# In This Corner…The Apple v. FBI Cage Match

Lawrence Husick is a Senior Fellow and co-director of FPRI's Center for the Study of Terrorism. He is also co-director of the FPRI Wachman Center's Program on Teaching Innovation.

## Related program(s)

Center for the Study of Terrorism

Since February 16, 2016, the media has breathlessly covered the painfully public dispute between the FBI and Apple, Inc., over the government's demand that Apple provide access to the iPhone 5c used by (but not owned by) one of the San Bernardino terrorists, Syed Rizwan Farook. According to a motion filed by United States Attorneys on behalf of the FBI, that iPhone is locked with a passcode, making its contents encrypted and thus, inaccessible. Because the iPhone software limits the speed at which attempts to unlock it may be made, getting slower with every failed entry, and because it is likely that after ten failures, all information on the phone will be automatically erased, the FBI asked federal magistrate judge Sheri Pym to use a 1789 law, the All Writs Act, to order Apple to bypass security on the device so that the Bureau could rapidly try every possible password. Apple's Chairman, Tim Cook, publicly stated that Apple would oppose the order, and Apple hired former Bush Solicitor General Ted Olsen to represent the company. Apple was given five business days to file its objections. Two days later, the Department of Justice filed a 25 page Motion to Compel asking Judge Pym to again order Apple to comply with her order.

**What is this iPhone?**

The "SUBJECT DEVICE", as the court calls it, is an iPhone 5c, recovered by law enforcement from a Lexus parked outside Farook's home after the gun battle that resulted in his death. The phone was issued to Farook, and is owned by his employer, San Bernardino County Department of Public Health. It was associated with a county Apple iCloud account that was used to back up the information stored in the phone, and the last backup, made approximately six weeks prior to the mass shooting in San Bernardino, is in the FBI's possession, as are logs of every call and text message sent to and from the phone. The County did not use Apple's free Configurator software, which would have allowed administrative access to unlock the iPhone, even remotely. Farook had at least one other personal phone, which he destroyed, and that, too, is in the FBI's hands. Thus far, the FBI has not published any information about what it believes is stored on the SUBJECT DEVICE. It has only said that it was used by Farook, and that the Bureau has been unable to access its contents, which may include the address book, transcripts of iMessage chats, which are encrypted by Apple's software, and stored files and photos.

From public statements and court filings, we know that the FBI attempted to access the iCloud backup of the phone in the hours just after it was seized, by instructing an employee of the county to change the iCloud password. This was a mistake, because the change meant that the phone would not then execute

an automatic backup through a WiFi connection without entry of the passcode. This password change may have precluded the simplest way to gain access to the information the FBI now demands Apple help uncover.

**What the FBI Wants**

According to its brief, and to the magistrate judge's order, the FBI has demanded that Apple write a new version of its iOS operating system that bypasses the auto-erase function, accepts passcodes electronically (rather than typing them in), and removes any delay function between attempts. This new software would then be loaded to the iPhone through a cable connected to a computer running iTunes software, verified by a new version of Apple's internal security server software (which Apple would also have to create) and the FBI would be given access to try every possible passcode to unlock the phone.

The FBI believes that the All Writs Act provides a legal mechanism for the court to order Apple to comply. The Act gives courts broad authority to order a third party to provide non burdensome technical assistance to law enforcement officers, but has never been interpreted as broadly as to require that someone write extensive new software to modify an existing system. Courts have forced companies to write simple software to search, for example, call logs and email logs to filter out information sought under a warrant. Telephone companies must attach wiretaps, and cellphones, including iPhones have been ordered unlocked. But those cases did not require that a company undo entire portions of its systems. In its motion, the Department of Justice says, "…writing software code in discrete and limited manner – is not an unreasonable burden for a company that writes software code as part of its regular business."

**Why Would Apple Object?**

Apple has issued a public statement objecting to Judge Pym's order, but has not yet filed its response in court. To understand the full context of Apple's position, it is instructive to recall that politicians and law enforcement officials, including the head of the FBI, state attorneys general, and state and local police officials called on all manufacturers of mobile phones, and on network operators to engineer a technical solution to an epidemic of smartphone-related killings, muggings and thefts.[1] Because smartphones were being stolen and resold overseas, these officials called on technology companies to make it more difficult to re-enable a stolen phone without the owner's consent. Apple was the first to respond in July 2013 by making its phones require a passcode and a confirming network response before becoming active. Enabling this feature required the use of encryption to prevent simple bypassing of the security feature when the iPhone was plugged into a computer.

In the wake of the Snowden revelations of warrantless surveillance by the NSA, Apple released new updates to its iOS software (iOS 8) and a new version of the processor at the heart of every iPhone and iPad (A8) that incorporated a new "secure enclave" co-processor that handles encryption and security for the devices. Older iPhones (the 5c model, and older) that lacked this new chip nonetheless benefited from increased encryption in software. Apple has stated, "For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."

