THE CHRISTIAN SCIENCE MONITOR

Influencers: FBI should disclose San Bernardino iPhone security hole to Apple

Sara Sorcher and Malena Carollo

March 24, 2016

Now that American law enforcement may have a way into the iPhone used by the San Bernardino, Calif., shooter, it should also disclose details about the security hole to Apple, said 81 percent of Passcode’s Influencers.

The Justice Department pulled out of a much-anticipated court hearing with Apple less than a day before it was set to begin Tuesday. Law enforcement said an “outside party” presented a new way to unlock Syed Rizwan Farook’s device without Apple’s help and it is optimistic the method will work.

While the government had previously insisted there was no other way to get the potentially critical data from the iPhone without Apple writing software to bypass security features, the FBI may now face a new conundrum: Should it inform the company so it can fix a vulnerability that may affect millions of consumer devices – even if that disclosure could make it harder for law enforcement to unlock iPhones in the future?

But a strong majority of security and privacy experts from across government and the private sector, surveyed by Passcode this week, cautioned about serious security risks if investigators don’t reveal the security flaw, and the dangerous precedent it might set.

“The security of a product used by so many people – including and especially Americans – is part of national security,” said Jonathan Zittrain, professor of law and computer science at Harvard Law School. “While it is appropriate for law enforcement, with a warrant, to use a security flaw to gain access to which it is legally entitled, the flaw should be patched as soon as possible for everyone else’s sake.”

If a previously unknown security vulnerability "puts current users of those devices at risk for increased likelihood of criminal conduct such as identity theft," the FBI should inform Apple to "fulfill its law enforcement mission," said one Influencer who chose to remain anonymous. "Fighting crime isn't just about catching criminals after the fact; it's about reasonable measures to prevent avoidable criminality from happening as well." To preserve the candor of their responses, Influencers have the option to reply either on record or anonymously.

If the government has actually found a way into locked iPhones, adds Kevin Bankston, director of New America's Open Technology Institute, "Then bad guys can find it, too."

"It would be dangerously shortsighted and irresponsible for the government to stockpile that vulnerability for its own use and leave every iPhone user at risk," Mr. Bankston continued. "Indeed, this case highlights the need for the government to have a strict process in place – a process required by law – that ensures government disclosure of vulnerabilities as quickly as possible."

For its part, Apple says it would prefer the government share the details of its iPhone hack tactics if the case continues. But on Thursday, FBI Director James Comey declined to comment about whether he would tell Apple the details – and officials have so far said nothing about whether it would be subject to what's known as the Vulnerability Equities Process.

The equities review, chaired by White House cybersecurity coordinator Michael Daniel, is a relatively secretive process in which multiple agencies help determine whether security flaws in government hands must be disclosed to companies for fixing – or kept secret for national security reasons. As part of the decisionmaking process, officials consider whether keeping the vulnerabilities secret would result in significant risks to consumers, Mr. Daniel has previously explained in a 2014 blog post about how the US decides about when to disclose vulnerabilities. *(Editor's note: Daniel is also an Influencer.)*

However, the high profile nature of this case, and public knowledge that a vulnerability exists, bolsters the case for disclosure here, said Robert M. Lee, cofounder of Dragos Security.

"I'm normally for the government disclosing vulnerabilities anyway, but after publicly touting it, [the FBI has] to – as there would be potential financial impact through customer confidence issues in Apple if the FBI did not," Mr. Lee said. "In other words, the current policy is to disclose vulnerabilities anyway, but if you were going to hide one you can't do so after putting it in the press."

What's more, added Steve Weber, professor at the University of California at Berkeley's School of Information, the discussion between the government and tech sector is more important than any one security hole. "The two sides need to establish a new foundation of shared interests on which to deal with this kind of problem in the future. And the DoJ could send an important signal to Apple: it would say, ‘We believe in security as deeply as you do. We may disagree over lawful access, but that doesn’t mean we want to weaken encryption’.”

A small but vocal 19 percent minority said the US government should not tell Apple about the security hole.

“It’s Apple’s job to create the best security that it can,” said Jeffrey Carr, president and CEO of Taia Global. “It’s the government’s job to find ways, under cover of law, to break encryption for law enforcement and national security reasons. As long as both do their respective jobs, everything works as it should. Apple asking the FBI to reveal its methods is as bad as the FBI asking Apple to weaken its encryption. Both need to stay in their respective lanes.”

Ultimately, it might not be beneficial for Apple to tell them about the flaw, one Influencer said. After all, it wouldn’t be forced to create new software to bypass its own security. “If Apple’s goal is a phone they can’t open with a gun to their head – and a highly resources law enforcement agency can do it without them – do they really want to know?” one Influencer said.

While “it would be polite” to tell Apple about it, added another anonymous Influencer, it’s up to the FBI. “Lawful hacking is a technique they should be using, and they have to decide where they are in the [breach prevention] community – in it or outside of it.”

