COMING SOON TO APPLE VS FBI: LIVE WITNESSES AND DEAD TERRORISTS

Apple today revealed that the FBI intends to call two witnesses in the March 22 hearing regarding the All Writs Act order to help crack Syed Rizwan Farook's phone: what I understand to be Privacy Manager Erik Neuenschwander and its Law Enforcement Compliance lawyer Lisa Olle. The tech company declined to say whether it will call the FBI personnel who made sworn statements in the case.

Things could get interesting fast, especially if Apple calls FBI's forensics guy, Christopher Pluhar — or even better, FBI Director Jim Comey — as there's an apparent discrepancy between their sworn testimony.

Here's what Jim Comey had to say in response to a Jerry Nadler question in the March 1 House Judiciary Committee hearing.

> As I understand from the experts, there was a mistake made in the, that 24 hours after the attack where the County at the FBI's request took steps that made it hard later — impossible later to cause the phone to back up again to the iCloud. The experts have told me I'd still be sitting here, I was going to say unfortunately[?], I'm glad I'm here, but we would still be in litigation

> because — the experts tell me — there's no way we would have gotten everything off the phone from a backup, I have to take them at their word.

Comey's comments appear to conflict with this sworn declaration of FBI Christopher Pluhar.

> To add further detail, on December 3, 2015, the same day the Subject Device was seized from the Lexus IS300, I supervised my Orange County Regional Computer Forensics Laboratory ("OCRCFL") team who performed the initial triage of the Subject Device, and observed that the device was powered off, and had to be powered up, or booted, to conduct the triage.
>
> [snip]
>
> I learned from SBCDPH IT personnel that SBCDPH also owned the iCloud account associated with the Subject Device, that SBCDPH did not have the current user password associated with the iCloud account, but that SBCDPH did have the ability to reset the iCloud account password.
>
> Without the Subject Device's passcode to gain access to the data on the Subject Device, accessing the information stored in the iCloud account associated with the Subject Device was the best and most expedient option to obtain at least some data associated with the Subject Device. With control of the iCloud account, the iCloud back-ups of the Subject Device could be restored onto different, exemplar iPhones, which could then be processed and analyzed.
>
> [snip]
>
> After that conversation with Ms. Olle, and after discussions with my

> colleagues, on December 6, 2015, SBCDPH IT personnel, under my direction, changed the password to the iCloud account that had been linked to the Subject Device. Once that was complete, SBCDPH provided exemplar iPhones that were used as restore targets for two iCloud back-ups in the Subject Device's iCloud account. Changing the iCloud password allowed the FBI and SBCDPH IT to restore the contents of the oldest and most recent back-ups of the Subject Device to the exemplar iPhones on December 6, 2015. Once back-ups were restored, OCRCFL examiners processed the exemplar iPhones and provided the extracted data to the investigative team. Because not all of the data on an iPhone is captured in an iCloud back-up (as discussed further below), the exemplar iPhones contained only that subset of data as previously backed-up from the Subject Device to the iCloud account, not all data that would be available by extracting data directly from the Subject Device (a "physical device extraction").

That's true for several reasons. First, as I understand it, once the phone was turned off, such a backup would no longer be possible, so it would have not been a mistake to change the password. And while Pluhar's assertion that you can't get everything from an iCloud backup is consistent with Comey's claim (presumably Pluhar is one of the experts Comey relied on), Neuenschwander explained that that was false in his own supplemental declaration.

Note, this passage is also the first confirmation that the FBI had *already* told Apple this phone was part of the investigation by December 6, meaning it must have been one of the ones Apple provided metadata for on December 5.

There is just one way that Pluhar's declaration and Comey's statement (again, both were sworn)

can be true: if the FBI turned off the phone themselves [update: or let it drain, h/t Some Guy]. That would also mean Comey's claim that "a mistake was made in that 24 hours after the attack" would make more sense, as it would refer to the decision to turn off the phone, rather than FBI's direction to San Bernardino County to change the password.

That said, I wonder whether FBI isn't trying something else by calling Olle and Neuenschwander to testify.

As part of its reply, Apple had Senior Vice President for Software Engineering Craig Federighi submit a declaration to rebut government claims Apple has made special concessions to China. After making some absolute statements — such as that "Apple has also not provided any government with its proprietary iOS source code," Federighi stated, "It is my understanding that Apple has never worked with any government agency from any country to create a "backdoor" in any of our products or services."

I was struck at the time that the statement was not as absolute as the others. Federighi relies on what he knows, without, as elsewhere, making absolute assurances.

Which got me wondering. If any country had demanded a back door (or, for that matter, Apple's source code) would Federighi really need to know? From Neuenschwander's declaration, it sounded like a smallish team could make the back door the FBI is currently demanding, meaning he might be as high as such knowledge would rise.

So I wonder whether, in an attempt to be dickish, the government intends to ask Neuenschwander and Olle, who would be involved in such compliance issues, if they also back Federighi's statement.

We shall see. For now, I just bet myself a quarter that Apple will call Comey.