DOJ'S PRE-ASS-HANDING CAPITULATION

In its February 16 application for an All Writs Act to force Apple to help crack Syed Rizwan Farook's phone, DOJ asserted,

> Apple has the exclusive technical means which would assist the government in completing its search, but has declined to provide that assistance voluntarily.
>
> [snip]
>
> 2. The government requires Apple's assistance to access the SUBJECT DEVICE to determine, among other things, who Farook and Malik may have communicated with to plan and carry out the IRC shootings, where Farook and Malik may have traveled to and from before and after the incident, and other pertinent information that would provide more information about their and others' involvement in the deadly shooting.
>
> [snip]
>
> 3. As an initial matter, the assistance sought can only be provided by Apple.
>
> [snip]
>
> 4. Because iOS software must be cryptographically signed by Apple, only Apple is able to modify the iOS software to change the setting or prevent execution of the function.
>
> [snip]
>
> 5. Apple's assistance is necessary to effectuate the warrant.
>
> [snip]
>
> 6. This indicates to the FBI that Farook may have disabled the automatic iCloud backup function to hide evidence, and

> demonstrates that there may be relevant, critical communications and data around the time of the shooting that has thus far not been accessed, may reside solely on the SUBJECT DEVICE, and cannot be accessed by any other means known to either the government or Apple.

FBI's forensics guy Christopher Pluhar claimed,

> 7. I have explored other means of obtaining this information with employees of Apple and with technical experts at the FBI, and we have been unable to identify any other methods feasible for gaining access to the currently inaccessible data stored within the SUBJECT DEVICE.

On February 19, DOJ claimed,

> 8. The phone may contain critical communications and data prior to and around the time of the shooting that, thus far: (1) has not been accessed; (2) may reside solely on the phone; and (3) cannot be accessed by any other means known to either the government or Apple.
>
> [snip]
>
> 9. Apple left the government with no option other than to apply to this Court for the Order issued on February 16, 2016.
>
> [snip]
>
> 10. Accordingly, there may be critical communications and data prior to and around the time of the shooting that thus far has not been accessed, may reside solely on the SUBJECT DEVICE; and cannot be accessed by any other means known to either the government or Apple.
>
> [snip]

> 11. Especially but not only because iPhones will only run software cryptographically signed by Apple, and because Apple restricts access to the source code of the software that creates these obstacles, no other party has the ability to assist the government in preventing these features from obstructing the search ordered by the Court pursuant to the warrant.
>
> [snip]
>
> 12. Apple's close relationship to the iPhone and its software, both legally and technically — which are the produce of Apple's own design — makes compelling assistance from Apple a permissible and indispensable means of executing the warrant.
>
> [snip]
>
> 13. Apple's assistance is also necessary to effectuate the warrant.
>
> [snip]
>
> 14. Moreover, as discussed above, Apple's assistance is necessary because without the access to Apple's software code and ability to cryptographically sign code for the SUBJECT DEVICE that only Apple has, the FBI cannot attempt to determine the passcode without fear of permanent loss of access to the data or excessive time delay. Indeed, after reviewing a number of other suggestions to obtain the data from the SUBJECT DEVICE with Apple, technicians from both Apple and the FBI agreed that they were unable to identify any other methods — besides that which is now ordered by this Court — that are feasible for gaining access to the currently inaccessible data on the SUBJECT DEVICE. There can thus be no question that Apple's assistance is necessary, and that the Order was therefore properly

> issued.

Almost immediately after the government made these claims, a number of security researchers I follow not only described ways FBI might be able to get into the phone, but revealed that FBI had not returned calls with suggestions.

On February 25, Apple pointed out the government hadn't exhausted possible of means of getting into the phone.

> 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. See Hanna Decl. Ex. DD at 34–36 [October 26, 2015 Transcript] (Judge Orenstein asking the government "to make a representation for purposes of the All Writs Act" as to whether the "entire Government," including the "intelligence community," did or did not have the capability to decrypt an iPhone, and the government responding that "federal prosecutors don't have an obligation to consult the intelligence community in order to investigate crime"). As such, the government has not demonstrated that "there is no conceivable way" to extract data from the phone.

On March 1, members of Congress and House Judiciary Committee witness Susan Landau suggested there were other ways to get into the phone (indeed, Darrell Issa, who was one who made that point, is doing a bit of a victory lap). During the hearing, as Jim Comey insisted that if people had ways to get into the phone, they should call FBI, researchers noted they had done so and gotten no response.