YES

“We must stop hoarding zero-days and responsibly disclose them to everyone.” - Nico Sell, Wickr

“Strong security is paramount to public safety and trust.” - Chris Young, Intel Security Group

“In a perfect world the FBI would disclose all vulnerabilities to vendors. But we don’t live in a perfect world. More generally: my guess is that Apple already knows what this vulnerability is – replay attacks on NAND Flash memory. Apple has already addressed this attack vector in their A7 and later processors.” -Matthew Green, Johns Hopkins University

“The FBI should follow the equities process, chaired by the White House cybersecurity coordinator, on whether to reveal exploits known the government.” - Peter Swire, Georgia Tech Scheller College of Business

“The US government has a policy on how it handles 0-days, unfortunately not much is known about the policy as extracting information via FOIA requests has been difficult at best. I would presume that the policy has some sort of exemption for National Security and or Law Enforcement activity. While I would love for the FBI to disclose whatever method they are using in this case I would be very surprised if they actually did so.” - Cris Thomas, aka Space Rogue, Tenable Network Security

“The government absolutely needs to inform Apple, or any company, of any security hole they discover. Failure to do so could compromise public safety, privacy and national security. Tens of millions of people use iPhones. We know that criminals, terrorists and spies are actively searching for flaws they can exploit, in order to steal information. The government has an obligation to do all it can to prevent this.” - Jenny Durkan, Quinn Emanuel

“It is irresponsible of the FBI to let a vulnerability go un-patched in a device used by millions of people around the world. Not reporting the vulnerability to Apple so that it can be patched leaves all of those users exposed.” - Amie Stepanovich, Access Now

“The role of the government should be to strengthen, not weaken, security. This means that the government should report zero-day exploits to the private sector rather than hoarding them for its own purposes. At a minimum, the FBI should release its vulnerability disclosure policy so there can be a public discussion on what responsible disclosure should look like for the government.” - Daniel Castro, Information Technology and Innovation Foundation

“The government should discretely disclose security vulnerabilities once intelligence gain/loss equities are properly considered, as well as the privacy, data security and economic implications. In this case, the chief problem was the way the Justice Department, and particularly the FBI, publicly handled the case. I’m not sure you could craft a faster way to move terrorists to foreign-made devices and open source encryption apps. The fact that they also managed to hurt US tech competitiveness in the process made this a masterpiece of incompetence.” - Chris Finan, Manifold Security

“If the FBI wants to be seen as not abusing their power to invade the privacy of US citizens, then they must turn over the vulnerabilities this outside party is exploiting to gain access to the iPhone. Any other behavior from them will confirm the fears of the American public that the US is entering a surveillance state in which privacy is no longer a right that Americans have. They will be in line policy-wise with non-Western values of freedom of expression. This road is dangerous to freedom, and will ultimately erode American technology companies' ability to compete in a global market. If users can't trust the services they use, they will turn to technologies that are safer, and that won't be subject to arbitrary, warrantless invasions of privacy." - Katie Moussouris, HackerOne

"Flaws should be fixed. It really is that simple." - Marc Rotenberg, Electronic Privacy Information Center

"Security is a shared responsibility. How can government officials expect to be trusted if they don't do their part?" - Influencer

"With the caveat that the FBI does not need to give out full information on how it gets in, but enough for Apple to fix vulnerabilities." - John Pescatore, SANS Institute

"The Bureau is a consumer of Apple goods as well as an LEA. They'll want the flaw remediated for their own users as well as law-abiding citizens." - Scott Montgomery, Intel Security

"Security is hard enough without your government refusing to assist and actually treating you like an adversary. The US government should be helping Apple increase its security, not becoming a threat to it." - Cindy Cohn, Electronic Frontier Foundation

"Trust must be a two- way street and law enforcement and government agencies have as great a duty to collaborate and share sensitive information as vendors of technology products." - Influencer

"Maybe it should, it certainly won't with all but the most extraordinary flaws. If you want bugs to get fixed you need organization's not rewarded by them." - Dan Kaminsky, White Ops

“Known security exploits should always be reported. The FBI would otherwise be doing an end run on the legal controls that are in place to limit law enforcement access to data.” - Influencer

“Yes, but only if Apple pays them a bug bounty.” - Influencer

“It doesn’t matter whether it’s the FBI or the NSA – closing security holes makes us all safer and should be a standard practice for the US government.” - Sascha Meinrath, X-Lab

“Current US law doesn’t seem to recognize an obligation on the part of law enforcement to prevent loss before-the-fact, so it isn’t clear that the FBI would have a legal obligation to do so. That having been said, if the FBI recognized that a bank had a back door that didn’t lock, one would hope that they would notify the operators about the vulnerability. Given that there are quite a few people in the FBI investigating ‘cybercrime’ these days, it would seem to be within their mission to let a vendor know about something like that.” - Influencer

“It’s standard good security practice to disclose vulnerabilities. The FBI should also explain whether it deliberately misled the court about the necessity of compelling Apple to help break the security of its devices or didn’t make a serious effort to explore the alternatives, which amounts to the same thing.” - Jim Harper, Cato Institute

“It is best overall for the good of the majority of people that their communications be protected.” - Influencers

NO

“Apple can’t have it both ways. Either it is going to cooperate with legitimate law enforcement demands, or it can suffer the consequences.” - Influencer

“It is unlikely that the FBI has any new vulnerability information about the iPhone. There is a publicly disclosed technique that a vendor may have offered to perform, which involves copying the flash memory on the phone. In general, law enforcement and intelligence agencies face difficult tradeoffs with respect to vulnerability information that they possess. These agencies use vulnerabilities to collect intelligence, but if they fail to disclose them, they may miss an opportunity to prevent attacks in the event that the vulnerabilities are independently discovered by a malicious third party. The risks are heightened in the scenario where exploiting a vulnerability requires sending payloads to the target that contain vulnerability information, which the target might recover and use to launch their own attacks. Therefore, agencies must carefully balance the opportunities presented by a vulnerability against the infrastructural risks associated with holding on to them and using them. It’s reasonable to have concerns about this balancing process, because the decisions are opaque to the general public, and the risks are an externality to the agency’s mission, and therefore may be underestimated.” - Tom Cross, Drawbridge Networks

“If Apple’s goal is a phone they can’t open with a gun to their head - and a highly resources law enforcement agency can do it without them - do they really want to know? Why is law enforcement obliged to help Apple close off an important access point for them?” - Influencer