Law360
A LexisNexis® Company

Expert Analysis

Did Apple Get It Right On Data Security And Privacy?

February 25, 2016, 10:11 AM EST

Law360, New York (February 25, 2016, 10:11 AM EST) -- In 1984, Apple Inc. released an American television commercial aptly titled, “1984,” which introduced the Apple Macintosh personal computer for the first time. The commercial, directed by now world-famous director Ridley Scott, showed an unnamed heroine using a sledgehammer to destroy a giant screen where an Orwellian-like version of Big Brother spoke to an auditorium of zombie like citizens in a trance.

More than three decades have passed since Apple first positioned itself as the great high-tech advocate of individual liberties. However, once again Apple’s commitment to, and defense of, its customers right to privacy and security in the digital world is being challenged at the highest levels by the FBI, the federal judiciary, and the U.S. government.

On Feb. 16, 2016, Tim Cook posted a message to all Apple customers informing them that the federal government had demanded that Apple take an unprecedented step to develop an operating system that would allow them to bypass Apple’s digital security infrastructure in order to access the information on an iPhone that belonged to one of the terrorists involved in the recent shooting in San Bernardino, California.

Think about that for a minute.

To date, Apple has cooperated extensively with the FBI to provide them with any and all information in Apple’s possession or control related to the terrorists involved in the San Bernardino shooting. However, this level of cooperation has proved to be inadequate from the government’s perspective.

Instead, they want Apple to create a new version of the iPhone operating system, circumventing several important security features, and to install it on the recovered iPhone. However, this software (which does not exist today) would have the potential to unlock any iPhone in someone's physical possession, not just the terrorist's.

Cook says that "building a version of iOS that bypasses security in this way would undeniably create a backdoor," which could compromise the integrity of every single iOS user in the world. Currently, there are approximately 700 million such iOS users.

People use iPhones to store an incredible amount of personal information including, among other things, private conversations and photos, calendars and contacts, and financial information and health data.

Cook points out that "all that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission."

Moreover, Cook states that Apple customers "expect Apple and other technology companies to do everything in [their] power to protect … personal information" through encryption. In Cook's opinion, the only way to truly safeguard personal data is to use encryption and put such data out of Apple's reach — or anyone else's reach for that matter. As a result, Apple is refusing to build a new iOS that includes a way to undermine and circumvent Apple's digital security systems.

If Apple builds a "back door" to unlock the data of the San Bernardino terrorist's phone, the technique could fall into the hands of hackers and be used to undermine Apple's iOS encryption software by anyone with knowledge of the technique. Cook equates this to giving cybercriminals "a master key … capable of opening hundreds of millions of locks … from restaurants and banks to stores and homes."

As a member of my firm's privacy and data security law team and former general counsel to a software development company, I can tell you that Cook is being pragmatic and not paranoid. As breaches at Sony Corp., Target Corp., Anthem Inc. and other major corporations have demonstrated in recent months, we're in a constant battle to stay a step ahead of the hackers. The thought of having the world's biggest technology company create this kind of software opens a potential Pandora's box of problems that can cause far more

trouble than it's worth.

Moreover, Apple feels that there is no meaningful legal precedent for requiring it to comply with the San Bernardino court order.

The Declaration of Independence was signed by the Founding Fathers in 1776. A few years later, in 1789, the All Writs Act was passed. It stated, in part, that "the Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." This excessively vague and ambiguous 227-year-old language is the basis upon which the FBI is trying to justify an expansion of its authority to require Apple to build the back door to iOS.

It is important to recognize that the right to privacy in modern western society is not an inviolable, static, fundamental right. It is equally as important for individuals (including, but not limited to, the 94 million Apple customers in the United States who own iPhones) to be able to limit and control disclosures about their personal lives. And when you engage in dangerous criminal conduct like the San Bernardino shooters, or align yourself with the ideals of terrorism, or threaten the lives of others, you give up some of those rights to privacy. However, even when important governmental interests outweigh the interests of one's right to privacy, Apple (and similarly situated technology companies) should not necessarily be forced to expose their customers to a large-scale digital attack that results from a court order requiring the development of a new operating system that can perform an end-around on sophisticated encryption software. Not even the 200-year-old All Writs Act provides a reliable legal precedent for the U.S. government to force Apple to subject its iPhone users to exponentially greater risks of digital attacks on their personal information.

Some have claimed that Apple is refusing to develop the back door to its encryption software as a marketing strategy — much like that of the "1984" television ad campaign. However, Cook says that "nothing could be further from the truth." Apple claims that its refusal to comply with the court order and build the back door to its encryption software is not about the company at all. Rather, it is and always has been about Apple customers.

All of the above notwithstanding, as the battle between the U.S. government and Apple over digital security and privacy of iPhone users begins to unfold, based on his open letter to the public, Cook is laying the groundwork for Apple's "2016" advertising campaign. And through Cook's words, I envision him wielding yet another sledge hammer on behalf of the vast

majority of good and law abiding citizens who rely on Apple and their iPhones to protect their most personal and important data.

As Cook points out, “the best way forward would be for the government to withdraw its demands under the [227-year-old] All Writs Act and, as some in Congress have proposed, form a commission or other panel of experts on intelligence, technology, and civil liberties to discuss the implications for law enforcement, national security, privacy, and personal freedoms.” I’ll bet that George Orwell would also be in favor of such a commission.

—By Jeffrey Glassman, Ervin Cohen & Jessup LLP

Jeffrey Glassman is a partner at Ervin Cohen in Beverly Hills, California, and former in-house counsel at Firetalk Communications.