Q&A: A look at the Apple vs US Justice Dept. court fight

February 17 2016, by Eric Tucker And Tami Abdollah

In this photo taken Nov. 15, 2015, Apple CEO Tim Cook speaks in Milan, Italy. A U.S. magistrate judge has ordered Apple to help the FBI break into a work-issued iPhone used by one of the two gunmen in the mass shooting in San Bernardino, California, a significant legal victory for the Justice Department in an ongoing policy battle between digital privacy and national security. Apple CEO Tim Cook immediately objected, setting the stage for a high-stakes legal fight between Silicon Valley and the federal government. (AP Photo/Luca Bruno)

A U.S. magistrate judge has ordered Apple to help the FBI break into a work-issued iPhone used by a gunman in the mass shooting in San Bernardino, California. Apple chief executive Tim Cook immediately objected, setting the stage for a high-stakes legal fight between high-tech region Silicon Valley and the federal government.

Here's a look at the case so far:

___

WHAT DID THE JUDGE DECIDE?

Magistrate Judge Sheri Pym, a former federal prosecutor, ordered Apple Inc. to help the FBI hack into an encrypted iPhone used by Syed Farook, who along with his wife, Tashfeen Malik, killed 14 people in December in the worst terror attack on U.S. soil since Sept. 11, 2001. The phone was provided to him by San Bernardino County, where he worked as a government health inspector. Prosecutors say they don't know whether anything relevant is on the phone but can't access the information because they don't know the password and Apple won't cooperate.

___

WHAT MAKES THIS RULING SO IMPORTANT?

Federal law enforcement and leading technology companies have long been at an impasse about how to balance digital privacy for consumers against the responsibility of federal agents and police to investigate crimes or terrorism. The Obama administration has acknowledged encryption as valuable for privacy protection but, until now, had struggled to identify a major case that shows how Apple's encryption can hobble their investigations.

—

HOW'S APPLE SUPPOSED TO HELP?

The judge's order forces Apple to create and supply highly specialized software that the FBI can load onto the iPhone. That software would bypass a self-destruct feature that erases the phone's data after too many unsuccessful attempts to guess the passcode. The FBI wants to be able to try different combinations in rapid sequence until it finds the right one.

—

WHAT IMPACT WILL THIS HAVE ON OTHER APPLE USERS?

The Justice Department said it's asking Apple only to help unlock the iPhone used by Farook. The judge said the software should include a "unique identifier" so that it can't be used to unlock other iPhones. But it's unclear how readily the software could be adapted to work against other phones. And the FBI would likely share its new tool with U.S. intelligence agencies—and possibly foreign allies—that are investigating global terrorism.

Cook warned, "Once created, 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."

—

WHY DO THE FEDS WANT INFORMATION OFF THE PHONE?

Prosecutors say they think the device could hold clues about who the couple communicated with before and after the shooting and where they

traveled.

—

WHAT DID APPLE SAY?

The government asked the judge to rule in its favor in a 40-page court filing submitted without Apple's participation. After the ruling, in a strongly worded message to its customers early Wednesday, Cook warned that the judge's order would set a "dangerous precedent." He said the company was being asked to take an "unprecedented step" that would threaten the security of Apple's customers. The company defended its use of encryption as the only way to keep its customers' personal data—their music, private conversations and photos— from being hacked. The statement foreshadows a fierce legal fight.

—

HOW IS THIS LEGAL?

Pym relied on the 1789 All Writs Act, which has been used many times in the past by the government to require a third party to aid law enforcement in its investigation. Apple's CEO said the government was trying to dangerously expand what the law requires a third party to do. He said the government could require Apple to build surveillance software or more to help law enforcement. In a months-long federal case in New York, another federal judge has delayed ruling on whether the law can compel Apple to help the government break the security on its devices. That case remains pending.

Citation: Q&A: A look at the Apple vs US Justice Dept. court fight (2016, February 17)