THE NEW YORKER

THE DANGEROUS ALL WRITS ACT PRECEDENT IN THE APPLE ENCRYPTION CASE

By Amy Davidson Sorkin February 19, 2016

Tim Cook, the C.E.O. of Apple, which has been ordered to help the F.B.I. get into the cell phone of the San Bernardino shooters, wrote in an angry open letter this week that "the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create." The second part of that formulation has rightly received a great deal of attention: Should a back door be built into devices that are used for encrypted communications? Would that keep us safe from terrorists, or merely make everyone more vulnerable to hackers, as well as to mass government surveillance? But the first part is also potentially insidious, for reasons that go well beyond privacy rights.

The simple but strange question here is exactly the one that Cook formulates. What happens when the government goes to court to demand that you give it something that you do not have? No one has it, in fact, because it doesn't exist. What if the government then proceeds to order you to construct, design, invent, or somehow conjure up the thing it wants? Must you?

The F.B.I.'s problem is that it has in its possession the iPhone used by Syed Rizwan Farook, one of the San Bernardino shooters, but the phone is locked with a passcode that he chose. (The phone, which investigators found while executing a search warrant for Farook's car, is actually the property of the San Bernardino County Health Department, Farook's employer, which has consented to its search—and so, as Orin Kerr points out, on the Washington *Post* blog the Volokh Conspiracy, there is no Fourth Amendment issue there.) If the F.B.I. enters the wrong passcode ten times, the data may be turned to gibberish. And if the F.B.I. disables that feature, allowing it to enter every possible passcode until it hits the right one, it may still come up against another barrier: a built-in delay between wrong entries, so that typing in five thousand

possibilities, for example, might take thousands of hours. Both sides agree that Apple has given significant technical assistance with the San Bernardino case already; in response to a separate warrant, it gave the F.B.I. the iCloud back-ups for Farook's phone (the most recent was from some weeks before the shooting). In the past, in response to court orders, Apple has helped the government extract certain specific information from older iPhones—perhaps seventy times, according to press reports. But there is apparently no way for the company to do so on the newer operating system, iOS 9, which the shooter was using and which was built without a "back door." In other words, there is no set of instructions or a skeleton key in a drawer somewhere in Cupertino that Apple could give the F.B.I. to allow it to get in.

And so Sheri Pym, a California district-court magistrate judge, has ordered Apple to come up with a new software bundle that can be loaded onto the phone and, in effect, take over the operating system and tell it to let the F.B.I. in. (Apple will have a chance to object to the order in court.) As an added point of convenience, this bundle is also supposed to let the agents enter passcodes electronically, rather than tapping them in, which is one of the many points on which the government seems to have moved from asking for compliance with a subpoena to demanding full-scale customer service. In its request for the order, the government says that "Apple has the exclusive technical means which would assist the government in completing its search," for a number of reasons. One is that iPhones look for a cryptographic signature before accepting operating-system software as legitimate. But the government, again, is not asking for a signature or even for the equivalent of a handwriting guide (which would be problematic, too) but for an entire ready-to-run bundle. It has said that it wants Apple to put in a code that makes the bundle usable only on Farook's phone—but that is a desire, not a description of an existing, tested, software protection. (The government also says that it will pay Apple for its work.) The other reasons that the government says that Apple should be compelled to do this work come down to Apple being Apple—being a smart company that designs this kind of thing. What is the government's claim on that talent, though? Would it extend to a former engineer who has left the company? The government's petition notes that the operating system is "licensed, not sold," which is true enough, but conveys the darkly humorous suggestion that Apple's terms of service are holding the F.B.I. back.

It is essential to this story that the order to Apple is not a subpoena: it is issued under the All Writs Act of 1789, which says that federal courts can issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." Read as a whole, this simply means that judges can tell people to follow the law, but they have to do so in a way that, in itself, respects the law. The Act was written at a time when a lot of the mechanics of the law still had to be worked out. But there are qualifications there: warnings about the writs having to be "appropriate" and "agreeable," not just to the law but to the law's "principles." The government, in its use of the writ now, seems to be treating those caveats as background noise. If it can tell Apple, which has been accused of no wrongdoing, to sit down and write a custom operating system for it, what else could it do?

In the motion filed on Friday, the government dismissed Apple's objection by saying that it "appears to be based on its concern for its business model and public brand marketing strategy," and that writing new code shouldn't be an "undue burden"—one of the standards for applying the All Writs Act—since Apple writes a lot of code. This particular use of the All Writs Act is fairly novel, however. The precedent the government's supporters cite is the use of All Writs in a 1977 Supreme Court decision involving telephone taps, called pen registers. In that case, the F.B.I. wanted New York Telephone, which was already helping it to set up a tap in an illegal-gambling sting, to let it use some spare cables that were, physically, in the same terminal box as those hooked up to the suspect's phone. The telephone company told the F.B.I. to get its own wires and string them into the apartment of one of the alleged gamblers some other way. When the F.B.I. objected that the suspects might spot the rigged cables, the Court agreed that it could legitimately ask the telephone company for its technical help and "facilities." But the F.B.I. wasn't asking New York Telephone to design a new kind of cable.

If a case involving a non-digital phone network could be applied to smartphones, what technologies might an Apple precedent be applied to, three or four decades from now? (The N.S.A. used, or rather promiscuously misused, another pen-register case from the same era to justify its bulk data collection.) It no longer becomes fanciful to wonder about what the F.B.I. might, for example, ask coders adept in whatever genetic-editing language emerges from the recent developments in CRISPR technology to do. But

some of the alarming potential applications are low-tech, too. What if the government was trying to get information not out of a phone but out of a community? Could it require someone with distinct cultural or linguistic knowledge not only to give it information but to use that expertise to devise ways for it to infiltrate that community? Could an imam, for example, be asked not only to tell what he knows but to manufacture an informant?

This is the situation that Apple is in, and that all sorts of other companies and individuals could be in eventually. There are problems enough with the insistence on a back door for devices that will be sold not only in America but in countries with governments that feel less constrained by privacy concerns than ours does. And there are reasons to be cynical about technology companies that abuse private information in their own way, or that jump in to protect not a principle but their brands. But the legal precedent that may be set here matters. By using All Writs, the government is attempting to circumvent the constitutionally serious character of the many questions about encryption and privacy. It is demanding, in effect, that the courts build a back door to the back-door debate.

Amy Davidson Sorkin, a New Yorker staff writer, is a regular contributor to Comment for the magazine and writes a Web column, in which she covers war, sports, and everything in between. Read more »