In legal showdown, FBI vs. Apple could make or break Silicon Valley

Zack Whittaker

February 18, 2016

It was the apocalyptic ruling that many in security circles thought was possible, but would never happen.

A California magistrate judge handed down an order Tuesday, invoking a 230-year-old law, ordering Apple to punch a hole in the security of its own product, a ruling the company said it will oppose.

The FBI scores a game-changing win in the battle between tech firms and law enforcement over device access, setting legal precedent that may never be undone.

Judge Sheri Pym said Apple must assist the FBI in its efforts to unlock an iPhone belonging to Syed Farook, one of the shooters in the San Bernardino attack in December.

The attacker's device, like more than nine-out-of-ten modern iPhones, is encrypted with a passcode. Apple introduced the encryption in response to the Edward Snowden disclosures so that even it has no way to unlock the device without the passcode. After a number of failed unlock attempts, the phone will erase all of the user's data.

The judge, knowing Apple can't beat the encryption, instead ordered the company to write new software that would allow federal agents to beat the security feature that erases the phone's data.

Apple's bid to shut itself out of the encryption loop was precisely to avoid the kind of ethical dilemma that would force it into handing over customer data to the authorities.

The order was unexpected, landing late in the day in California. Apple chief executive Tim Cook said in an open letter hours later that the order was "unprecedented... which has implications far beyond the legal case at hand." Federal prosecutors noted in a memo alongside the order that the software would only affect Farook's iPhone. but Cook disagreed. Referencing comments he has previously made, Cook said the move would "undeniably create a backdoor" to its software, widely seen as an effort by the FBI to unravel more than two years of the tech giant's counter-surveillance efforts.

It was a *de facto* declaration of war against not just the tech titan, worth more than half-a-trillion dollars in market size, but the US tech industry.

Where once the government sought a civil, reasonable solution to its issues with encryption, Tuesday's legal showdown is a rapid escalation from publicly traded barbs between tech firms and law enforcement -- one that the government will struggle to back down from.

Old Law, New Tricks

The 40-page court order said Apple must provide "reasonable technical assistance" to the FBI.

After Snowden documents showed how the law allowed a massive scope of bulk surveillance, everyone forgot about a little-known law from the 18th century that courts still had at their disposal.

Apple tells judge 200-year-old law can't unlock iPhones

But the company said it has the "technical capability" to extract data in one-in-ten iPhones.

The All Writs Act is designed to gives a court the "authority to issue [orders] that are not otherwise covered by statute," so long as the request is not impossible. A court forcing Apple to reverse its encryption would be "substantially burdensome," but asking it to remove the feature that prevents the phone from erasing after ten failed passcode attempts is not.

Dan Guido, a respected security researcher, said on his blogthat he believes all of the FBI's requests are "technically feasible."

Cook didn't say in his letter whether the court order was possible, but hit back with a hard truth. "The government is asking Apple to hack our own users," he said in an open letteron Apple's website. (We have more on the specifics of how Apple must comply.)

Guido said that the FBI wants Apple to create a "special version of iOS" that only works on the iPhone 5c that belongs to the terrorist. Apple has to sign the custom version with its own secret keys, which "is why the FBI cannot load new software onto an iPhone on their own."

But Cook said the US government has "asked us for something we simply do not have, and something we consider too dangerous to create."

It's a nicer way of saying that the FBI is asking Apple to blow up its own backyard, or clean up the splatter from its own assassination -- a move that now that it's public may harm Apple's public image of privacy-mindedness.

"Troubling Precedent"

This case will snowball. There's a broad consensus that if this can happen to Apple, what's stopping it from happening to any other company?

The government invoking All Writs Act could set, in Cook's words, a "dangerous precedent" down the line. That's because "coding is not burdensome," the government says, according to Andrew Crocker, a staff attorney at the Electronic Frontier Foundation.

"This isn't about one iPhone. If this precedent gets set it will spell digital disaster for the trustworthiness of any and every device."

— Kevin Bankston, Open Tech Institute

Kevin Bankston, director of the Open Tech Institute, said in a tweet: "This isn't about one iPhone. If this precedent gets set it will spell digital disaster for the trustworthiness of any and every device." He added that, "potentially any software vendor could be forced to update any device with malware."

That echoed similar comments by Apple's external counsel Marc Zwillinger, a national security attorney, who wrote in an electronic filing days earlier regarding a similar case, that Apple has been advised that "the government intends to continue to invoke the All Writs Act in this and other districts in an attempt to require Apple to assist in bypassing the security of other Apple devices in the government's possession."

