DID FBI ASK CELLEBRITE TO OPEN FAROOK'S PHONE BEFORE GETTING AN AWA ORDER?

In this post, I note that DOJ obtained a warrant to search (among other things) an iPhone 6 using Cellebrite's assistance on the same day as it obtained an All Writs Act order to Apple to help crack Syed Rizwan Farook's iPhone 5C. That other warrant demonstrates not only that DOJ was at least willing to *try* opening a late model iPhone with Cellebrite's help during the same period it was claiming it could only do so with Apple's help, but it also shows us what it would look like if DOJ tried to enlist Cellebrite's help.

I'd like to look at the underlying "warrant" such as it exists for this phone. There are two dockets in this case. 5:15-mj-00451, the docket under which DOJ got a search warrant for Farook's (actually, his mother's) Lexus. And 5:16-cm-00010, where the fight with Apple lives. The order for an All Writs Act actually lives in the earlier docket, with the first numerical docket item in the newer one is the government's motion to compel.

Technically, we have never seen any free-standing warrant for Farook's phone. Rather, what got attached to the AWA order application was actually the warrant for the Lexus. That warrant includes a bunch of boilerplate language about any devices found in the car, which basically permit authorities to search a device to find out if it contains any items covered by the search warrant, but requiring further legal order to keep that information.

> g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

Obviously, FBI hasn't gotten to the point where they've found the phone includes evidence relating to the crime, because they haven't yet been able to search the phone, so they haven't gotten the point where they'd need this "further court order." Moreover, the phone doesn't belong to Farook, it belongs to San Bernardino County, and they've consented to any search (but you can't get an AWA unless you have a search warrant).

But it appears DOJ covered their asses, given the following entries in the original docket.

12/21/2015	5	Search and Seizure Warrant Returned Executed on 12/21/15 (Case terminated.) (ja) (Entered: 12/22/2015)
01/26/2016	6	GOVERNMENT'S EX PARTE APPLICATION for Order Sealing Document Filed by Plaintiff USA. (ad) (mrgo). (Entered: 01/27/2016)
01/26/2016	7	ORDER SEALING DOCUMENT by Magistrate Judge Sheri Pym. (ad) (mrgo). Modified on 2/25/2016 (ad). (Entered: 01/27/2016)
01/26/2016	8	GOVERNMENT'S EX PARTE APPLICATION for Order Unsealing Search and Seizure Warrant and Attachments A, A-2 and B Filed by Plaintiff USA. (ad) (mrgo). (Entered: 01/27/2016)
01/26/2016	9	ORDER UNSEALING Search and Seizure Warrant and Attachments A, A-2 and B ONLY by Magistrate Judge Sheri Pym. (ad) (mrgo). Modified on 2/25/2016 (ad). (Entered: 01/27/2016)
01/29/2016	10	EX PARTE APPLICATION for First Extension of Time Within Which to Retain and Search Digital Devices Filed by Plaintiff USA as to Defendant Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification Number JTHBD192X50094434. (mrgo) (Entered: 02/02/2016)
01/29/2016	11	ORDER by Magistrate Judge Sheri Pym: granting 10 EX PARTE APPLICATION for Order as to Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification Number JTHBD192X50094434 (1). (mrgo) (Entered: 02/02/2016)
01/29/2016	12	EX PARTE APPLICATION FOR ORDER SEALING DOCUMENTS as to Defendant Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466 Vehicle Identification Number JTHBD192X50094434. Filed by Plaintiff USA as to Defendant Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification Number JTHBD192X50094434. (mrgo) (Entered: 02/02/2016)
01/29/2016	13	ORDER by Magistrate Judge Sheri Pym: granting 12 EX PARTE APPLICATION to Seal Document as to Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification Number JTHBD192X50094434 (1). (mrgo) (Entered: 02/02/2016)
02/02/2016	14	GOVERNMENT'S EX PARTE APPLICATION FOR ORDER SEALING DOCUMENT Filed. (ad) (Entered: 02/04/2016)
02/02/2016	15	ORDER SEALING DOCUMENT by Magistrate Judge David T. Bristow. (ad) (Entered: 02/04/2016)
02/02/2016	16	GOVERNMENT'S AMENDED EX PARTE APPLICATION FOR ORDER UNSEALING THIS MATTER, Specifically the Search Warrant and Attachments, All Else Remain Under Seal Filed. (ad) (Entered: 02/04/2016)
02/02/2016	17	ORDER UNSEALING THIS MATTER, SPECIFICALLY THE SEARCH WARRANT AND ATTACHMENTS, ALL ELSE TO REMAIN UNDER SEAL by Magistra Judge David T. Bristow. (ad) (Entered: 02/04/2016)

As I understand it, this warrant docket was terminated on December 21. But then on January 26, it got active again, with the government sealing a document, then unsealing the parts of the search warrant. Then, on January 29, the government applied for and got and then sealed an extension of time on the original warrant, but noting they just needed an extension for devices related to it (that is, for Farook's phone). Then on February 2, they submitted and got sealed another document. Finally, they got parts of the original warrant that had been unsealed in part days earlier unsealed (again?) so they could get the AWA, which they did.

I'm interested in all this for several reasons. First, if they closed this docket in December, *after they had already obtained the content of Farook's iMessage account*, does that indicate they had determined the phone had no evidence relating to the crime? That's consistent with what everyone believes. But it would also seriously undermine their claims that they do need the information (especially since the claims they made in their AWA application

are inconsistent with that they've claimed in later documents).

I also suspect that FBI asked Cellebrite to open this phone. If I'm reading the docket correctly, the parts of the search warrant pertaining to the phone have been unsealed twice, the latter time for the AWA. I suspect the earlier activity in the docket pertained to a Cellebrite request, in which case the February 2 docket document might resemble the method of search language, naming Cellebrite, found in the February 16 warrant for the iPhone 6 in the other case.

The thing is, Judge Pym may know that, if that's the case, because she's the one who signed off on the January 26 and 29 activity. Which is interesting given that, in the phone hearing on whether to vacate the hearing yesterday, she suggested FBI might need to brief on what this effort was.

> I'm not — to some extent I'm not sure how much difference it makes whether the order is vacated at this point or not, because if it turns out, after exploring this possibility, that the FBI believes it won't work, you know, I would be inclined to go forward without really — and there might need to be some additional briefing, supplemental submissions, with respect to this effort, but I think the matter's been fully briefed.

She may be less willing to decide for FBI if she knows that Cellebrite is actively working on a solution that would solve FBI's needs, which she may already know.

In any case, given the import of this case, citizens really deserve to know what the government was asking for at the end of January, particularly if their first effort to get into the phone involved a request to Cellebrite that has now been answered.