theguardian

Inside the FBI's encryption battle with Apple

Danny Yadron, Spencer Ackerman and Sam Thielman

February 18, 2016

Two weeks ago, the FBI called Apple's headquarters in Cupertino, California, with a jarring message: the agency wanted Apple to help them hack an iPhone. Apple refused.

The request stepped up a level on 16 February when a federal magistrate ordered Apple to help the FBI unlock a single iPhone – the phone belonging to one of the killers in the December mass shooting in San Bernardino, California. Apple again refused.

But this carefully planned legal battle has been months in the making, US officials and tech executives told the Guardian, as the government and Apple try to settle whether national security can dictate how Silicon Valley writes computer code.

Apple chose to protect a dead Isis terrorist's privacy over the security of the American people

Senator Tom Cotton

Both sides expect the ensuing legal battle to have far-reaching implications that will touch on encryption, law enforcement, digital privacy and a 227-year-old law from America's post-colonial days.

"The law operates on precedent, so the fundamental question here isn't whether the FBI gets access to this particular phone," said Julian Sanchez, a surveillance law expert at the libertarian-leaning Cato Institute in Washington. "It's whether a catch-all law from 1789 can be used to effectively conscript technology companies into producing hacking tools and spyware for the government."

Apple and the government, observers and people close to the case said, want to set a legal precedent about where digital security ends and national security begins after nearly two years of hearings, open letters and Washington-Silicon Valley shadowboxing. Speculation has already begun about how far both sides are willing to go in appealing unfavorable rulings.

The politics are tricky. Apple is popular and code is protected by America's free-speech law. Privacy advocates planned to gather at Apple stores across the US in support of the iPhone maker.

On the other hand, one technology executive Wednesday acknowledged, “it’s an incredibly sympathetic case” from the governments’s perspective.

“Apple chose to protect a dead Isis terrorist’s privacy over the security of the American people,” Senator Tom Cotton of Arkansas wrote in a statement.

Apple CEO Tim Cook said in a impassioned statement: “We have no sympathy for terrorists. But now the US government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.”

The House judiciary committee plans to hold a hearing on the matter 1 March and has invited Apple, a person familiar with the matter said.

Apple introduced enhanced encryption in 2014

Apple’s actions in this case require some context. In September 2014, Apple introduced new encryption into its iPhone operating system that would make it mathematically impossible for the company to unlock them for investigators. This was a departure from the past, when investigators could get access to a device if they sent it to Apple headquarters with a search warrant.

The shift was in response to increased digital privacy concerns and distrust of America’s digital spies following revelations from former National Security Agency contractor Edward Snowden.

Since then, FBI director James Comey has been trying to figure out a way around the software as he and Apple’s Cook have traded barbs publicly and privately. Comey hit a snag, however: the Obama administration didn’t want to pick a fight with one of America’s most popular – and valuable – companies.

In October 2015, the director abandoned his push for legislation that would require Silicon Valley to maintain some sort of way to unlock smartphones and inboxes for investigators. Since then, the Obama administration has sounded notes of cooperation, sending officials to Silicon Valley for what they billed as an air-clearing discussion. Comey’s later rounds of rhetoric focused on mutual interests in safety and privacy felt in Washington hearing rooms and Palo Alto boardrooms.

But their tones have shifted in the past week. Comey testified on 9 February that the FBI was unable to unlock the San Bernardino iPhone. His NSA counterpart, Adm Michael Rogers, called encryption “foundational to the future” in a January appearance, but said on 17 February that the terrorists who killed about 130 people in Paris in November would not have been successful had security agencies penetrated their encrypted communications.

In the meantime, Justice Department lawyers believed they had found another way into a locked iPhone. The All Writs Act, passed in 1789, gives judges broad authority to ensure their orders are fulfilled. Justice Department lawyers believed it would provide an underpinning for forcing companies to grant them access, sources said. But some of the test cases that involved modern

technology companies were either low profile or didn't fit the right set of circumstances to set a precedent.

Apple lawyers, regardless, began studying the law and preparing counter-arguments after these initial test cases. The law, they argued, can't be used to force a company to rework how it makes products.

And then came San Bernardino

On 2 December a husband and wife opened fire on a local government office building in southern California. The FBI quickly said the two suspects, who both practiced Islam, had been "radicalized" and declared the incident a terrorist attack.

