

Other Tech Firms Say They Didn't Spy on Emails for Feds Like Yahoo Did

Shirley Siluk

October 5, 2016

The revelation that Yahoo might have spied on all of its users' emails on behalf of U.S. intelligence agencies underscores the need for by-default end-to-end encryption for electronic communications, according to privacy advocates. Meanwhile, other tech giants, including Google, Microsoft, Twitter and Apple, have denied receiving such surveillance requests or said they would not comply with such requests.

According to yesterday's exclusive report by Reuters, Yahoo developed custom software so it could scan "hundreds of millions" of incoming email messages for specific types of information specified by the National Security Agency (NSA) or the Federal Bureau of Investigation (FBI). It appears to be the first time an Internet service provider has searched such a large number of emails in real time for an intelligence agency, Reuters added, citing "some surveillance experts."

Yahoo's initial response to the Reuters report stated only, "Yahoo is a law abiding company, and complies with the laws of the United States." However, in a statement emailed to some news outlets this morning, a spokesperson quoted Yahoo as saying, "The article is misleading. We narrowly interpret every government request for user data to minimize disclosure. The mail scanning described in the article does not exist on our systems."

Yahoo Response 'Not Terribly Comforting'

Yahoo's "meticulously worded" follow-up statement was "not terribly comforting," Julian Sanchez, a senior fellow at the libertarian Cato Institute who closely follows "the intersection of privacy, technology and politics" noted in a tweet today. He added in a separate tweet, "What Yahoo could have easily said but didn't: 'We have not conducted such scanning. We produce content only about specific accounts.'"

Former NSA contractor and whistleblower Edward Snowden, who first revealed the widespread government surveillance of personal email and telephone conversations in a 2013 document leak to the press, also commented on the news on Twitter yesterday. "Heads up: Any major email service not clearly, categorically denying this tomorrow -- without careful phrasing -- is as guilty as Yahoo."

In the wake of yesterday's report, other technology companies have sought to distance themselves from Yahoo's alleged compliance with the intelligence surveillance request. "We've never received such a request, but if we did, our response would be simple: 'no way,'" a Google spokesperson told us today.

A spokesperson for Facebook told us, "Facebook has never received a request like the one described in these news reports from any government, and if we did we would fight it."

Other companies did not immediately respond to our requests for comment. However, BuzzFeed yesterday quoted statements from Apple, Microsoft and Twitter that suggested those companies have not taken actions similar to Yahoo's.

"We have never engaged in the secret scanning of email traffic like what has been reported today about Yahoo," a Microsoft spokesperson stated. Twitter's statement said, "We've never received a request like this, and were we to receive it we'd challenge it in a court."

"We have never received a request of this type," Apple said via a spokesperson. "If we were to receive one, we would oppose it in court." Apple earlier this year did just that after being ordered by the FBI to write special software to enable the agency to break the security of an iPhone used by Syed Rizwan Farook, who with his wife, carried out a shooting in San Bernardino in late 2015 that left 14 people dead. While Apple was fighting that order in court, the FBI eventually found a third party to break into the iPhone and dropped its case against Apple.

On the Heels of Massive 2012 Hack

If true, yesterday's report about Yahoo would mean yet another major hurdle for the company, which is currently in the process of being acquired by Verizon for \$4.83 billion. The first obstacle to that deal emerged in August, when Motherboard reported that a massive data breach in 2012 could have affected hundreds of millions of Yahoo users.

Last month, Bob Lord, Yahoo's chief information security officer (CISO), confirmed in a post on the company's Tumblr account that a suspected "state-sponsored actor" in late 2014 might have hacked information connected with at least 500 million user accounts. Noting that the company is working with law enforcement authorities, Lord urged Yahoo users to "promptly" change their passwords and security questions.

Lord replaced former Yahoo CISO Alex Stamos, who resigned in June 2015 after Yahoo's own security team discovered the company's secret email scanning software and initially believed it to be connected to a hacking attempt, according to yesterday's Reuters report. Shortly afterward, Stamos joined Facebook as CISO.

"When Stamos found out that [Yahoo CEO Marissa] Mayer had authorized the program, he resigned as chief information security officer and told his subordinates that he had been left out of a decision that hurt users' security," Reuters reported, citing comments from three unnamed former employees and a fourth source familiar with the events. "Due to a programming flaw, he told them hackers could have accessed the stored emails."

In a commentary in the Guardian yesterday, columnist Trevor Timm, who is also executive director of the Freedom of the Press Foundation, wrote, "The Yahoo story, if borne out, would be the quintessential example of how government-mandated backdoors are dangerous for everyone's security, and why end-to-end encryption needs to be standard on all our communications platforms."

"The sweeping warrantless surveillance of millions of Yahoo users' communications described in the Reuters story flies in the face of the Fourth Amendment's prohibition against unreasonable searches," Electronic Frontier Foundation attorneys Andrew Crocker and Mark Rumold wrote in a blog post yesterday. They added that Yahoo's secret software "may have, itself, opened up new security vulnerabilities for Yahoo and its users."