FBI CLAIMED IT CONSULTED A MANUAL RATHER THAN CELLEBRITE DIRECTLY

Yesterday, I suggested that the initial docket pertaining to efforts to search Syed Rizwan Farook's Lexus and the work phone found in it is consistent with FBI first asking Cellebrite (or some other outside party) to break into the phone before asking the court to use an All Writs Act to compel Apple to help.

In an article today in the wake of possibly incorrect reports the outside entity now helping FBI is Cellebrite, the NYT claims that FBI did try them.

> The F.B.I. has tried many ways to get into the iPhone used by Mr. Farook, such as exploiting a previous bug that allowed unsigned code to be loaded and run on the device, Stacey Perino, an electronics engineer with the F.B.I. has said in a court filing in the case.
>
> The F.B.I. also tried tools made by the agency and a mobile forensics company, Cellebrite, which let older iPhones load and run code that could crack a device passcode, Ms. Perino wrote. Cellebrite describes itself on its website as a subsidiary of Sun Corporation, a publicly traded Japanese company; it has done work for a number of government agencies.
>
> Yet none of those tools worked, Ms. Perino wrote in the court document that was filed March 10.

I think this misreads Perino's declaration, which in the section in question basically repeats what she found in the standard law

enforcement tool UFED manual.

> Those previous tools that are available cannot be used on the Subject Device because they are not signed by Apple, and the current chain of trust on the Subject Device requires Apple to have signed any software that will be allowed to run
>
> [snip]
>
> From this open source research, several forensic tools were developed that combined (1) the boot ROM code signing defeat, and (2) brute-force passcode guessing. Examples include the Cellebrite UFED tool and an FBI-developed tool. Both the Cellebrite13 and FBI tools utilize the boot ROM exploit, allowing iPhone 3GS and iPhone 4 devices to load and boot an unsigned RAMdisk containing code to brute force the device passcode. The passcode recovery process operated from RAM, and did not alter the system or user data area
>
> [snip]
>
> Apple addressed the bug, and subsequently a jailbreak (i.e., allowing code unsigned by Apple) could only occur on an iPhone after it had been booted and unlocked.
>
> 13Cellebrite is a private company that makes forensic data recovery tools for mobile devices. While I have not examined the source code for the UFED tool, based on the Cellebrite Physical Extraction Manual for iPhone and iPad (Rev 1.3) and the fact that the Cellebrite tool no longer supports iPhone 4S and later devices, I believe the UFED tool relied on the same ROM exploit. The manual states: “The extraction application does not load iOS but instead loads a special forensic

> utility to the device. This utility is loaded to the device's memory (RAM) and runs directly from there." The utility is loaded from recovery mode.

It does not reveal that DOJ agencies continue to request Cellebrite's help on more sophisticated phones, nor that Cellebrite advertises the ability to crack iOS 8 phones (which is still an earlier operating system than Farook's phone runs).

Perino's passage is one that Apple's Erik Neuenschwander discussed, dismissively, at length.

> 21. Paragraphs 25 through 28 of the Perino Declaration describe supposedly already existing software that Mr. Perino suggests Apple use as a starting point to create GovtOS. For example, Mr. Perino points to a security exploit that supposedly allowed an iPhone to load a minimal operating system in RAM that had not been signed by Apple, which is what the government is requesting here. Similarly, Mr. Perino points to a hacking tool the FBI created that supposedly allowed it to brute force the device passcode on older iPhones.
>
> *22. These descriptions show that the FBI, along with its partners, currently have, and have had in the past, the capability to develop the types of code that Apple is being asked to create.*
>
> 23. Mr. Perino is incorrect, however, in his suggestion that Apple can use these third-party items, add Apple's signature, and load the finished product on to the subject device to accomplish the result that the government seeks with less effort than what I described in my initial declaration.
>
> 24. Using the allegedly already existing software code that Mr. Perino identifies

> would not be an appropriate way to accomplish what the government wants. Setting aside the legal question of whether Apple can incorporate a software tool created by some other party (such as the Cellebrite UFED tool Mr. Perino identifies) for this purpose, Apple would not save time and effort by incorporating unfamiliar third-party code that has never been used and deployed by Apple before, and it would introduce a host of new issues and potential risks that would need to be addressed. [my emphasis]

Of particular note, Neuenschwander noted that "FBI, along with its partners, currently have…the capability to develop the types of code that Apple is being asked to create." Cellebrite was the only partner listed by name.

Neuenschwander went on to note that the jailbreaking Perino described is precisely why Apple works so hard to improve its security.

The NYT wants to claim FBI researched all possibilities before repeatedly claiming, more than 19 times (I did not include Perino's declaration in my count), that only the FBI or Apple could open this phone.

But Perino's declaration understates what Cellebrite itself claims to be able to do — and that DOJ asks Cellebrite to do.

That still doesn't mean Cellebrite is the entity now helping FBI crack the phone. It does mean FBI and DOJ engaged in affirmatively misleading briefing on whether Cellebrite might be able to do so.