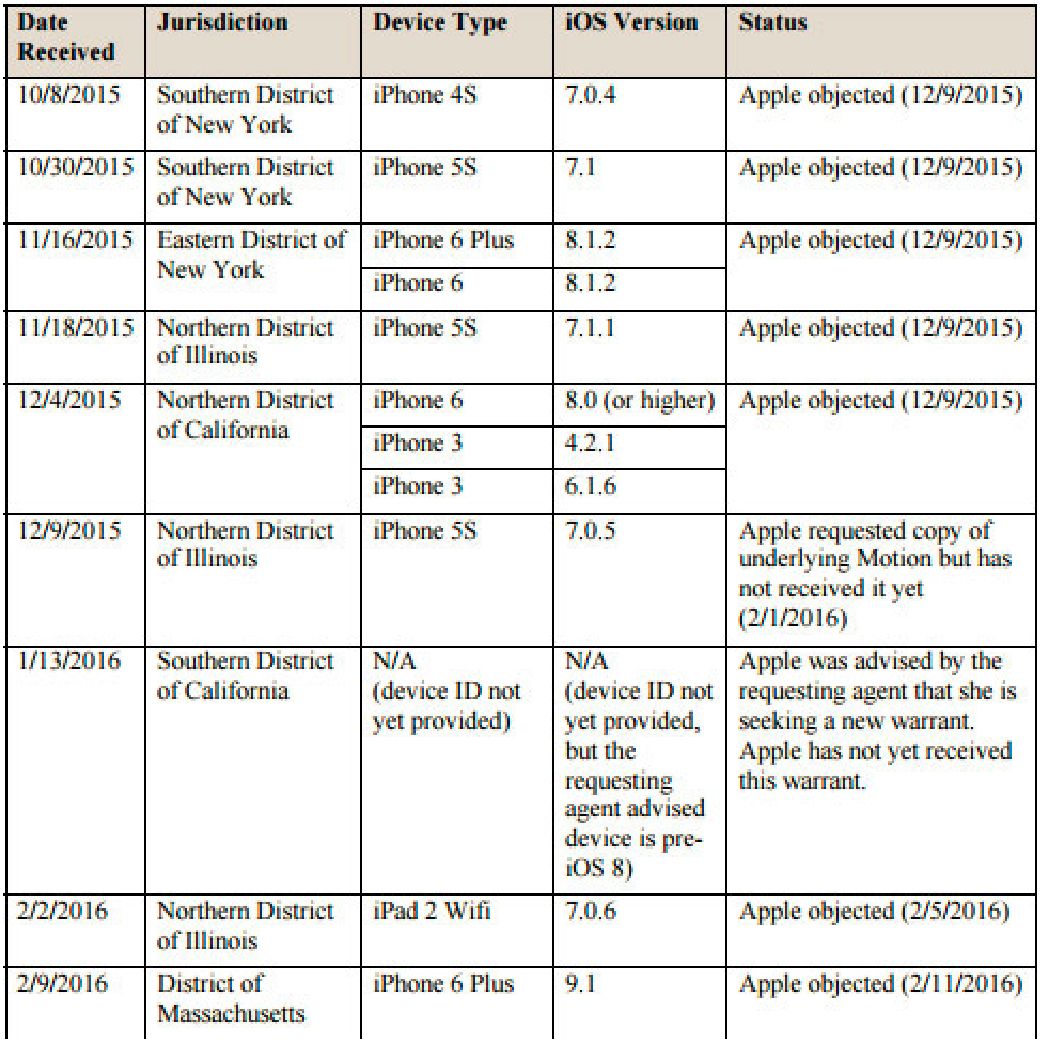
Exhibit B

How the Feds Could Get Into iPhones Without Apple's Help

It's a showdown that has the country mesmerized. In court battles brewing across the nation, the FBI is trying to force Apple to help it extract data from iPhones seized in more than a dozen cases.

The government is so intent on forcing Apple's hand that in each case the Justice Department has invoked the 200-year-old law All Writs Act to do it. But application of the Act requires the government to show that it has no other method of extracting data from the phones. And according to experts who spoke with WIRED, that's not necessarily the case. They say there are ways the government can extract data on phones without Apple's help, from using outside contractors to asking its friends at the NSA—ways that it has, in fact, already used in the past. The solutions won't work for every iPhone the government has collected, and the solution offered for extracting data from the phone in San Bernardino involves some speculation about the NSA's capabilities. But they do raise questions about whether the government has done everything it can do to collect the data it says it needs.