Kicking down the door to one tech giant is going to leave other companies at risk. An attack on one is an attack on all is a sentiment shared by many in security circles. After all, Apple wasn't the only company named on the leaked PRISM documents. AOL (now owned by Verizon), Facebook, Google, Microsoft, and Yahoo were also implicated.

Yet none of those thrown under the PRISM bus gave explicit or direct support for Cook's message by the end of Wednesday.

Sundar Pichai, chief executive of Google, which began to add device encryption by default to newer versions of its Android operating system, in a series of tweets on Wednesday called for "a thoughtful and open discussion on this important issue." Pichai fell short of demanding an end to the FBI's offensive, but did say that hacking of devices could set a "troubling precedent."

That's where Pichai was right -- it's the "precedent" that makes the case going forward so striking.

Christopher Soghoian, principal technologist at the American Civil Liberties Union, said the government is "desperate to establish" the legal case, rather than just hack the iPhone on its own.

The government isn't just assaulting encryption and security; it's fundamentally chipping away at the trust that many of these companies have needed to rebuild in the wake of the Snowden leaks. Billions have already been lost in foreign investment because of the NSA revelations.

Undermining that trust further will only alienate one of the world's economic powerhouses.

Congress May Wade In

Despite the damage already caused to confidence in the tech sector, the government is unlikely to back down without a fight.

Congress has already waded into the encryption battle on a state-by-state basis, and may have to expand its scope to a federal level. But any legislative fix that would override the courts may not come this side of the election. And any proposed law could be as decisive and as partisan as the very real-world encryption battle it's trying to fix.

After a number of failed unlock attempts, Farook's phone will erase its data. (Image: file photo)

Rep. Ted Lieu, the author of a new draft bill that would prevent states from enacting anti-encryption legislation, and one of just four computer science majors in Congress, commented that tech companies "are not, and should not be, an arm of government or law enforcement," in an emailed statement. "This precedent-setting action will both weaken the privacy of Americans and hurt American businesses," said Lieu.

Rep. Zoe Lofgren (D-CA, 19th), a congresswoman whose district covers much of Silicon Valley and privacy advocate, said in a statement that Congress could wade in to legislate.

Even that would be hotly contested. Sen. Dianne Feinstein (D-CA), the former chair of the Senate Intelligence Committee and vocal proponent of the intelligence agencies, said live on CNN that she would draft a bill forcing Apple's hand.

Lofgren noted that tech companies would have "no choice" but to further lock down systems that were exploited by the FBI, a trend that could continue until members of Congress draft and pass laws that bar tech companies from adding backdoors -- willingly or otherwise.

That could lead tech companies down a game of security one-upmanship.

"If you make the system more secure, what you may be doing as a company is increasing the burden on yourself down the road if the government is going to order you to break it later," said Julian Sanchez, a senior fellow at the Cato Institute, speaking to the Washington Post.

Others have warned that other countries are carefully watching how the FBI's assault on Apple pans out.

"This move by the FBI could snowball around the world," said Sen. Ron Wyden (D-OR), a member of the Senate Intelligence Committee. "Why in the world would our government want to give repressive regimes in Russia and China a blueprint for forcing American companies to create a backdoor?"

If you're content with the US government dictating the iPhone's encryption, "ask yourself how you'll feel when China demands the same," said Matthew Green, a cryptographer and Johns Hopkins professor, in a tweet.

Uncertain Times Ahead

Congress moves slowly. A bill could land on the desk of the incoming president, only to be trashed. None of the contenders in either party have so far lent their support to embattled Apple.

Republican nominees unanimously scolded the company. The party's presidential front-runner Donald Trump said unlocking the phone is "common sense," reports Reuters. Sen. Marco Rubio said Apple should be a "good corporate citizen," a statement nudging Apple towards compliance.

Apple is expected to appeal in the coming days. The case has a way to go, and may end up in the hands of the Supreme Court.

US tech companies will be eagerly watching the case unfold. Apple, backed into a corner by the feds, is in unchartered, hostile waters. What was the darling child of Silicon Valley is now a prisoner in its own country, forced to comply with an order that would undermine its core values. What long-term effect this will have on US tech titans remains to be seen, but undermining trust could see an economically catastrophic exodus from the US to safe havens where security is treated as a matter of constitution.

Welcome to the "most important tech case in a decade." It's one that Apple can't afford to lose, and one the FBI shouldn't be allowed to win.