Zoom got big fast. Then videobombers made it rework security

July 1 2020, by Michael Liedtke

This April 18, 2019, file photo shows a sign for Zoom Video Communications ahead of the company's Nasdaq IPO in New York. (AP Photo/Mark Lennihan, File)

intrusive "videobombers" barged into private meetings or just spied on intimate conversations.

On April 1, following a wave of lawsuits over privacy breaches, CEO Eric Yuan ordered a halt to work on new features and vowed to fix the service's weaknesses in 90 days. That time is up, and Zoom is ready to take a bow.

The work on "security and privacy is never going to be done, but it is now embedded in how we approach everything we do at Zoom now," the company's chief financial officer, Kelly Steckelberg, told The Associated Press in a recent interview. Zoom hailed some of the strides that it says it has made in a Wednesday blog post.

The most visible changes included a switch that automatically protected all meetings with passwords and kept all participants in a digital waiting room until the meeting host let them in.

Behind the scenes, Yuan began meeting regularly with a council consisting of top security executives in the tech industry and brought in former Yahoo and Facebook executive Alex Stamos as a special consultant. He also conferred with other supportive executives such as Oracle founder Larry Ellison, who took the unusual step of posting a video hailing Zoom as an "essential service."

(Perhaps not coincidentally, Zoom relies on Oracle and Amazon for much of the computing power it needs to handle an expected two trillion minutes of meetings—the equivalent of 38,000 centuries—this year.)

The biggest security leap is still to come. Zoom has promised to make it virtually impossible for anyone outside a meeting to eavesdrop by scrambling conversations via end-to-end encryption. The technique would lock up conversations so that even Zoom couldn't play them back. Law enforcement generally opposes such encryption—already in use on apps such as iMessage, WhatsApp and others—saying it impedes legitimate police investigations.

Such a security feature would give the company an even bigger advantage over competing services from Google, Microsoft, Cisco Systems and Facebook, said Rory Mir, a grassroots advocacy organizer for the Electronic Frontier Foundation, a digital rights group.

"People don't have a lot of great options right now, but Zoom is kind of leading the charge to make these improvements," said Mir, who uses they/them pronouns.

Zoom hasn't said when end-to-end encryption will be ready, but it's already had to expand on its original plan to make it available only to paid subscribers. The day after its original announcement, faced with a backlash, Zoom agreed to extend the encryption to free plans as well.

It's been a heady ride for the company. Its shares closed Tuesday at $253.54, nearly four times their value in December, creating $50 billion in shareholder wealth. The San Jose, California, company expects paid subscribers to generate $1.8 billion in revenue for the company this year, triple what Zoom pulled in last year.

If Zoom wants to prove it puts the privacy of its users first, Mir believes it will have to show it's willing to fight requests from law enforcement and other government agencies trying to pry into the conversations on its service. The Zoom CEO has said he wanted to limit the use of end-to-end encryption so that the company could continue to work with law enforcement; the company later said he was referring to efforts intended to prevent Zoom from being used for child pornography. "Some activists now believe Zoom is like a cop," Mir said.

In a familiar refrain among tech companies operating around the world, Steckelberg said Zoom complies with local laws in each of the more than 80 countries where its service is used.

More privacy issues could loom if, as some analysts anticipate, Zoom decides to start showing ads on the free version of is service to boost its profit. Steckelberg said the company doesn't have any immediate plans to sell ads, but didn't rule out that possibility.

If Zoom goes down that road, Mir believes it will be difficult to resist the opportunity to mine the personal information it's collecting because, they said, "data is the new oil. But it also can be toxic."