The Apple iPhone Unlock Showdown: What is at Stake?

David W. Opderbeck

New Jersey Law Journal, March 7, 2016

Apple CEO Tim Cook made headlines recently when he posted a public letter to Apple customers about why the company would not help federal investigators unlock an iPhone used by San Bernardino shooter Syed Rizwan Farook. What is really at stake in this showdown? In particular, how do the technological realities of this situation relate to the law?

Farook and his wife, Tafsheen Malik, shot and killed 14 people and injured 22 others on Dec. 2, 2015. Just prior to the attack, Malik posted a Facebook message pledging allegiance to the leader of the terror group ISIS. After the attack, police discovered thousands of rounds of ammunition and over a dozen pipe bombs at Farook's residence. Farook and Malik were killed in a shootout with police after the attack.

Farook's employer, the Inland Regional Center, a government agency, had issued him an iPhone as part of his employment. The phone was found in Farook's vehicle pursuant to a search warrant that also authorized the FBI to search the digital data on the phone. Investigators have been able to recover some data from Farook's phone through backup data stored on an Apple iCloud account associated with the phone. However, the government claims the iCloud data ends on Oct. 19, 2015. Separate toll and billing records obtained by the government show that the phone was used in November 2015, prior to the December 2 attacks. The government has not been able to access the phone itself because the phone is locked.

iPhone users are familiar with the lock screen, which requires the user to input a 4-digit PIN code to access the phone. This security feature is relatively easy to defeat using a "brute force" attack—that is, an effort to run through multiple variations of possible passwords or PIN codes. With a 4-digit PIN code, the possible variations run from 0000 to 9999, with a total of 10,000 possible combinations. Although it would be time consuming, it is entirely feasible to work through a list of possible combinations to find the right code. Because of this vulnerability, Apple upgraded its iPhone operating system to allow users to limit the number of attempts that can be made to enter the PIN. When this feature is enabled, after the tenth consecutive incorrect attempt, any data on the phone is wiped. The phone used by Farook employed this more recent version of the operating system, although it is impossible to know whether Farook enabled the

wiping feature. The FBI therefore cannot attempt to unlock the phone without running the risk of wiping the data.

The government asked Apple to supply technical assistance required to disable the wiping feature. Inland Regional Center, the owner of the phone, consented to having Apple disable the wiping feature. Apple says it cannot comply because it would have to create a new version of the iPhone operating system without the wiping feature. Once created, Apple says, this new operating system could be used by anyone, including criminal hackers or rogue states, on any iPhone. Apple also claims that allowing the government access in this case would create a precedent in favor of access in other cases. In fact, Apple claims there are already more than a dozen similar orders for iPhone cracks. See Feb. 17, 2016, letter of Mark Zwillinger to Hon. James Orenstein. The government argues that this "crack" could be specific to Farook's phone and could be controlled securely by Apple, so that it could not be used by the government or anyone else to defeat the security on any other phone.

After Apple refused to cooperate voluntarily, the government obtained an order from a Federal Magistrate Judge under the All Writs Act (AWA), 28 U.S.C. §1651, which empowers federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law," requiring Apple to render "reasonable technical assistance" to the government in its effort to examine Farook's phone, including specifically providing a crack of the wiping feature. The first version of the AWA was part of the Judiciary Act of 1789, passed by the First Congress and signed into law by President Washington. Apple claims the government should not have broad power under the AWA to compel a technology company to write new code that unlocks its products' security features. The government has cited a number of cases in support of the propriety of this order.

In particular, the Supreme Court addressed a somewhat similar situation in *U.S. v. New York Telephone Co.*, 434 U.S. 159 (1977). In that case, the FBI sought the assistance of New York Telephone Co. in placing a pen register device on a phone line in order to gather evidence relating to a suspected illegal gambling establishment. A pen register records the numbers dialed on a telephone but does not record any actual conversations.

At the time of the *New York Telephone* case, there was no statute specifically authorizing court orders for the use of pen registers, although such a statute exists today. *See* 18 U.S.C. §1831. The government obtained an order from the U.S. District Court for the Southern District of New York, under the AWA, requiring the company to supply "'all information, facilities and technical assistance'" necessary to place the pen registers. *Id*. at 161. The company agreed to help the FBI identify the pairs of wires upon which the pen register should be placed. However, the company refused to provide the FBI with lines that would enable the device to be placed inconspicuously, and challenged the district court's authority to issue the order.

The Supreme Court held by a 6-3 majority that the district court had authority under the AWA to issue the order. Writing for the majority, Justice White stated that:

The power conferred by the [AWA] extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice . . . and encompasses even those who have not taken any affirmative action to hinder justice.

Id. at 174. In dissent, Justice Stevens, joined by Justices Brennan and Marshall, argued that the order was analogous to the general "writs of assistance" issued by the British Crown, which were among the key issues that led to the American Revolution. *See id*. at 186-89.

In the Apple case, there is no dispute that the search warrants issued for Farook's phone and its contents were valid. Indeed, since Farook is dead and the phone's owner, Inland Regional Center, consents to the search, there does not seem to be any Constitutional privacy issue with this particular order. In this sense, the government's case is even stronger than in *New York Telephone*, which was decided in the absence of a specific pen register statute. On the other hand, the court in *New York Telephone* noted that the use of pen registers in general was common practice and was often used by the phone company itself for billing and fraud prevention purposes. Here, Apple claims that it is being asked to do something unprecedented in its business operations: the creation of a new operating system, which involves writing new computer code, specifically designed to defeat a security mechanism that is a core feature of its existing product.

As a broad policy matter, then, this case is about the level of security that should be allowed in personal computing and communications devices such as cellphones. In this sense, the case is part of a roiling policy debate about whether manufacturers and distributers of encryption technology should be required to provide a "backdoor" or key through which the government may access encrypted data pursuant to a search warrant or other process. But just how deep this particular case falls into this thick soup may depend on a factual issue that seems to remain in dispute: whether Apple really can create a crack that is unique to a particular suspect's phone or that can be kept entirely within Apple's control and either locked away or destroyed after implementation. Either way, the case highlights the tensions that inevitably surface when large, international private technology and communications infrastructure and device companies hold the key—perhaps literally—to information about ongoing criminal or terrorist activity.