Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks

By Ellen Nakashima February 17, 2016 at 9:42 AM, Washington Post

Tech giant Apple and the FBI appeared headed for a deepening confrontation Wednesday after the company's chief pledged to fight federal demands to help mine data from an iPhone used by one of the shooters in December's terrorist attacks in San Bernardino.

The clash reflects wider debates in the United States and elsewhere over security measures used by companies to protect users of devices such as smartphones — and how much leverage authorities should have to gain special access.

"We have great respect for the professionals at the FBI, and we believe their intentions are good," Apple chief executive Tim Cook said in a strongly worded open letter posted late Tuesday on the company's website.

"Up to this point, we have done everything that is both within our power and within the law to help them," it continued. "But now the U.S. 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 Justice Department sought the order "in the hopes of gaining crucial evidence" about the Dec. 2 shooting rampage, which killed 14 people and injured 22.

The order, signed Tuesday by a magistrate judge in Riverside, Calif., does not ask Apple to break the phone's encryption but rather to disable the feature that wipes the data on the phone after 10 incorrect tries at entering a password. That way, the government can try to crack the password using "brute force" — attempting tens of millions of combinations without risking the deletion of the data.

The order comes a week after FBI Director James B. Comey told Congress that the bureau has not been able to open the phone belonging to one of the killers. "It has been two months now, and we are still working on it," he said.

The Silicon Valley giant has steadfastly maintained that it is unable to unlock its newer iPhones for law enforcement, even when officers obtain a warrant, because they are engineered in such a way that Apple does not hold the decryption key. Only the phone's user — or someone who knew the password — would be able to unlock the phone.

The FBI's efforts may show how impervious the new technology is to efforts to circumvent it. According to industry officials, Apple cannot unilaterally dismantle or override the 10-tries-and-wipe feature. Only the user or person who controls the phone's settings can do so.

However, U.S. Magistrate Judge Sheri Pym said in her order, Apple can write software that can bypass the feature. Federal prosecutors stated in a memo accompanying the order that the software would affect only the seized phone.

Who was involved in the San Bernardino attack?

In the statement, Cook said such a step would dangerously weaken iPhone security.

“Once created,” he wrote, “the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.”

The Apple CEO said that “opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.”

The phone, an iPhone5C, was used by Syed Rizwan Farook, who with his wife, Tashfeen Malik, opened fire at a holiday party at the Inland Regional Center, a county facility. The couple, who pledged loyalty to the Islamic State terrorist group, died a few hours later in a shootout with police.

FBI investigators recovered a number of electronic devices, including thumb drives, computer hard drives and Farook’s cellphone. His phone belonged to the county public-health department, where he was an inspector. Prosecutors noted that the county consented to allow the phone to be searched and to have Apple’s assistance in the matter.

Data that would be encrypted on the device includes contacts, photos and iMessages. Having access to that material could shed light on why the couple picked the target they did, whether they were planning other attacks and whether they received any direction or support from overseas.

FBI Supervisory Special Agent Christopher Pluhar stated in a declaration that he was able to obtain from Apple all the data backed up to its iCloud servers from the phone. That data showed that Farook was in communication with individuals who were later killed. Significantly, Pluhar said, the most recent backup took place on Oct. 19, 2015, indicating that Farook may have intentionally disabled the backup feature.

Pluhar, who is director of the Orange County Regional Computer Forensics Laboratory, said he believes there may be “relevant, critical communications and data” on the phone from around the time of the shooting. Former National Counterterrorism Center director Matt Olsen, who recently co-authored a paper that asserted that the government had other ways to obtain data without creating a backdoor into devices, said the public interest in this case supports the government getting access to the data.

“This is the kind of case where companies like Apple need to demonstrate that they’re good corporate citizens and comply with lawful court orders,” said Olsen, who was also a general counsel at the National Security Agency.

But Kevin Bankston, director of New America’s Open Technology Institute, said what the court is ordering Apple to do is “custom-build malware to undermine its own product’s security features.” He said it is not clear whether Apple can do that technically. But if a court can compel Apple to do it, then it can compel other software providers to do so as well.

“This isn’t just about one iPhone, it’s about all of our software and all of our digital devices,” he said. “If this precedent gets set, it will spell digital disaster for the trustworthiness of everyone’s computers and mobile phones.”

The phone ran on Apple’s iOS 9 operating system, which was built with default device encryption. When a user creates a password, that phrase generates a key that is used in combination with a hardware key on a chip inside the phone. Together, the keys encrypt the device’s data.

If the autowipe function is suspended, the FBI can run a massive number of combinations of letters, symbols and numbers until the right combination is found.

But there’s a complication.

If the combinations are run on the phone itself, the process can be painfully slow, taking, according to Apple, 5 ½ years for a six-digit lower-case password mixing numbers and letters.

If run on a supercomputer, it can be done many thousands of times faster. But to do it that way, the FBI would need the hardware key, which is built into the phone. Apple says it does not keep a copy of that key. To get that key, one could use a number of techniques, including melting the plastic off the chip and hitting it with bursts of lasers or radio frequencies to recover bits of the key.

Matthew D. Green, a cryptography expert at Johns Hopkins University, said the FBI could crack a six-digit numeric code in about 22 hours.

“But once there’s numbers and letters, that’s when things get interesting,” he said. “It might take 10 years to crack a strong password on the phone, which means they might be stuck till 2026.”

The government requested the order under the All Writs Act, a law dating to the colonial era that has been used as a source of authority to issue orders that are not otherwise covered by a statute. Though Apple has previously complied with court orders under that statute to retrieve data from iPhones running earlier versions of its operating system, it is now resisting such an order in a separate iPhone case in Brooklyn. That case, unlike the one in California, involves a phone with software that allows the firm to extract data.

The government contends that courts over the years have issued orders based on that law for the unencrypted contents of computers, for credit card records and for security camera videotapes. It noted that the Supreme Court in 1977 held that the law gave courts the authority to direct a phone company to execute a search warrant for numbers dialed by a particular customer.

Some legal scholars, however, said the use of the All Writs Act in the California Apple case presents a slippery slope issue. “If the writ can compel Apple to write customized software to unlock a phone, where does it end?” said Ahmed Ghappour, a professor at the University of California’s Hastings College of the Law. “Can the government use it to compel Facebook to customize an algorithm that predicts crime? It’s not clear where the line will be drawn, if at all.”

Apple has another friend in its fight against the FBI.

CNN, February 18, 2016: 1:42 PM ET

Google CEO Sundar Pichai has come out in support of Apple, which is fighting an order to help the FBI break into the iPhone owned by one of the San Bernardino shooters.

While acknowledging law enforcement faces "significant challenges" to protect the public, Pichai voiced his support for Apple CEO Tim Cook in a series of tweets.

"Forcing companies to enable hacking could compromise users' privacy," Pichai said in the first of five tweets.

Pichai said that while Google gives "law enforcement access to data based on valid legal orders," that's different than requiring companies to hack devices.

In an earlier public letter, Cook called the government's order "an overreach." Cook warned that complying would entail building "a backdoor to the iPhone" -- "something we consider too dangerous to create."

Pichai isn't alone in his support for Apple. Ex-NSA contractor Edward Snowden, who kicked off the privacy debate, came out in defense of Apple Wednesday.

"The FBI is creating a world where citizens rely on Apple to defend their rights, rather than the other way around," Snowden tweeted.

Before Pichai commented on the issue, Snowden was critical of Google's silence.

"This is the most important tech case in a decade. Silence means @google picked a side, but it's not the public's," he tweeted.