Is Apple Intentionally Crippling Law Enforcement Access to Digital Evidence?

Author : Jeff Welty

Categories : Search and Seizure, Uncategorized

Tagged as : apple, encryption, ios, operating system, search warrants

Date : October 1, 2014

Apple recently announced new iPhones and a new operating system for its mobile devices. Amidst the hubbub, Apple also revealed that the new operating system would render it impossible for Apple to give law enforcement officers access to locked iPhones, even with a search warrant. Many in law enforcement aren't happy about this, with FBI Director James Comey stating that he can't understand why companies would "market something expressly to allow people to place themselves beyond the law." But is that what's going on?

Background. Under previous versions of its mobile operating system, Apple had the ability to recover certain items from locked phones. According to its law enforcement guidelines:

For iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant . . . Apple can extract certain categories of active data from passcode locked iOS devices [including] . . . SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party app data.

Change with the new operating system. Apple has just rolled out iOS 8, the latest version of its mobile operating system. Apple says that "[f]or all devices running iOS 8.0 and later versions, Apple will no longer be performing iOS data extractions as the data sought will be encrypted and Apple will not possess the encryption key." The technical explanation is detailed, but basically, in the new operating system, Apple is encrypting more data and is using stronger encryption – so strong that Apple itself can no longer crack it. Note that data backed up to Apple's iCloud service will still be available to law enforcement with a warrant, but users may configure their phones not to link to iCloud.

One view: Apple's helping bad guys and hurting police. As noted above, the law enforcement is disturbed by this turn of events. A Chicago police executive stated that "Apple will be the phone of choice for the pedophile." Manhattan District Attorney Cyrus Vance has called on Apple to reverse course – and for Congress to intervene if Apple doesn't act. And law professor Orin Kerr initially stated that he was "troubled" by Apple's new policy, though he has since moderated his view. This reaction may be due in part to Apple's proud touting of its inability to provide data to law enforcement. At this web site, Apple crows that "[u]nlike our competitors, Apple cannot bypass your passcode and therefore cannot access [user] data [in response to government requests]." That makes it seem as though the purpose of the enhanced encryption is to impede law enforcement.

Another view: Apple's improving phone security. There's another possible perspective on Apple's actions. This *Slate* article argues that "Apple is not designing systems to prevent law enforcement from executing legitimate warrants. It's building systems that prevent everyone who might want your data—including hackers, malicious insiders, and even hostile foreign governments—from accessing your phone." On this view, Apple is strengthening encryption to protect user data from bad actors, like those who apparently hacked Apple's iCloud system and accessed nude photos of various celebrities a month ago. Apple's inability to comply with search warrants for locked phones is a negative, but innocent, side effect of a positive security development.

The next shoe to drop. Whichever view of Apple's motives is correct, Apple's actions will have consequences.

Already, Google has announced a similar privacy enhancement to its next Android operating system, due next month. Going forward, it will be interesting to see whether Congress takes legislative action to require mobile operating systems to be equipped with “backdoors” that can be used by law enforcement pursuant to court order. As always, reader perspectives and insights are welcome.