APPLE TO FIGHT COURT ORDER

Tech giant refuses to help unlock iPhone of shooter in San Bernardino terror attack

BY TRACY LIEN & BRIAN BENNETT

SAN FRANCISCO

Setting up a pitched battle between Silicon Valley and the counterterrorism community, Apple's chief executive said Wednesday that his company would fight a court order demanding the tech giant's help in the San Bernardino attack investigation, turning what had been a philosophical dispute into a legal skirmish that could have major ramifications for the tech industry.

Apple CEO Tim Cook said that the FBI request that the company develop software to hack into one of its own devices, an iPhone 5C, used by gunman Syed Farook, would set a dangerous precedent that could compromise security for billions of customers. The government, Cook contends, is asking Apple to create a "backdoor" to its own security systems.

"Up to this point, we have done everything that is both within our power and within the law to help them," Cook wrote in a letter published on the company's website. "But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create."

The company will file an opposition to the court order, which was handed down in Riverside on Tuesday. The court order marks the first time Apple has been asked to modify its software to access data sought by the government, according to an industry executive familiar with the matter who spoke on condition of anonymity.

The Dec. 2 San Bernardino terrorist attack killed 14 people. Investigators said unlocking the phone could provide valuable information about the terror plot and whether Farook and his wife, Tashfeen Malik, received help from anyone else.

Chenxi Wang, chief strategy officer at the network security firm Twistlock, said the court battle would be a seminal moment in balancing "privacy and civil liberty against government data access."

"If Apple succeeds in fighting the court order, it will set up a high barrier for the FBI and the other government groups to access citizen data from now on," Wang said. "This will absolutely have a ripple effect. Apple is now viewed as the flag bearer for protecting citizen data, and if they succeed, there will be a flood of other companies following suit." Tensions between tech magnates and Washington, D.C., have been high since the 2013 Edward Snowden leaks revealed a massive domestic spying network that left millions concerned about communications privacy. Apple also changed the way it manages phone encryption in 2014, making it nearly impossible for forensic investigators to sidestep its pass-code system. Previously, investigators could tap into a device's hardware port to access encrypted data, according to Clifford Neuman, director of USC's Center for Computer System Security.

The pass-code system is the key issue blocking federal investigators from gaining access to the

data hidden on the phone used by Farook. Investigators want to unlock the phone by using a computer program to automatically guess numeric pass codes until one works, according to a court filing. But they say they require special access from Apple to attempt that on the phone without erasing data or getting bogged down in a long process.

Investigators say a feature is probably enabled that would immediately and permanently destroy encrypted data in the event of 10 consecutive failed log-in attempts.

In the government motion, the FBI argued that Farook intentionally disabled the phone's iCloud backup function six weeks before the terror attack at the Inland Regional Center. Any communications linked to the shooting, as well as location data that might help the FBI map the movements of Farook and his wife before and after the attack, are accessible only through the phone itself, the government said.

Investigators were able to retrieve some data from previous iCloud backups, and companies like Apple normally comply with requests to retrieve cloud data because they do not involve giving the government access to company servers or altering software, Neuman said. The San Bernardino County Department of Health, which employed Farook, actually owned the device and gave the FBI consent to search it, according to court filings.

The court order handed down Tuesday would require Apple to provide the FBI with a "recovery bundle" or file that would reboot Farook's device while disabling the auto-erase feature. That would allow the FBI to repeatedly enter pass codes remotely without risk of destroying the data on the phone.

Robert Cattanach, a cybersecurity attorney and former Department of Justice special counsel to the secretary of the Navy, said the government's request leaves Apple in a difficult position as the company is thrust into the center of the battle to balance privacy needs against counterterrorism efforts.

"The FBI's request ... represents the next step in the journey to find the Holy Grail of backdoor unencryption, and the next salvo in the ever-escalating battle between law enforcement and tech companies," Cattanach said.

In seeking this week's court order, the U.S. attorney's office cited the All Writs Act of 1789, a rarely used law that allows judges to issue orders they deem necessary and appropriate. Apple's argument that the government is overreaching has met favorable reception in at least one court.

Late last year, a U.S. magistrate in Brooklyn, N.Y., halted a government request to obtain a suspect's iPhone data in a drug conspiracy case, saying that the All Writs Acts might not provide enough legal foundation for such an order.

The Brooklyn magistrate hasn't issued a final order, but Apple told the court in a filing last week that it would like a decision because it has "been advised that the government intends to continue to invoke the All Writs Act ... to require Apple to assist in bypassing the security of other Apple devices in the government's possession."

Apple drew support from civil liberties advocates, who fear that totalitarian governments such as China will demand the company use a similar tool to open phones of opposition leaders and human rights activists.

“If the FBI can force Apple to hack into its customers’ devices, then so too can every repressive regime in the rest of the world,” ACLU staff attorney Alex Abdo said in a statement.

Apple’s objection to the FBI’s request may increase calls for a federal law that requires tech companies to design products that law enforcement officials can access with a search warrant. Earlier this year, a California legislator proposed a similar measure that would require all cellphones produced and sold in the state to have the capacity to be unlocked by law enforcement.

Any push for legislation would face stiff resistance from privacy advocates and technology companies, which say they are building products with encryption to protect users’ privacy and data from hackers, and because customers want it.

The Obama administration, which has increasingly reached out to Silicon Valley over the last year, has not asked Congress to intervene in the hope that tech company executives would find a way to comply with search warrants while still protecting customers’ privacy.

In the government’s motion, the FBI asked Apple to create a software package designed to function only on Farook’s phone. But Cook said in his letter that he was concerned about the potential for abuse.

“While the government may argue that its use would be limited to this case, there is no way to guarantee such control,” he wrote.

Presidential candidates began weighing in on the issue Wednesday morning. GOP front-runner Donald Trump said he was floored that Apple had not volunteered to aid the FBI.

“Who do they think they are?” he asked on Fox News.

Speaking to reporters in South Carolina, Sen. Marco Rubio said he hoped the tech giant would voluntarily comply with the government’s request, but acknowledged the court order is far from a simple issue.

In San Bernardino, locals reacted to news of Apple’s refusal with mixed emotions. Some expressed concern about government overreach. But others sympathized with the FBI.

Aaron Winchester of Menifee, who wore an Apple Watch and carried an iPhone 6S Plus, said he bought the products because he felt they were more secure and less prone to being hacked. Even so, he wants Apple to help law enforcement access the information on Farook’s phone. “When it comes to terrorism,” he said, “if there’s information they can get that will help prevent future crimes, that’s in the best interest of everyone.”

Lien and Bennett write for the California News Group, publisher of the Union-Tribune and the Los Angeles Times.