> Issa: Is the burden so high on you that

> you could not defeat this product, either through getting the source code and changing it or some other means? Are you testifying to that?
>
> Comey: I see. We wouldn't be litigating if we could. We have engaged all parts of the U.S. Government to see does anybody that has a way, short of asking Apple to do it, with a 5C running iOS 9 to do this, and we don not.
>
> [snip]
>
> a) Comey: I have reasonable confidence, in fact, I have high confidence that all elements of the US government have focused on this problem and have had great conversations with Apple. Apple has never suggested to us that there's another way to do it other than what they've been asked to do in the All Writs Act.
>
> [snip]
>
> b) Comey [in response to Chu]: We've talked to anybody who will talk to us about it, and I welcome additional suggestions. Again, you have to be very specific: 5C running iOS 9, what are the capabilities against that phone. There are versions of different phone manufacturers and combinations of models and operating system that it is possible to break a phone without having to ask the manufacturer to do it. We have not found a way to break the 5C running iOS 9.
>
> [snip]
>
> c) Comey [in response to Bass]: There are actually 16 other members of the US intelligence community. It pains me to say this, because I – in a way, we benefit from the myth that is the product of maybe too much television. The only thing that's true on television

> is we remain very attractive people, but we don't have the capabilities that people sometimes on TV imagine us to have. If we could have done this quietly and privately we would have done it.
>
> [snip]
>
> Cicilline: I think this is a very important question for me. If, in fact – is it in fact the case that the government doesn't have the ability, including the Department of Homeland Security Investigations, and all of the other intelligence agencies to do what it is that you claim is necessary to access this information?
>
> d) Comey: Yes.

While Comey's statements were not so absolutist as to suggest that only Apple could break into this phone, Comey repeatedly said the government could not do it.

On March 10, DOJ claimed,

> 15. The government and the community need to know what is on the terrorist's phone, and the government needs Apple's assistance to find out.
>
> [snip]
>
> 16. Apple alone can remove those barriers so that the FBI can search the phone, and it can do so without undue burden.
>
> [snip]
>
> 17. Without Apple's assistance, the government cannot carry out the search of Farook's iPhone authorized by the search warrant. Apple has ensured that its assistance is necessary by requiring its electronic signature to run any program on the iPhone. Even if the Court ordered Apple to provide the government

> with Apple's cryptographic keys and source code, Apple itself has implied that the government could not disable the requisite features because it "would have insufficient knowledge of Apple's software and design protocols to be effective."
>
> [snip]
>
> 18. Regardless, even if absolute necessity were required, the undisputed evidence is that the FBI cannot unlock Farook's phone without Apple's assistance.
>
> [snip]
>
> 19. Apple deliberately established a security paradigm that keeps Apple intimately connected to its iPhones. This same paradigm makes Apple's assistance necessary for executing the lawful warrant to search Farook's iPhone.

On March 15, SSCI Member Ron Wyden thrice suggested someone should ask NSA if they could hack into this phone.

On March 21, DOJ wrote this:

> Specifically, since recovering Farook's iPhone on December 3, 2015, the FBI has continued to research methods to gain access to the data stored on it. The FBI did not cease its efforts after this litigation began. As the FBI continued to conduct its own research, and as a result of the worldwide publicity and attention on this case, others outside the U.S. government have continued to contact the U.S. government offering avenues of possible research.
>
> On Sunday, March 20, 2016, an outside party demonstrated to the FBI a possible method for unlocking Farook's iPhone

You might think that FBI *really did* suddenly find a way to hack the phone, after insisting over and over they could only get into it with Apple's help. Indeed, the described timing coincides remarkably well with the announcement that some Johns Hopkins researchers had found a flaw in iMessage's encryption (which shouldn't relate at all to breaking into such phones, though it is possible FBI is really after iMessages they think will be on the phone). Indeed, in describing the iMessage vulnerability, Johns Hopkins prof Matthew Green ties the discovery to the Apple fight.

> Now before I go further, it's worth noting that the security of a text messaging protocol may *not* seem like the most important problem in computer security. And under normal circumstances I might agree with you. But today the circumstances are anything but normal: encryption systems like iMessage are at the center of a critical national debate over the role of technology companies in assisting law enforcement.
>
> A particularly unfortunate aspect of this controversy has been the repeated call for U.S. technology companies to add "backdoors" to end-to-end encryption systems such as iMessage. I've always felt that one of the most compelling arguments against this approach – an argument I've made along with other colleagues – is that we just don't know how to construct such backdoors securely. But lately I've come to believe that this position doesn't go far enough – in the sense that it is woefully optimistic. The fact of the matter is that forget backdoors: *webarely know how to make encryption workat all*. If anything, this

> work makes me much gloomier about the subject.

Plus, as Rayne noted to me earlier, Ellen Nakashima's first report on this went up just after midnight on what would be the morning of March 21, suggesting she had an embargo (though that may be tied to Apple's fix for the vulnerability). [Update: Correction — her story accidentally got posted then unposted earlier than that.]

But that would require ignoring the 19 plus times (ignoring Jim Comey's March 1 testimony) that DOJ insisted the only way they could get into the phone was by having Apple's help hacking it (though note most of those claims only considered the ways that Apple might crack the phone, not ways that, say, NSA might). You'd have to ignore the problems even within these statements. You'd have to ignore the conflicting sworn testimony from FBI's witnesses (including Jim Comey).

It turns out FBI's public argument went to shit fast. Considering the likelihood they screwed up with the forensics on this phone and that there's absolutely nothing of interest on the phone, I take this as an easy retreat for them.

But that doesn't mean this is over. Remember, FBI has already moved to unlock this iPhone, of similar vintage to Farook's, which seems more central to an actual investigation (even if FBI won't be able to scream terrorterrorterror). There are two more encrypted phones FBI has asked Apple to break open.

But for now, I take this as FBI's attempt to take its claims back into the shadows, where it's not so easy to expose the giant holes in their claims.

Updated with Comey testimony.