8 MINUTE READ | TECHNOLOGY

These Are Apple's Top 10 Legal Points In The iPhone Encryption Case

In a motion filed Thursday, Apple asked that the FBI's court order demanding it help hack into an iPhone 5c be vacated.

[Photo: Flickr User petter palander]

MARK SULLIVAN | 02.26.16 | 1:45 AM

Apple lawyers Thursday fired back at the federal district court that ordered it to help the FBI hack into the iPhone used by San Bernardino shooter Syed Farook.

Apple has made no secret of its unwillingness to comply with the order, and the motion filed today with the District Court of the Central District of California makes it official.

Apple's attorneys, who come from two outside law firms, included an impressive array of arguments. Here are the most interesting and compelling ones:

1) "JUST THIS ONE TIME," YEAH, RIGHT

People in law enforcement have argued that the FBI's demand for Apple to build a custom OS to access Farook's phone is a one-off. The "backdoor" created would be destroyed and

Apple doesn't believe it, and its concern over the issue is perhaps the central reason it won't help the FBI.

" . . . the government knows those statements are not true; indeed the government has filed

multiple other applications for similar orders, some of which are pending in other courts."

Documents ordered unsealed at a Brooklyn federal court on Tuesday show the FBI has requested that Apple help unlock iPhones at least nine times, and possibly as many as 17 times, since last October.

"If this order is permitted to stand, it will only be a matter of days before some other prosecutor, in some other important case, before some other judge, seeks a similar order using this case as precedent," the order reads.

2) LETTING THE GENIE OUT

The court order demanded that Apple build a custom OS that could be uploaded to Farook's phone to disable the security features that prevent multiple logins. The FBI wants to use a computer to quickly enter thousands of passwords into the phone until Farook's passcode is found, making a login possible. But that custom OS amounts to a "master key" that could be used to unlock other iPhones if it falls into the wrong hands.

The lawyers take pains to explain to the court that once a master key is created, it's hard to uncreate it:

"The virtual world is not like the physical world. When you destroy something in the physical

world, the effort to recreate it is roughly equivalent to the effort required to create it in the first place. When you create something in the virtual world, the process of creating an exact and perfect copy is as easy as a computer key stroke because the underlying code is persistent."

3) THERE'S A REASON CONGRESS HASN'T MADE A LAW FOR THIS

Law enforcement has for a few years been trying to persuade Congress to pass a law making it easier to demand "backdoor" access to devices. But it's failed.

Legal experts say law enforcement now hopes that the courts will yield some legal footing for the backdoor requests. Apple argues that the courts are the wrong venue for that.

APPLE'S STANDOFF WITH THE FBI

- These Are Apple's Top 10 Legal Points In The iPhone Encryption Case
- From Fines To Jail Time: How Apple Could Be Punished For Defying FBI
- FBI Has Asked Apple To Unlock As Many As 17

Apple lawyers point out that the government has pushed for changes to the Communications Assistance for Law Enforcement Act ("CALEA"), which defines the circumstances under which private companies must assist law enforcement. Today CALEA says that if a tech company does not keep encryption keys to its products, it's not required to provide them to law enforcement.

iPhones In Last 4 Months

- Now Apple Could Make The iPhone 7 Even Harder To Unlock
- Why The FBI Chose To Try The Apple Encryption Case In The Media

"Congress, keenly aware of and focusing on the specific area of dispute here, thus opted not to provide authority to compel companies like Apple to assist law enforcement with respect to data stored on a smartphone they designed and manufactured," the filing reads.

4) YOU CAN'T USE THE ALL WRITS ACT TO MAKE US DO THIS

The order compelling Apple to help the FBI used as its legal basis an archaic law called the All Writs Act. Back in 1977, the Supreme Court ruled in U.S. v. New York Telephone that federal courts can rely on the All Writs Act in some cases to compel private companies to help the government in the "proper administration of justice."

In one of the central points of its case, Apple argues that the district court used the All Writs Act to expand its powers beyond its true jurisdiction.

"The All Writs Act authorizes courts to 'issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law,' . . . but as the Supreme Court has held, it does not authorize [courts] to issue ad hoc writs whenever compliance with statutory procedures appears

inconvenient or less appropriate," the motion says.

It continues: "The Ninth Circuit likewise has emphasized that the 'All Writs Act is not a grant of plenary power to federal courts. Rather, it is designed to aid the courts in the exercise of their jurisdiction."

5) MAKING A MASTER KEY WOULD BE HARD

The February 16 court order described *one way* that Apple might avoid complying with the FBI's demands—by declaring the job of creating the wholly new firmware needed to hack into Farook's iPhone to be "unreasonably burdensome."

The lawyers make the argument in the brief. It isn't one of Apple's stronger arguments, but because it's the one objection the court has already said it would hear, it's worth including.

In the motion, Apple's attorneys offer some specifics on the time and resources that would be needed:

"The compromised operating system that the government demands would require significant resources and effort to develop. Although it is difficult to estimate, because it has never been done before, the design, creation, validation, and deployment of the software likely would necessitate six to ten Apple engineers and

MUST READS

- Sony's Streaming Cable T
  Service Is Going National

employees dedicating a very substantial portion of their time for a minimum of two weeks, and likely as many as four weeks."

"Members of the team would include engineers from Apple's core operating system group, a quality assurance engineer, a project manager, and either a document writer or a tool writer," the filing says.

This last point underscores the risk of creating a master key. The more people involved, the greater the likelihood of a leak.

