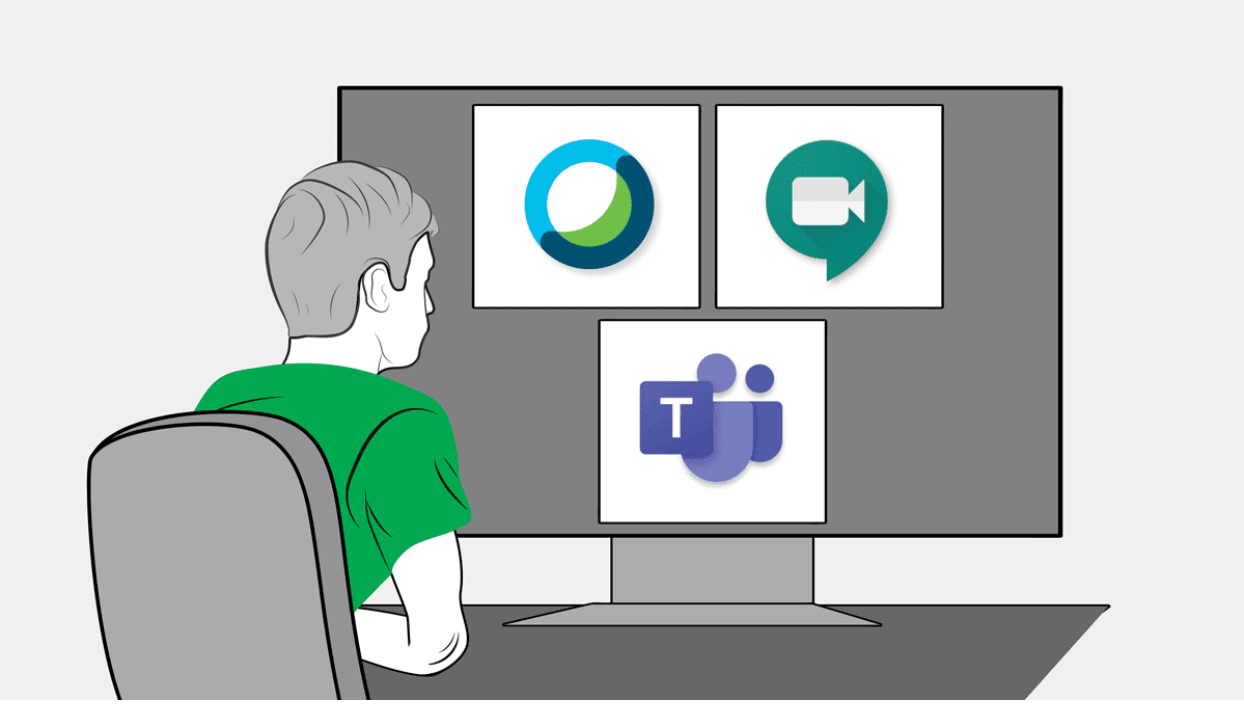
It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.

CR evaluated videoconferencing privacy policies and found these services may collect more data than consumers realize

By Allen St. John
April 30, 2020



When Pat Biswanger's family was planning to hold their Easter get-together by videoconference because of the coronavirus pandemic, her sister insisted on using Microsoft Teams instead of Zoom, because of bad press about the popular newer company's privacy and security flaws.

"My sister's smart about these things, and I was happy to go along," Biswanger recalls, but she wondered whether all videoconferencing services were equally bad on privacy. When she got together online with her grandchildren the next weekend, the Philadelphia attorney hosted it on Zoom, which she finds easier to use. However, she still wasn't quite sure which platform was safer.

MORE ON TECHNOLOGY AND THE CORONAVIRUS

Tracking Everyone With Coronavirus Is a Huge Task. Help.

How to Prevent Zoombombing

Medical Privacy Gets Complicated as Doctors Turn to Video Chats

CR's Guide to the Coronavirus

At Consumer Reports, we had the same question as Biswanger: Are there differences in how major videoconferencing platforms handle privacy?

It's an important issue at a moment, when consumers are making heavy use of videoconferencing platforms for business meetings, classes, and visits with family.

We had already looked at Zoom, which is now fixing a number of privacy and security problems. Next, we decided to evaluate the privacy policies of the biggest, best-known videoconferencing platforms.

These are Webex from Cisco; Skype and Teams from Microsoft; and Meet, Duo, and Hangouts from Google. A single privacy policy governs Google's three videoconferencing services, and Teams and Skype share the same Microsoft privacy policy.

"While there are differences among the privacy policies of the different platforms, on balance, the differences aren't enormous," says Bill Fitzgerald, a privacy researcher in Consumer Reports' Digital Lab who analyzed the documents. "And from a privacy point of view, none of these options are great."

