Voice of America

February 18, 2016

FBI-Apple Standoff Was Years in the Making

by Doug Bernard

If the FBI and the tech industry had been looking for a near-perfect test case to establish the limits — if any — of encryption, it now appears they've found what they're looking for.

This week, U.S. District Judge Sheri Pym ruled that engineers at Apple must help the FBI gain access to a locked iPhone by creating a custom bit of code that would break Apple's proprietary auto-destruct security system. In response, Apple CEO Tim Cook called the ruling "chilling" and said his engineers would not comply. The company is expected to appeal the ruling.

The FBI believes it has the legal upper hand for two reasons. First, the phone was allegedly used by Syed Farook, one of the two shooters who carried out last year's terror attack in San Bernardino. That makes it at least possible the iPhone could contain contacts, images or other data that might help the ongoing federal investigation of the attack.

And second, Pym's ruling is limited and specific, addressing only one phone already in the FBI's possession, which is also owned by San Bernardino County, where officials have granted consent for the phone to be searched.

On the other side, Apple and a coalition of tech companies and privacy advocates call the ruling unprecedented both for its scope and its potential applications. They say that for the first time, the U.S. government is ordering a corporation to intentionally destroy proprietary security features that will open a massive hole on all its products that hackers will exploit.

Worse yet, they argue a victory for the FBI will establish precedent for governments around the world who want to spy on their citizens to simply order companies to help, potentially putting millions at risk for punishment, prison or worse.

Whatever the outcome, this much is clear: The standoff between Apple and the FBI is unlikely to be resolved soon. In the meantime, the debate over encryption and national security in the U.S. may now move from the back burners to the center of national dialogue.

Big deal — for whom?

"It's clear that it's desirable for the FBI to always try to find out information for investigations," said Ed Black, CEO of the Computer and Communications Industry Association. "Our industry has a huge history, in many, many ways, of cooperating extensively with legitimate law enforcement undertakings."

The problem, Black said, is that what the FBI is asking for in this case would create a "model" that could very well weaken the overall privacy and security of the global Internet and the digital world.

"We understand what they want and why they want it," Black told VOA. "Law enforcement always wants as much information as it can get. But what they want here has the precedent of being used in many ways in the future that we think would cause overall harm to the security of the Internet."

Black credited industry innovation with giving police a "more powerful array of investigative tools" than at any other time in history. However, he said that governments should not always get "100 percent of what they want," and they definitely should not be ordering a company to write what he called "malware" that would intentionally make its own products less secure.

Alan Berman agreed that a final ruling in the case, at whatever court level, might set a huge precedent, but for reasons opposite of Black.

"FBI wins, no big deal," Berman said. "Apple wins, big deal."

Berman is president and CEO of the Disaster Recovery Institute, an organization that assists in disaster recovery, cyber or otherwise. He argued that the court ruling was tightly constructed and focused.

“It’s highly technical and specifically focused on this one phone, and a one-time modification that doesn’t even touch Apple’s encryption,” he said.

Berman pointed out that Pym’s order does not force Apple to break its own encryption technologies. The court, he said, is merely requesting Apple’s help in deactivating an iPhone security feature known as “auto-erase”; namely, if someone tries to use the wrong passcode to unlock the phone more than 10 times, all data on the phone are destroyed, and the action is irreversible.

“They’ve been very big into security; this is very consistent with their approach to security and privacy,” Berman told VOA. “Auto-erase? Invented by Apple. The ability to erase your phone remotely? Apple. I’m actually surprised that anybody thought that Tim Cook would have said anything other than what he did.”

“The real chilling effect,” Berman said, "is you may set a precedent where law enforcement will never be able to get to these locked devices. A win [for Apple] means no one would ever be able to do this again, and these things could go dark forever."

'A very dark place'

FBI Director James Comey has made access to encrypted devices a high priority. Since Apple and Google announced they were making encryption a standard option on their devices, Comey has publicly warned that encryption is creating “millions of unbreakable safes” that threatened “to take us to a very dark place.”

His office has been working with tech companies to craft some sort of emergency access protocol, whereby law enforcement officials conducting a legitimate investigation could ask a court for a subpoena to decrypt the device. Those efforts have largely failed.

While Apple is not a member of the Computer and Communications Industry Association, many tech giants such as Google are, and increasingly they’re lining up in support behind Apple.

Shortly after Cook announced that his company would not comply with Pym’s order, Google CEO Sundar Pichai took to Twitter to announce his firm’s support for Cook.

“We build secure products to keep your information safe and we give law enforcement access to data based on valid legal orders,” he wrote. “But that’s wholly different than requiring companies to enable hacking of customer devices & data. Could be a troubling precedent.”

Marc Rotenberg, president of the Electronic Privacy Information Council, is a leading national advocate for digital privacy. He said the court order was unusual in several respects, in part because Pym based her ruling on a 227-year-old measure called the All Writs Act, which is almost never invoked today.

"It’s not a simple request and it’s not a limited request," Rotenberg said. "It’s not just that one phone that becomes broken, it’s every single Apple 5c iPhone that the government could open, because the patch becomes like a master key for all iPhones."

False promise of success

While decrypting devices used by suspected terrorists may sound like a good idea, Rotenberg said it’s probably a false promise of data access.

"What if you have a secure communications app overlaying on top of the Apple operating system?” he told VOA. “That will also be encrypted. Apple won’t have control over those keys, so the FBI will still be facing a locked door. This is why it’s so very important to understand the very significant downside when the government makes these kinds of requests. There’s no guarantee of success.”

An even larger downside for both Rotenberg and the CCIA’s Black is the precedent a successful FBI ruling might mean around the world.

"The precedent of asking a tech company to break a privacy feature on behalf of the government [makes] it very difficult for the U.S. government to argue that any other government shouldn’t do the exact same thing,” Rotenberg said. “The Chinese, the Russians, all of them would love to be able to say to service providers, ‘We have a serious investigation. We need your help. Please break the device.’ "

http://www.voanews.com/content/federal-bureau-investigation-apple-standoff-years-in-making/3197134.html