6) YOU HAVEN'T PROVED THAT YOU NEED US

The attorneys argue that the government didn't try everything else in its power to find some other way of hacking into the Farook phone before it "conscripted" Apple to help.

"Moreover, the government has not made any showing that it sought or received technical assistance from other federal agencies with expertise in digital forensics, which assistance might obviate the need to conscript Apple to create the back door it now seeks," the motion reads.

And this is where the attorneys call the government out for effectively ruining a possible way of hacking into the phone (without Apple's help). The feds reportedly asked that the password on Farook's iPhone be reset soon after

it was recovered. This ended the possibility of accessing the the phone by connecting it to a trusted Wi-fi network.

"Indeed, the FBI foreclosed one such avenue when, without consulting Apple or reviewing its public guidance regarding iOS, the government changed the iCloud password associated with an attacker's account, thereby preventing the phone from initiating an automatic iCloud."

7) THE ORDER VIOLATES FIRST AMENDMENT RIGHTS

In one of the stranger arguments in the motion, Apple attorneys assert that because the court is demanding the company write code it doesn't want to write, it's violating the First Amendment.

The First Amendment, precedent shows, regards computer code as a form of speech, the lawyers point out. Case law shows that The First Amendment is violated not just when one party prevents another from speaking, but also when a party is compelled to say something that they either don't want to say, or don't believe, or both.

"Forcing Apple to write software that would create a back door to millions of iOS devices would not only 'usurp the legislative function,' but also unconstitutionally compel speech and expose Apple iPhone users to exceptional security and privacy risks," the lawyers write.

8) WHAT EXACTLY DOES THE FBI HOPE TO FIND ANYWAY?

Law enforcement has not described what data it hopes to find on Farook's phone, and how it might help in the wider fight against terror. The government is asking people to potentially trade away a little bit of their digital privacy, but hasn't been clear about what's being gained in security.

"Apple does not question the government's legitimate and worthy interest in investigating and prosecuting terrorists, but here the government has produced nothing more than speculation that this iPhone might contain potentially relevant information."

The attorneys cite a statement by FBI Director James Comey: "Maybe the phone holds the clue to finding more terrorists. Maybe it doesn't."

9) ISIS LIKES ENCRYPTION

Apple also argues that even if the FBI could hack into Farook's iPhone it might just find more encryption from other companies.

"It is well known that terrorists and other criminals use highly sophisticated encryption techniques and readily available software applications, making it likely that any information on the phone lies behind several other layers of non-Apple encryption."

The attorneys cite a *Tech Savvy* article noting that

the Islamic State has issued to its members a ranking of the 33 most secure communications applications, and "has urged its followers to make use of [one app's] capability to host encrypted group chats."

10) THE PRIVACY-SECURITY BALANCE

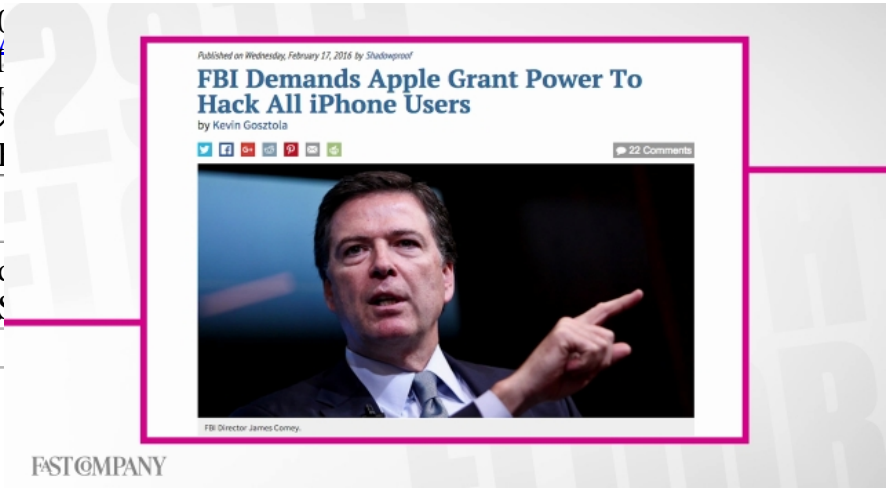
In the conclusion of the motion, Apple's lawyers express sympathy for law enforcement's desire to use all means possible to locate and prosecute terrorists. They also state that society is still getting its head around the trade-off between personal data privacy and the need to protect security. So, the lawyers say, it's far too early to make lasting decisions on the subject.

"Society is still debating the important privacy and security issues posed by this case," the motion says. "The government's desire to leave no stone unturned, however well intentioned, does not authorize it to cut off debate and impose its views on society."

The Apple filing is impressive in the breadth and depth of its arguments. Magistrate Judge Sheri Pym, the judge who signed the order, will again review the case at a March 22 hearing. After that she'll hand down a decision to either vacate or uphold the original order. But it may take months for that to happen.

[

APPLE VS. THE FBI: WHAT'S AT STAKE



TOP STORIES

Welcome To The Post-Work Economy

The World Changing Ideas Of 2016

Now The Justice Department Suggests It May Demand Apple's "Source Code"

How To Rebuild A Burned Bridge

THE LATEST

- Lyft And GM Are Starting A Car Rental Service Together
- Like The Maid In "The Jetsons," iRobot's Braava Will Mop The Floors
- How Imgur Became An Image-Sharing, Meme-Generating Megacommunity