zoom does not mine user data or sell user data of any kind to anyone.*

If the data can be accessed, however, Zoom could be compelled to share it with government or law enforcement requests. Zoom, unlike many other technology and social media platforms, does not publish a transparency report regarding takedown and law enforcement requests it may have received.

All the reports, taken together, have drawn the attention of at least one legal authority: the office of New York Attorney General Letitia James is now investigating Zoom's privacy and security practices.

The New York Times obtained a letter from James' office to Zoom, which expressed concern "that Zoom's existing security practices might not be sufficient to adapt to the recent and sudden surge in both the volume and sensitivity of data being passed through its network." And while the company is responding quickly to specific vulnerabilities piecemeal as they become widely known through media reports, the attorney general's office "would like to understand whether Zoom has undertaken a broader review of its security practices."

"Zoom takes its users' privacy, security, and trust extremely seriously," the company said in a statement. "We appreciate the New York Attorney General's engagement on these issues and are happy to provide her with the requested information."

https://arstechnica.com/?p=1664495