Date Received	Jurisdiction	Device Type	iOS Version	Status
10/8/2015	Southern District of New York	iPhone 4S	7.0.4	Apple objected (12/9/2015)
10/30/2015	Southern District of New York	iPhone 5S	7.1	Apple objected (12/9/2015)
11/16/2015	Eastern District of New York	iPhone 6 Plus	8.1.2	Apple objected (12/9/2015)
		iPhone 6	8.1.2	
11/18/2015	Northern District of Illinois	iPhone 5S	7.1.1	Apple objected (12/9/2015)
12/4/2015	Northern District of California	iPhone 6	8.0 (or higher)	Apple objected (12/9/2015)
		iPhone 3	4.2.1	
		iPhone 3	6.1.6	
12/9/2015	Northern District of Illinois	iPhone 5S	7.0.5	Apple requested copy of underlying Motion but has not received it yet (2/1/2016)
1/13/2016	Southern District of California	N/A (device ID not yet provided)	N/A (device ID not yet provided, but the requesting agent advised device is pre-iOS 8)	Apple was advised by the requesting agent that she is seeking a new warrant. Apple has not yet received this warrant.
2/2/2016	Northern District of Illinois	iPad 2 Wifi	7.0.6	Apple objected (2/5/2016)
2/9/2016	District of Massachusetts	iPhone 6 Plus	9.1	Apple objected (2/11/2016)

Chart showing other cases in which the government is using the All Writs Act to compel Apple to assist it in extracting data from iPhones. Not included in this chart is the San Bernardino case or the one involving the drug case in New York.

The Commercial Ways In

According to one expert in the forensic industry who spoke with WIRED on condition of anonymity, there are commercial solutions that could possibly help the government extract data from more than half the iPhones in question and possibly more—the phones are running various versions of operating system ranging from 4.2.1 to 9.0. Many of these capabilities involve defeating security mechanisms put in place by Apple and the phone owners, such as encryption and passcodes.

"Forensic companies have been working on ways to extract evidence from mobile phones for years," says the expert. "They develop proprietary software and hardware to do that. It is well-known that these solutions exploit vulnerabilities on the device that allow them to perform these extractions."

The FBI in fact has a sole-source contract with one of them, a mobile forensic firm founded in Israel called Cellebrite. The company offers data-extraction services and tools for iPhones, Android and Windows phones and Blackberries. And according to its web site, this includes extracting data from locked phones that are using any version of operating system up to 8.4.1, the last version of iOS8 that Apple released.

It's a service the company only began providing last year for iOS 8, according to a newsletter it published last August. The first version of iOS 8 was released by Apple in September 2014.

"Cellebrite has a unique unlock capability for devices running iOS 8.x that will provide you with unprecedented access to evidence you can stand behind," the company says on its web site. "This unique capability is the first of its kind—unlock of Apple devices running iOS 8.x in a forensically sound manner and without any hardware intervention or risk of device wipe."

This could possibly have worked in the case of the phone in New York and in other cases where the FBI is trying to force Apple to help extract data. The New York case, which the judge ruled on yesterday in Apple's favor, involved a drug suspect whose phone was seized by Drug Enforcement Agency agents. The agents obtained a warrant to search the phone, but during the two-week window covered by the warrant, they were unable to access data stored on it. The government "initiate[d] the execution of the search warrant by attempting to search the device, turning it on and placing it in airplane mode," the court ruling reads. "The [DEA] agents … began that search but were unable to complete [it] because" the device required a password to allow access to certain information… The DEA agents then sought the assistance of the Federal Bureau of Investigation ("FBI"), but remained unable to bypass the iPhone's passcode security."

The government asserted in that case that "examining the iOS device further without Apple's assistance, if it is possible at all, would require significant resources and may harm the iOS device." But Cellebrite uses what's called a boot-loader extraction method with phones like this. A custom operating system gets loaded into the device's memory during the boot sequence and makes the user-data partition read-only.

"This guarantees the forensic soundness of the extraction, unlike other methods," the forensic expert says.

Asked to clarify if it actually involves unlocking the phone or simply extracting data from it, he replied, "it's quite similar to what FBI is asking Apple to do [in the San Bernardino case] but Cellebrite is able to create a situation where you can bruteforce the passcode."

In the San Bernardino case, the government has asked a California court to force Apple to write a new version of its operating system that eliminates certain protections against bruteforcing the passcode that exist in the iOS9 software that's running on the phone.

The forensic expert won't describe how the commercial forensic tool for other versions of iOS works in detail. "Apple can close that, so if they realize what forensic investigators are doing, they can fix the vulnerability," he says. In fact, Apple may already have fixed it in iOS 9, since the method no longer works for that version of its operating system.

