FBI'S LATEST STORY ABOUT THE HACK OF FAROOK'S PHONE

There's a lot that doesn't quite make sense in Ellen Nakashima's explanation for how FBI broke into Syed Rizwan Farook's iPhone.

> The FBI cracked a San Bernardino terrorist's phone with the help of professional hackers who discovered and brought to the bureau at least one previously unknown software flaw, according to people familiar with the matter.
>
> The new information was then used to create a piece of hardware that helped the FBI to crack the iPhone's four-digit personal identification number without triggering a security feature that would have erased all the data, the individuals said.
>
> The researchers, who typically keep a low profile, specialize in hunting for vulnerabilities in software and then in some cases selling them to the U.S. government. They were paid a one-time flat fee for the solution.
>
> [snip]
>
> At least one of the people who helped the FBI in the San Bernardino case falls into a third category, often considered ethically murky: researchers who sell flaws — for instance, to governments or to companies that make surveillance tools.
>
> This last group, dubbed "gray hats," can be controversial. Critics say they might be helping governments spy on their own citizens. Their tools, however, might also be used to track terrorists or hack

> an adversary spying on the United States. These researchers do not disclose the flaws to the companies responsible for the software, as the exploits' value depends on the software remaining vulnerable.

Don't get me wrong. I don't doubt Nakashima is reporting what she learned; I know other reporters were working on a similar direction.

It's just that the FBI's currently operative story still makes no sense. For starters, why would the FBI pay someone selling zero days but not be willing to consider the solutions offered by (just as an example of one forensics person I know who offered to help) Jonathan Zdziarski?

And I still wonder why the government apparently unsealed the warrant in Farook's case once before it unsealed it to compel Apple. Indeed, while Nakashima (and other reporters) says FBI "did not need the services of the Israeli firm Cellebrite," I still think using them (or someone similar) as a middle-man might offer the best of all worlds: no official possession of this exploit, easy contracting, the ability to give (as FBI has been) conflicting stories without any of them being fully false. Just as an example, if Cellebrite told FBI it currently couldn't crack the phone before FBI got an All Writs Act order obligating Apple, then FBI could fairly claim, as they did, that only Apple or FBI could open the phone (even if they hadn't actually asked many other people who might be able to hack the phone). But if someone went to Cellebrite or even FBI with the exploit after that, then FBI would have a way of using the exploit without having it and therefore having to submit it to the Vulnerabilities Equities Process (though technically they should still have to). FBI would have a way of promising to keep the exploit hidden, which the vendor would require, because it would technically never be in possession of it.

There's one more thing that is getting lost in

this debate. Comey and others keep talking about the use of this for an intelligence function, as if to justify keeping this exploit secret. I know that's the convenient part of using a terrorism case to raise the stakes of back dooring phones. But this is ultimately a law enforcement issue, not an intelligence one, no matter how much FBI wants to pretend we're going to find out something going forward. And as such it should be subject to greater standards of disclosure than a pure use of an exploit for intelligence purposes would.

In other words, FBI is still playing word games.