One of the suspects, Syed Farook, had worked for the county, which meant the government owned his iPhone 5C. With a search warrant, Apple provided the FBI data from weekly backups Farook made with Apple's iCloud service. But those backups stopped on 19 October, according to a federal search warrant request.

FBI investigators believed there was more data about Farook's motives in the phone but couldn't get to it without unlocking the device. The phone's contents were encrypted and Apple didn't have the four-digit passcode. Modern iPhones also have an optional feature that will erase all data on the phone with 10 incorrect passcode entries. FBI agents weren't willing to take the risk.

So FBI lawyers came up with a clever request for Apple: don't turn off the encryption – just make it easier for agents to guess the password as many times as they wanted.

Eileen Decker, the US attorney for the central district of California, took the lead on the case, supported by the Justice Department's national security division in Washington. In their view, the access they sought was narrow and didn't rely on undermining encryption standards. This model of phone, the 5C, did not run Secure Enclave, Apple's newer and more robust encryption measure, leaving department officials convinced that they could hive off the heart of the "backdoor" debate from the specific San Bernardino case.

In the 16 February court order, Apple was told to build software that, when combined with the unique identification number, would allow the FBI to guess Farook's password as many times as it wanted. The court also ordered Apple to disable a feature that added a delay after multiple incorrect passcode entries. And since a four-digit passcode has only about 10,000 possible combinations, a powerful computer could plow through guesses fairly quickly, a technology executive said.

US officials on Wednesday stressed that their request for Apple is only limited to Farook's phone. "The judge's order and our request in this case do not require Apple to redesign its products, to disable encryption or to open content on the phone," the Justice Department said in a statement on 17 February.

But Apple said that it would be impossible to limit the technology to this case. Once Apple built such an investigative tool, any iPhone's security system – even the most modern ones – could be weakened by it, an Apple executive said. Dan Guido, co-founder of security analyst Trail of Bits, called such a system, "FBiOS", a riff on Apple's smartphone operating system iOS.

Additionally, Apple's lawyers are concerned that if a judge validates the FBI's use of the All Writs Act in this case, it will give the government sweeping authority to dictate how Silicon Valley builds products in the future.

"We are challenging the FBI's demands with the deepest respect for American democracy and a love of our country," Cook wrote in his letter. "We believe it would be in the best interest of everyone to step back and consider the implications."

If the FBI succeeds, it could be a 'troubling precedent'

To Justice Department officials, San Bernardino is a long-awaited test case. In October 2014, the FBI's James Comey first told a Washington audience that encryption on mobile devices effectively left law enforcement "dark" to emerging threats. Ever since, officials believed it was only a matter of time until they came upon a case like the San Bernardino shootings: a device from a terrorist whose lock screen they couldn't bypass by guesswork to get at the data held on the phone, and not in Apple's iCloud.

"This wasn't a fluke they picked this one," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies who advises technology companies and the government on encryption. "They're always strategic in how they do these things."

Both sides are gaming out how far their legal strategies will go. Amid speculation that the case is sure to reach the supreme court, litigation is almost certain. There are precedents for the Justice Department backing down: in 2012, it chose not to challenge a decision by the 11th circuit court of appeals in Atlanta that it could not compel a suspect in a child abuse image case to decrypt his hard drives, something it considered crosswise with the fifth amendment's protections against self-incrimination.

Senior law enforcement officials were briefed on the decision to go after Apple in such a high-profile way, sources said. The FBI also appears to have been preparing its press strategy for the search warrant for weeks. They expected Apple to push back heavily: Cook, who has managed threats from China to force decryption of the iPhone, had taken unyielding stances against backdoors, both in the US and overseas, where a host of foreign countries are debating or have passed measures to give their security services access to customer data from Apple and other firms.

US law enforcement officials were less concerned about the precedent they were setting for foreign governments than in the task at hand: compel Apple to allow them to unlock the phone.

At a closed-door January meeting with national security officials in San Jose, Cook urged the Obama administration to make a public statement in support of strong encryption. That statement was never made.

But on Wednesday night, Google chief executive Sundar Pichai posted several messages on Twitter backing Apple.

Giving law enforcement officials occasional access to user data is “wholly different than requiring companies to enable hacking of customer devices & data”. If the bureau succeeds, it “could be a troubling precedent”.