"The presumption is that they have a vulnerability that's basically a jailbreak for a locked phone," says Nicholas Weaver, a senior researcher at the International Computer Science Institute at UC Berkeley. Generally jailbreaking a phone—which removes software restrictions written into the code by the phone maker—requires the phone to be unlocked; but this would allow jailbreaking, and data extraction, from a phone that is locked. "It's a harder vulnerability to find than most jailbreaking vulnerabilities," Weaver says.

The solution wouldn't work on the San Bernardino phone, since that device uses iOS 9, for which there is currently no commercial solution, the expert says; he notes, however, that forensic analysts are currently working on finding a solution to get into the latest iOS9 phones as well.

The current method *would* work with most versions of iOS 7, though the amount of effort involved varies with different versions, the forensic expert says. It's not clear if it would work with the specific phone in New York, however, since the exact version of iOS 7 on that phone is unknown. Apple did not respond to inquiries asking about the phone. But the government is using the All Writs Act to force Apple's assistance in opening at least five other iPhones that use various versions of iOS 7.

Paging the NSA

Weaver says there is one possible method the government could use to crack the San Bernardino iPhone without Apple's help. It would involve a vulnerability and exploit for the phone's baseband.

Operating system exploits for the iPhone—that allow investigators to hack a phone that is still being actively used by a target—can be very powerful but also very expensive. Zero-day exploit seller Zerodium claimed last year that it paid $1 million for an iOS zero-day exploit. Such an exploit wouldn't help in the San Bernardino case, since the phone would need to be unlocked.

But a baseband zero-day would.

iPhones don't have just one operating system, but two. A second low-level operating system in the baseband controls the cellular interface, which means if investigators can take over that operating system, they can take over the phone. Since a booted iPhone will connect to a nearby cellular network even before you enter a passcode, investigators could get it to connect to a rogue cell tower that they control—a more powerful version, for example, of a stingray—and use an exploit to take over the phone. But they would need to have an exploit capable of attacking a vulnerability in the baseband operating system.

"Once you have the baseband exploited you're able to bypass all that bruteforce protection and just try all the passwords that you want," Weaver says. "If you take over the baseband, you have the ability to write to memory, which means you can take over the running operating system. And because the phone is running but locked, you take over that running but locked operating system and now you can do what the FBI wants to do, where you just keep trying PINs against the secure enclave until you get in…So you corrupt the root operating system to say, don't do these protections."

The FBI may not have access to a $1 million baseband exploit if one exists, but it likely has friends who do. Apple suggested in its brief last week, that there may be some untapped resources the government has failed to tap to help it get into the San Bernardino phone. The government, Apple wrote, "has not made any showing that it sought or received technical assistance from other federal agencies with expertise in digital forensics, which assistance might obviate the need to conscript Apple to create the back door it now seeks."

Who might provide the kind of assistance the FBI needs? The obvious answer is the NSA.

"My hunch is that the NSA does have exploits for iPhones—operating system exploits and baseband exploits," says Weaver. And if that's the case, it would greatly undermine the government's contention that only Apple can help it get into the phone.

But does the NSA have the ability to help the FBI crack the phone?

FBI Director Comey suggested to Congress on Tuesday that it doesn't. He told lawmakers that the FBI has "talked to anybody who will talk to us about [the phone]," when asked if he had spoken to other government agencies.

Nate Cardozo, a lawyer for the Electronic Frontier Foundation, finds this hard to believe.

“The best hackers in the world are employed over at Fort Meade,” where the NSA is located, says Cardozo. “They’re not at Quantico,” the FBI’s home base. “The phone is at Quantico. That, I think, speaks volumes about what’s going on here.”

Either the NSA doesn’t have the ability to open the phone or doesn’t want to risk exposing its methods in a very public case like the San Bernardino one. Or there’s another reason why the FBI might be claiming helplessness when it comes to the phone.

Cardozo and other experts say the fact the FBI has opted for a very public legal battle in the case when other methods for getting the data may be at its disposal suggests that the case is not about getting data but about setting a legal precedent. Specifically, a precedent that could compel Apple and other tech companies to create or alter their software to make it less secure.

“This case was selected very carefully by the FBI in order to develop precedent going forward,” Cardozo says. “They want to be able to order American tech companies to include (or remove) specific features in order to enable surveillance. They’ve never before claimed such a power.”

So while there may be other ways the FBI could get into the cache of iPhones it currently has—and maybe even into the San Bernardino iPhone—that may be beside the point.

Brian Barrett contributed reporting.