The Mercury News
The Newspaper of Silicon Valley

Yahoo slammed over privacy after reports of mass email scanning

Ethan Baron

October 6, 2016

In the wake of a second explosive report alleging that Yahoo scanned users' emails for a federal agency, critics are attacking the company's stewardship of customers' private information.

And a senior fellow at the Cato Institute, a think tank, warns that software Yahoo reportedly created for the real-time scanning could be used to sweep up the private communications of innocent users.

On Tuesday, Reuters reported that Yahoo secretly scanned users' incoming email in real time to comply with a demand from the federal government. Yahoo on Wednesday issued a cryptic denial, calling the Reuters story, which was based on anonymous sources, "misleading."

"The mail scanning described in the article does not exist on our systems," Yahoo said in the statement.

Later on Wednesday, the New York Times published a report alleging Yahoo had been scanning users' emails and giving the FBI copies of messages containing the digital "signature" or fingerprint associated with communications from a state-sponsored terrorist group. Yahoo, in scanning emails for the FBI, had complied with an order from the Foreign Intelligence Surveillance Court, the Times reported.

For the scanning, Yahoo created software by modifying existing programs that identify child pornography, spam and malware, according to the Times, which based its report on anonymous comments from a government official and people familiar with the matter. The data collection has ceased, the official said.

The Times report indicated that Sunnyvale-based Yahoo had been ordered to search for "code uniquely used by the foreign terrorist organization" rather than the signature of software also used by others.

But Julian Sanchez, a senior fellow at the Cato Institute, a think tank, said just because authorities say they believe the code is uniquely used by one group doesn't mean it is.

"How would you know until you do your scan and realize, 'Oops, the fingerprint we thought was unique is turning up in a lot of places — we didn't know because we weren't spying on those

other places because those users aren't terrorists,'" Sanchez said. "Most software is used by good people and bad people."

Commonly, the digital fingerprint or signature that authorities look for is related to privacy-protection software that may be used by criminals, terrorists and other bad actors — but may also be used by innocent people, Sanchez said.

"It is disturbing to think that the court has now accepted the idea that there is inherently suspicious software, and inherently suspicious privacy software, and that all you need to do to get your communications scooped up by a spy agency is to use the same kind of software."

And using a mass-scanning software architecture to comply with a government order creates a slippery slope for citizens' privacy, Sanchez said.

"(The government is) saying, 'We want to look at everyone's content so we can find out who's suspicious,'" Sanchez said. "That architecture can be used for a lot of different ideas about what's suspicious."

Coming after the news two weeks ago that it took almost two years for Yahoo to discover that hackers had stolen personal data from at least 500 million users, reports of mass email scanning by the firm drew further criticism of its treatment of users' personal data and communications.

"People just have to be more aware that your information may or may not be private, depending on the executives within an organization and their commitment to protecting your privacy," said Michael Lipinski, chief security analyst at digital-security firm Securonix.

The reports suggest Yahoo gave in to the order without a fight, and if that is the case, it "just shows where (Yahoo executives') heads are as far as their concern for people's privacy, Lipinski said.

In challenging the order, Yahoo probably would have lost because most companies do, but it still should have fought back, said Dimitri Sirota, CEO of data-protection firm BigID. "Optics matter, and I think the optics around this are that you don't feel strongly enough about the privacy of your customers," Sirota said.

Meanwhile, the head of the U.S. Cyber Command said that a "blanket look at all emails" held by a company such as Yahoo would be "illegal."

"No court would ever grant us the authority to do that," Admiral Michael Rogers said at The Cambridge Cyber Summit hosted by The Aspen Institute, CNBC and MIT.