WIRED

How Did the Feds Get Past Yahoo's Encryption?

Andy Greenberg

October 4, 2016

Ever since Edward Snowden leaked his unprecedented collection of NSA secrets three years ago, tech firms have scrambled to protect their users from the surveillance he revealed, in many cases adding robust encryption to consumer products. But as a new email spying scandal unfolds around Yahoo, it's clear that the post-Snowden encryption push not only failed to protect the company's hundreds of millions of email accounts from American intelligence agencies. It also seems to have driven those spies to demand more pervasive access to Yahoo's systems than ever—and Yahoo complied.

On Tuesday, Reuters broke the news that Yahoo in 2015 created a tool for scanning its trove of user webmail on behalf of the FBI or the NSA, scouring hundreds of millions of arriving emails for specific search terms the agencies provided. The revelation marks the first time this sort of large-scale, real-time email scanning by a tech firm is known to have been done on behalf of surveillance agencies, and the practice reportedly led Yahoo's chief information security officer at the time, Alex Stamos, to resign over the security and privacy issues it introduced.

The spying scandal is surprising, in part, because it follows years of improvements to Yahoo's email encryption practices. And from a broader perspective, it shows how law enforcement and intelligence agencies are aggressively responding to the spread of encryption in the services provided by companies like Yahoo, Apple, and perhaps other Silicon Valley stalwarts: When surveillance operations are stymied by uncrackable crypto, they increasingly respond by demanding that tech companies perform intrusive operations themselves.

A New Prism

"The webmail providers have encrypted everything that comes to them and leaves them," explains Stewart Baker, a former general counsel for the NSA in a phone call with WIRED. "I expect that what happened here is that the government went to Yahoo and said, 'we can't find this particular target anymore, but we believe he's communicating using your servers, so we're asking you to do what we used to do when we had access to your traffic.'"

Following Snowden's NSA leaks in the summer of 2013, Yahoo in early 2014 rolled out SSL encryption to its webmail services, rendering them unreadable in transit but still unencrypted on Yahoo's servers. That new layer of security likely foiled—or at least made far more difficult—the NSA's "upstream" collection of Yahoo users' messages, its practice of silently vacuuming up communications as they passed over sources like internet switching equipment and undersea cables.

The NSA has other, more active methods of gathering those communications directly from internet firms, like its PRISM program, which legally requires companies to hand over user data. But PRISM only allows the NSA to request data from specific accounts, says Cato Institute privacy researcher Julian Sanchez, rather than the sort of phrase- or character-string-based scanning of raw data that upstream collection allowed.

Sanchez suggests that the agency may have demanded that Yahoo enable scanning of emails on its servers through the same legal mechanism as PRISM, section 702 of the Foreign Intelligence Surveillance Act. “A bunch of useful stuff shows up when you scan content that doesn’t show up in the PRISM model,” Sanchez says. “If you can’t go into content upstream, you need to retool PRISM to start scanning it.” (A Yahoo didn’t respond to a request for comment on that scenario, writing only that “Yahoo is a law abiding company, and complies with the laws of the United States.”)

The demand that Yahoo build its own scanning software on behalf of the NSA echoes the FBI’s insistence, earlier this year, that Apple help break into the encrypted iPhone 5c of San Bernadino killer Rizwan Syed Farook. In that case, the Justice Department demanded Apple write new software designed to crack its own operating system’s security.

Apple resisted, arguing that the software’s creation would potentially endanger the privacy of all of its users. The DOJ eventually backed off its lawsuit after the FBI found another way into Farook’s phone.

Yahoo, by contrast, seems to have caved to the U.S. government’s parallel legal demands, and built exactly the sort of security-compromising software that Apple refused to.

Risky Business

It’s not yet clear exactly how privacy-invasive Yahoo’s scanning on behalf of U.S. intelligence might have been. Sanchez suggests, pointing to a New York Times story last year on the NSA’s upstream data collection scanning, that the agency may be searching only for strings like the headers of messages produced by encryption tools known to used by jihadis like Mujahideen Secrets, or malware signatures. Former NSA counsel Baker argues that legally, the NSA would only be permitted to use Yahoo’s tool to gather data on foreigners. (If FBI also had access to the scanning software’s results, it wouldn’t have faced that restriction.) And Baker also argues that targeted searching of Yahoo’s data by Yahoo itself still represents only “retail” spying compared to the “wholesale” mass surveillance of upstream data collection. “If you don’t think Yahoo should be reading your mail,” he argues, “You probably shouldn’t be using Yahoo mail.”

But Yahoo’s surveillance-focused scanning still put users’ security at risk, argues Electronic Frontier Foundation attorney Nate Cardozo, as evidenced by the Stamos resignation. In fact, the scanning tool was implemented without consulting Stamos or the rest of Yahoo’s security team. And beyond Yahoo’s sloppiness in implementing the system, Cardozo argues that the NSA’s demand that a tech firm help spy on its own users represents a secret sabotage of their privacy.

“Doing this without a clear legal authorization or any debate in Congress further undermines the public trust in law enforcement and intelligence,” Cardozo says. And he says the news contradicts statements from FBI director James Comey asking for an “adult conversation” on the conflict between encryption and law enforcement. “When you’re compelling a company to

backdoor its systems without its security team's knowledge, that's not a foundation on which we can base an adult conversation."

Cardozo has warned for months that the next step in the government's battle with tech firms over encryption would be legal demands for so-called "technical assistance" under the Wiretap Act. That provision might force companies that implement strong encryption, like Whatsapp or Apple, to rewrite their own software to introduce security vulnerabilities that allow access to cops or intelligence agencies despite their use of encryption. Cardozo says there's no clear evidence that's happened yet, or that other firms have received surveillance demands like the ones Apple and Yahoo did. (A spokesperson for Google, which also SSL-encrypts its webmail, wrote only that it's never received a request to create the sort of intelligence-friendly scanning tool Yahoo built. "But if we did, our response would be simple," the spokesperson writes. "No way.")

But Baker, the former NSA lawyer, says that government demands for tech companies to help surveil their users aren't going to stop. "Law enforcement and intelligence agencies are quite confident that what they're doing is good, that it's the right thing, that it needs to be done," he says. "And if they find that technology prevents from doing it one way, they'll look for every other mechanism available to do what society has asked them to achieve."