Yahoo secretly scanned customer emails for u.s. intelligence

Business, Marketing

Yahoo Inc. last year secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U. S. intelligence officials, according to people familiar with the matter.

The company complied with a classified U. S. government demand, scanning hundreds of millions of Yahoo Mail accounts at the behest of the National Security Agency or FBI, said three former employees and a fourth person apprised of the events.

Some surveillance experts said this represents the first case to surface of a U. S. internet company agreeing to an intelligence agency's request by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time.

It is not known what information intelligence officials were looking for, only that they wanted Yahoo to search for a set of characters. That could mean a phrase in an email or an attachment, said the sources, who did not want to be identified.

Reuters was unable to determine what data Yahoo may have handed over, if any, and if intelligence officials had approached other email providers besides Yahoo with this kind of request.

According to two of the former employees, Yahoo Chief Executive Marissa Mayer's decision to obey the directive roiled some senior executives and led to the June 2015 departure of Chief Information Security Officer Alex Stamos, who now holds the top security job at Facebook Inc.

" Yahoo is a law abiding company, and complies with the laws of the United States," the company said in a brief statement in response to *Reuters* questions about the demand. Yahoo declined any further comment.

Through a Facebook spokesman, Stamos declined a request for aninterview.

The NSA referred questions to the Office of the Director of National Intelligence, which declined to comment.

The request to search Yahoo Mail accounts came in the form of a classified edict sent to the company's legal team, according to the three people familiar with the matter.

U. S. phone and internet companies are known to have handed over bulk customer data to intelligence agencies. But some former government officials and private surveillance experts said they had not previously seen either such a broad demand for real-time web collection or one that required the creation of a new computer program.

" I've never seen that, a wiretap in real time on a 'selector,'" said Albert Gidari, a lawyer who represented phone and internet companies on surveillance issues for 20 years before moving to Stanford University this year. A selector refers to a type of search term used to zero in on specific information.

" It would be really difficult for a provider to do that," he added.

Experts said it was likely that the NSA or FBI had approached other internet companies with the same demand, since they evidently did not know what email accounts were being used by the target. The NSA usually makes requests for domestic surveillance through the FBI, so it is hard to know which agency is seeking the information.

Alphabet Inc.'sGoogleand Microsoft Corp., two major U. S. email service providers, separately said on Tuesday that they had not conducted such email searches.

" We've never received such a request, but if we did, our response would be simple: 'No way'," a spokesman for Google said in a statement.

A Microsoft spokesperson said in a statement, " We have never engaged in the secret scanning of email traffic like what has been reported today about Yahoo." The company declined to comment on whether it had received such a request.

Challenging the NSA

Under laws including the 2008 amendments to the Foreign Intelligence Surveillance Act, intelligence agencies can ask U. S. phone and internet companies to provide customer data to aid foreign intelligence-gathering efforts for a variety of reasons, including prevention of terrorist attacks.

Disclosures by former NSA contractor Edward Snowden and others have exposed the extent of electronic surveillance and led U. S. authorities to modestly scale back some of the programs, in part to protect privacy rights.

Companies including Yahoo have challenged some classified surveillance before the Foreign Intelligence Surveillance Court, a secret tribunal.

Some FISA experts said Yahoo could have tried to fight last year's demand on at least two grounds: the breadth of the directive and the necessity of writing a special program to search all customers' emails in transit.

Apple Inc. made a similar argument earlier this year when it refused to create a special program to break into an encrypted iPhone used in the 2015 San Bernardino massacre. The FBI dropped the case after it unlocked the phone with the help of a third party, so no precedent was set.

" It is deeply disappointing that Yahoo declined to challenge this sweeping surveillance order, because customers are counting ontechnologycompanies to stand up to novel spying demands in court," Patrick Toomey, an attorney with the American Civil Liberties Union, said in a statement.

Some FISA experts defended Yahoo's decision to comply, saying nothing prohibited the surveillance court from ordering a search for a specific term instead of a specific account. So-called " upstream" bulk collection from phone carriers based on content was found to be legal, they said, and the same logic could apply to web companies' mail.

As tech companies become better at encrypting data, they are likely to face more such requests from spy agencies.

Former NSA General Counsel Stewart Baker said email providers " have the power to encrypt it all, and with that comes addedresponsibilityto do some of the work that had been done by the intelligence agencies."

Secret siphoning program

Mayer and other executives ultimately decided to comply with the directive last year rather than fight it, in part because they thought they would lose, said the people familiar with the matter.

Yahoo in 2007 had fought a FISA demand that it conduct searches on specific email accounts without a court-approved warrant. Details of the case remain sealed, but a partially redacted published opinion showed Yahoo's challenge was unsuccessful.

Some Yahoo employees were upset about the decision not to contest the more recent edict and thought the company could have prevailed, the sources said.

They were also upset that Mayer and Yahoo General Counsel Ron Bell did not involve the company's security team in the process, instead asking Yahoo's email engineers to write a program to siphon off messages containing the character string the spies sought and store them for remote retrieval, according to the sources.

The sources said the program was discovered by Yahoo's security team in May 2015, within weeks of its installation. The security team initially thought hackers had broken in.

When Stamos found out that 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, the sources said. Due to a programming flaw, he told them hackers could have accessed the stored emails.

Stamos's announcement in June 2015 that he had joined Facebook did not mention any problems with Yahoo.

In a separate incident, Yahoo last month said " state-sponsored" hackers had gained access to 500 million customer accounts in 2014. The revelations have brought new scrutiny to Yahoo's security practices as the company tries to complete a deal to sell its core business to Verizon Communications Inc. for $4. 8 billion.

(Reporting by Joseph Menn; Editing by Jonathan Weber and Tiffany Wu)