Apple's Tim Cook has said that although he and all Apple employees deplore terrorism, and are sympathetic to the needs of law enforcement, acceding to the court's order, "would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them."

What Cook left unstated is that as soon as Apple opens the iPhone to the FBI, terrorists and criminals everywhere will instantly move to other methods of communication. We will have broken Apple's security and injured the company for no net gain. In addition, once Apple complies with a lawful court order in the

United States, this global company will have no choice but to comply with orders from authoritarian regimes around the world, as well as with more intrusive orders from the United States intelligence and law enforcement communities. It is a short technical step from a new iOS that disables encryption, to one that clones a suspect's iPhone to mirror all communications silently - and we can be sure that the government will secretly demand this, and more. As the Snowden documents demonstrate all-too-well, that kind of surveillance has been conducted without a warrant against citizens and US residents on numerous occasions. As for assurances that the FBI could keep the new Apple software safe from hackers, we should recall that recent hacks of the IRS, OPM, and other government agencies have let the personal information of every FBI employee and job applicant leak to China.

**What's At Stake**

The FBI and Department of Justice have carefully chosen this public fight with Apple, despite having quietly worked with the company on dozens of prior cases. It is difficult to know exactly why it has chosen to make this issue so public, when doing so stands to reveal very little of value on an old iPhone, and to result in potential harm to national security, individual privacy, and Apple.

After stating in its early-filed Motion to Compel that Apple refused to cooperate with the FBI, the government went on to detail that Apple's engineers had, in fact, suggested five separate ways in which the FBI could try to access the information stored on the SUBJECT DEVICE. Although the documents in this matter refer to just this one iPhone, there are presently at least a dozen pending warrants that have been served on Apple, and the company has filed objections to at least ten of these. It is also impossible to know how many times the FBI has issued nation security letters to Apple demanding similar assistance, as these are secret, and the company would be legally prevented from disclosing their existence.

For the FBI, getting what's in that iPhone, regardless of the cost, is a matter of complete and thorough investigation into a horrific act of terrorism. It also comports with a reported secret late-2015 National Security Council Decision Memorandum, ordering agencies of the US government to break encryption and gain access to devices including the iPhone. For Apple, being forced to engineer a method that will then be used to render its products untrustworthy is a matter of principle, as well as business.

There is nearly universal agreement that weak encryption harms everyone, and that building a digital backdoor is the equivalent of having no privacy in your own information - and that means in today's world, data about your health, associations, political views, religious practices, sex life, and all other forms of personal confidential information becomes publicly exposed. Once the door exists, say security experts, not just officers with warrants (and spies without), but criminals, despots, and other bad actors will enter, unbidden.[2]

**A Proposed Solution**

The legal arguments about whether the FBI's request is unduly burdensome for Apple will be central to the company's response. After all, the glib statement of the FBI in its motion to the court that because Apple is a company that writes software, it should be easy to write this particular software is disingenuous, at best. Most would agree, however, that the job of the FBI and the US intelligence community is to investigate and spy to the fullest extent of the law. If that is so, then why not have the FBI, with the assistance of the NSA, which has extensive experience hacking iPhones, write the software needed to access the SUBJECT DEVICE, and merely order Apple to digitally "sign" this software with its secret encryption key so that the Farook iPhone will execute it? This solution does not expose any of Apple's secrets, and may be accomplished in mere seconds inside Apple's engineering facilities. If it is the job of the FBI to investigate, it may fully execute that obligation - and, we should hope that if it is successful, it would not announce that fact to the world. It is not up to Apple to do the FBI's job. Not even under the All Writs Act. One should hope that our courts will recognize that difference, and act accordingly.

**The Larger Issues**

For its part, Apple has called for, "…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." Apple has said that it would gladly participate in such an effort. Other technology companies, including Alphabet (Google), and Facebook have joined with that suggestion. CIA Director John Brennan has sided with the FBI, while Retired Gen. Michael Hayden, former director of the NSA and CIA has said that while the burden is on Apple, creating means to defeat data protection are dangerous to American security and privacy. Clearly, reasonable experts differ widely.

Issues of privacy, law enforcement, intelligence, and line-drawing among competing interests are important to open societies. While the narrow legal and technical issues surrounding the Farook iPhone may be resolved after argument and appeal, the larger issues will remain. In considering these matters, there are several touchstones available. First, that encryption technology will always be at least one step ahead of the law, and will be used for both good and ill. Second, as the late Justice Scalia said, "There is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all."[3]

---

[1] http://www.dailymail.co.uk/news/article-2371391/Apple-launch-kill-switch-stolen-iPhones-Boris-Johnson-calls-mobile-phone-manufacturers-to-curb-thefts.html

[2] http://www.nytimes.com/roomfordebate/2016/02/23/has-encryption-gone-too-far/a-key-for-encryption-even-for-good-reasons-weakens-security

[3] Arizona v. Hicks, 480 U.S. 321 (1987).