ON FEBRUARY 16, DOJ GOT A WARRANT TO OPEN AN IPHONE 6 USING CELLEBRITE

As a number of outlets are reporting, the Israeli security firm Cellebrite is the source the FBI is using to attempt to break into Syed Rizwan Farook's phone.

> Israel's Cellebrite, a provider of mobile forensic software, is helping the U.S. Federal Bureau of Investigation's attempt to unlock an iPhone used by one of the San Bernardino, California shooters, the*Yedioth Ahronoth* newspaper reported on Wednesday.
>
> If Cellebrite succeeds, then the FBI will no longer need the help of Apple Inc, the Israeli daily said, citing unnamed industry sources.
>
> Cellebrite officials declined to comment on the matter.

According to the narrative the government is currently telling, it means 33 days after DOJ obtained an All Writs Act on February 16 ordering Apple to help unlock Farook's phone, and 108 days after FBI first seized the phone on December 3 — during which entire period the FBI *now* claims they were diligently researching how to crack the phone — on March 20, Cellebrite contacted the FBI out of the blue and told them they can help.

That's interesting, especially given this search warrant, approved (as coinkydink would have it) on February 16, the very same day DOJ got its AWA in California.

Among the phones DEA obtained a warrant to search was an iPhone 6, a later model than Farook's phone with default encryption (though

running unknown iOS). Here's what DEA Task Force Officer Shane Lettau had to say about how he (might) access the contents of this iPhone 6.

> **Apple iPhone, Model A1549, bearing IMEI: 359296065756836, FCC ID# BCG-E2816A; (A photograph of the cellular phone appears in Attachment A2).** The device will be charged and powered on. The device and all readable and searchable contents will be attempted to be downloaded to a "CellBrite" device. The "CellBrite" device allows the user to bypass any password protected utility on the phone. The contents downloaded on the CellBrite device will then be copied to a readable computer disc and reviewed by your affiant. However, your affiant knows through experience that Apple devices hold a unique encryption that typically only Apple Inc. can bypass. Therefore, it is possible that your affiant may have to send the SED to Apple Inc. located in California for the search. A search warrant return will be provided to the Court thereafter.

To be sure, these phones aren't the same, nor is the agency. Farook's is a 5C running iOS 9, this is a 6, and we don't know what iOS it is running. But if Cellebrite can break into a 6 they presumably can break into a 5C. FBI is seeking access in CA, whereas this MD phone is in DEA's possession.

The point is, however, that it is inconceivable to claim, as DOJ did 19 times, that the only way they could get into Farook's phone was with Apple's help when DOJ was at the same time participating in DEA's discussions with Cellebrite about whether they could crack a later model phone. It may be that Cellebrite only perfected their technique with iOS 8 and later model phones in recent weeks, or that they could not crack an iOS 9 in December or February but have since perfected that, but DOJ still shouldn't have been submitting sworn declarations pretending that Cellebrite was not a possible option.

Update: I originally said Farook's phone was a 5S. I've corrected the post to say it is a 5C, h/t JC.

Update: FBI signed a contract with Cellebrite on the same day it announced it had found a solution, though I think it's for license renewals for 7 machines in Cook County.