According to their privacy policies, all three companies can collect data while you're in a videoconference, combine it with information from data brokers and other sources to build consumer profiles, and

recognition systems.

All of the companies responded to questions by Consumer Reports, saying that they respect consumer privacy without refuting our core findings. Cisco, for example, said that "privacy is a basic human right, and we never rent or sell our customers' information."

Some companies have made improvements. While we were evaluating the platforms, Google gave hosts in Meet the option to require a password to enter a meeting. That was a welcome change; until then, it was harder for Google users to secure their meetings against intruders.

Consumer Reports is writing to Cisco, Google, and Microsoft with a number of recommendations on how to improve their privacy policies, and publishing a complete report on what we found. We think the reforms we're proposing also make sense for teleconferencing platforms we haven't evaluated, from Facebook's recently announced Messenger Rooms to Houseparty, which calls itself a "face-to-face social network."

You can see more details below. But first, there are steps you can take to protect your privacy while using any videoconferencing service.

How to Stay More Private in Videochats

When you join a videoconference, you face several potential threats to your privacy and security.

One risk is a Zoombombing-style attack in which a meeting is disrupted by an intruder. There's been a lot written on how to

platforms, too.

On the privacy side, information about the call could be collected by the companies that built the platform, as well as the host or administrator of your meeting, or even by other participants. And that information can then be shared either publicly or with businesses.

Here are four strategies from CR's privacy and security experts for keeping your personal information safe while teleconferencing.

Pick a platform. For starters, see whether you can use any of these services as a "guest," to share as little information as possible. If you decide to sign up, perhaps to access more features, you can minimize your digital footprint by sticking to a single platform. That way, fewer companies are watching you. There's another benefit, too: You can become acquainted with the service's privacy and security features, and learn to use those tools more effectively.

Use outside privacy tools. This tip applies to almost anything you do online. First, if you decide to create a videoconferencing account, use a dedicated "burner" email that you don't use for anything else, or at least for important functions like banking, healthcare, and social media accounts. It's also smart to use a highly rated password manager with the platform's password function. That can help keep your meetings secure from a Zoombombing intrusion.

Assume you're being recorded. Anything you say or do in a meeting can be recorded. It can be captured officially by a host, administrator, or another participant, or just grabbed by someone with screencasting software or even a smartphone. The solution? Turn off your camera and mic whenever possible. When you do have to be onscreen, consider using a virtual or

books on your shelf, your children's toys, or art on your wall. Videos can leak into public or end up being shared with a wider circle of friends, clients, or co-workers.

Just make a regular phone call. Many meetings simply don't need video. When that's the case, pick up the phone to talk to a colleague or loop a small group into an old-fashioned conference call.

What Platforms Should Do

When CR's testers delved into the privacy policies for these videoconferencing platforms, they found that none provide much detail on what kind of data the companies collect or how they use it. And because Cisco, Google, and Microsoft are sprawling companies with many products, it's often hard to tell which policies actually apply to videoconferencing.

The privacy policies differ in the details. But, broadly, all three companies reserve the right to store information on how long a call lasts; who's on it; and everyone's IP, or internet, address. They can combine this information with personal details they get from data brokers and potentially create individual consumer profiles that are not directly related to helping anyone make a call. They can access the audio, for instance, when a host orders a transcription of a meeting and to improve their voice-to-speech technologies. And it's unclear whether they might have people spot-check video recordings to develop facial recognition or similar technologies. (Consumers have been upset to learn about this practice by security camera companies in the past.)

When we reached out to the three companies, we got a small amount of new information. Cisco emailed us a PDF, which we then hunted down to a hard-to-find location on its website. It provides a

Reports that they only record videos or generate transcripts when a participant hits Record, and that the contents are not directly used for advertising.

Justin Brookman, director of privacy and technology policy for Consumer Reports, points out that these responses came in emails to a reporter, not published promises that any consumer could look up online.

"We're more likely to trust privacy policies because they're public commitments that are enforceable by regulators," he says. "Without self-imposed restrictions, tech companies have a history of surprising consumers by collecting, sharing, and using data in expansive and disturbing ways."

Here are the best practices Consumer Reports is recommending for all videoconferencing companies.

Minimize data collection. During a videoconference, companies should store only the information needed to deliver the service. Then, they should limit how that data is shared with third parties.

Restrict how data is used for "product improvement." Videoconferencing companies should only use data they collect to develop or improve features that are clearly related to the service the user is getting. They should not use the data to develop other products unless they've first acquired clear and informed consent from users. Video and voice recordings from videoconferences should not be used for machine learning or viewed by people for product development.

Turn on the most secure settings by default. The goal is for companies to help hosts and administrators to do everything

conference and therefore has heightened access to the participant's information.