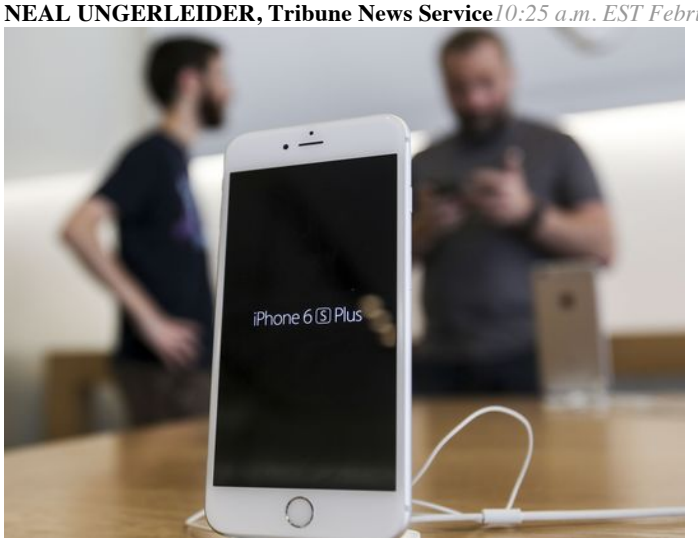
OPED: Apple vs. FBI: Unlocking Pandora's box

NEAL UNGERLEIDER, Tribune News Service *10:25 a.m. EST February 23, 2016*



(Photo: Ringo H.W. Chiu, AP)

In the locked-iPhone battle between the Federal Bureau of Investigation and Apple, the feds might have the judiciary on their side, but the tech giant has the better argument.

Last week, the FBI obtained a court order from the Federal District Court for Central California telling Apple to help unlock the iPhone 5C used by Syed Rizwan Farook, one of the attackers who killed 14 people in San Bernardino on Dec. 2. Specifically, the FBI wants Apple to create a custom operating system update that would give the FBI infinite tries at cracking the phone's passcode. Normally, after 10 failed attempts, an iPhone automatically deletes any encrypted data.

Tim Cook, chief executive of Apple, responded with a strongly-worded open letter saying the company would not comply. "The U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. (...) In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession."

That's not hyperbole. And it's not just the "wrong hands" we need to worry about.

We like to imagine that the law enforcement and government investigators tasked with preventing terrorist attacks are sober and dedicated, but the truth can be more sordid. In 2013, following disclosures that the National Security Agency had violated its own data collection rules more than 2,500 times in the course of a year, agency officials admitted that some of these incidents were personal in nature. A dozen or more cases involved NSA workers spying on their lovers and spouses.

Abuse of surveillance technology by law enforcement is more common than we think, which surely must be on Cook's mind. As his letter points out, there is no way to guarantee that the government won't use the altered operating system in other cases in the future.

Apple is also rightly worried that the case could establish a legal precedent to generate master keys to the encrypted data on any iPhone or iPad. Apple, Samsung, HTC, LG, Huawei and other smartphone manufacturers stake their business reputation on a tacit agreement: In exchange for a customer's money, the phone manufacturer does its best to ensure that his or her private information stays secure. With the creation of so-called backdoors or weakened encryption, they could face the loss of lucrative enterprise contracts from corporate clients who want to make sure proprietary information stays proprietary.

Apple's compliance with this court order also would harm America's whole tech sector, putting billions of dollars in profits — and tech industry jobs — at risk. In foreign markets, a perception (right or wrong) that an American technology company is working hand-in-glove with U.S. intelligence and law enforcement is ruinous for business.

That was the case when the tables were turned. Chinese smartphone maker Huawei found it nearly impossible to sell phones in the U.S. market for years because of fears here of surveillance by China. After it openly clashed with Beijing over cybersecurity, and entered into deals with Google, Deutsche Telekom and other Western companies, its Nexus 6P phone finally has a growing market share. In the European Union, meanwhile, merely storing European customers' data on U.S. servers has been a major policy concern.

Here's the kicker: Law enforcement hardly needs to bend Apple to its will in order to surveille terrorism suspects. It could instead just catch up with the superior tracking and data mining capabilities of the private sector.

To give one example of the sophisticated tracking tools in use, an advertising technology firm called Dstillery used location data to identify the smartphones of Iowa caucusgoers, and then scraped their online activities to find correlations between behaviors and voting patterns. (For instance, NASCAR fans correlated with caucuses supporting Donald Trump and Hillary Clinton.) Working within the law, the advertising tech industry has developed behavior monitoring and analysis techniques that are the government's envy.

It's important to note that we don't know if backdoors for law enforcement and intelligence secretly have been developed for some other tech products already. But the FBI's request, which will surely now wind up back in court, is terrible for American business and Americans in general. Writing on Twitter, Christopher Soghoian, principle technologist at the American Civil Liberties Union, summed it up: The court order gives law enforcement a precedent they have been seeking for a long time and clears the way to use software update mechanisms on mobile devices for surveillance.

Giving those capabilities to the FBI won't prevent further terrorist attacks. What might? Old-fashioned police work and cutting-edge analysis of the vast amount of legally available data.

The type of access the FBI wants, though, is a Pandora's box. Once it's developed, hackers, organized crime or foreign intelligence agencies stand to benefit as much as U.S. intelligence agencies and law enforcement. It is a cure, truly, that is worse than the disease.

— Neal Ungerleider is a reporter for Fast Company magazine and technology industry consultant who lives in Los Angeles.