LAWFARE

GOING DARK

Apple is Selling You a Phone, Not Civil Liberties

By **Susan Hennessey**, **Benjamin Wittes** Thursday, February 18, 2016, 12:32 PM

Note to Apple: As a general matter of strategic communications, following the words "We have no sympathy for terrorists" with a "But" generally means you've gone badly off message—even if you wedge a few sentences in between.

Unless you've been living in a cave, you already know by now that a federal magistrate judge in California has issued an order to compel the technology giant to provide technical assistance to the FBI in unlocking the iPhone of one of the San Bernardino mass shooters.

(If you *have* been living in a cave, more bad news: Justice Scalia is dead and Kanye West is in debt.)

Apple is outraged. In "A Message to Our Customers," it declares this "unprecedented step" a threat to "the security of our customers," who—it piously intones—"expect Apple and other technology companies to do everything in our power to protect their personal information." Apple has tried to be helpful to the bureau, the company contends. "But"—and here's the big But—"now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They asked us to build a backdoor to the iPhone." The company is promising a fight: "We are challenging the FBI's demands with the deepest respect for American democracy and a love of our country."

We will leave for another day the question of whether a multinational corporation with shareholders and customers worldwide and production in China, is meaningfully capable of patriotism, let alone love. In prior posts, we have offered some resources and background that might be useful to commentators and citizens looking to wrap their minds around how a 227-year old law came to be applied to an iPhone operating iOS9, what the scope of the company's obligation to provide "technical assistance" investigators really is, and what any of this has to do with "going dark."

In this post, however, we want to make an argument: Apple is being mischievous here, and the company's self-presentation as crusading on behalf of the privacy of its customers is largely self-congratulatory nonsense. In reality, the case poses starkly the stakes in the "Going Dark" debate. What's more, it was entirely predictable; indeed, one of us predicted it with some precision barely a month ago. Far from the "unprecedented" "overreach" of Apple's rhetoric, given the uncertain state of the law and the stakes in the case in question, it would have been akin to malpractice for the FBI and Justice Department to *not* fully explore the scope of Apple's obligation to help the government effectuate a warrant in a major ISIS case.

More particularly, given the company's simultaneous opposition to any legislation to clarify industry obligations as companies implement stronger encryption systems and its insistence that current law cannot force it to help the government, we submit that Apple is really trying to carve out a zone of impunity for itself that rightly alarms the government and should alarm the very citizens the company (which calls these citizens "customers") purports to represent. The company's near-duplicitous posture thus highlights the urgent need for a legislative intervention spelling out who has what obligations in situations like this one, situations that will only grow more common in the coming months and years.

Let's start with an important fact that Apple elides in its statement: Apple engineered this problem and it did so intentionally. In 2012, Apple specifically decided to encrypt communications end-to-end and data at rest by default on the devices it manufactures and to not maintain any ability to decrypt material unless users specifically gave it the power to recover that material. The categories of data intentionally placed out of Apple's reach—and law enforcement's—expanded signficantly in the years following Snowden and high profile celebrity hacking incidents. It boasted about this decision and used it as a marketing weapon against its competitors. Reasonable people can argue about whether or not Apple did so for good reasons and whether or not doing so was the optimal way for the company to enhance the cybersecurity of its users. But the simple fact remains that Apple used to have the capacity to comply with warrants, and now it cannot without a certain amount of reengineering. And that was a matter of its own choosing made despite repeated warnings from the government that this choice would cause substantial problems for law enforcement, national security investigators, and public safety.

In response to FBI expressions of alarm at this development, civil libertarians and cryptographers have made a number of arguments. For present purposes, two stand out. First, the Going Dark skeptics demand, show us the cases in which the absence of extraordinary law enforcement access to encrypted data is actually posing a problem. And this demand seemed quite reasonable, in our view. If the FBI wants to take the position that it has a problem, it has to do more than cry wolf. Show us the wolf.

And in the last couple of weeks, the bureau has shown some serious wolf. Consider this excerpt from Director James Comey's testimony before Congress last week: "A woman was murdered in Louisiana last summer, eight months pregnant, killed, no clue as to who did it, except her phone is there when she's found killed. They couldn't open it, still can't open it. So the case remains unsolved." (The discussion is available here starting at 31:00.)

Then came the filing in the San Bernardino case this week. Note that this is a case that has a potentially serious ISIS link. The FBI has been sitting on one of the shooter's phones for more than two months, unable to open it. It wants Apple's help to determine "who [the shooters] may have communicated with to plan and carry out the IRC shootings, where Farook and Malik may have traveled to and from before and after the incident, and other pertinent information that would provide more information about their and others' involvement in the deadline shooting."

This is, in other words, a law enforcement and intelligence interest of the highest order: involving knowing for criminal justice purposes who may have been involved in an attack that took place within the United States and for prospective purposes who may be planning other such attacks. The case illustrates how the investigation of crimes is often linked to crime prevention. The phone is actually owned by the shooter's employer, which has consented to the search. And there's a warrant too. So there's no legal issue with FBI access to the data whatsoever.

The only impediment is Apple.

We submit that it is the government's job in such cases to investigate the crime to the extent it is legally permitted to do so. Nobody should expect the FBI to leave a shooter's phone unexamined when the bureau has a defensible legal argument that a company is obliged to help it access the contents.

Here's the brief:

A second key argument that Going Dark skeptics have advanced is that the FBI doesn't really need backdoors, because it can always hack devices. This is a complicated argument, and an interesting one. But in order for it to be a genuinely constructive suggestion and not merely a diversionary tactic, we must confront the question of whether companies have any legal obligation to *help* the government hack their devices. There are various provisions in federal law that require that companies to give "technical assistance" to law enforcement carrying out wiretaps and lawful surveillance orders. And where this is a "gap" in legislation, there is the All Writs Act. The question of how these statutes might apply to a locked phone the government decides to hack is one that follows ineluctably from the decision to rely on device hacking, rather than, say, a decision to try to decrypt.

So to review the bidding, in this case, the government—in response to a problem that Apple intentionally engineered—is confronted by a situation in which its interest in access to the phone's data is undeniably compelling, in which it is *not* asking the company to decrypt anything or to alter any cryptographic standards, and in which it is merely asking for help in hacking the device.

The government's position here, it bears emphasis, is in no sense surprising. It is, rather, highly predictable—the inevitable consequence of not relying on some regulatory mandate to force companies into the decryption business. The position is, in fact, so predictable that it was specifically predicted by one of us only last month:

The more I think about both the "Lawful Hacking" [option], the more I think civil libertarians and cryptographers should be careful what they wish for. The law, it turns out, interacts with this idea in some curious ways, ways I doubt the advocates of lawful hacking as an alternative to encryption regulation have fully considered.

[To wit,] I suspect that by advocating that the government bypass encryption systems, rather than requiring decryption, this approach will actually deprive companies of one of the strongest legal protections now granted them in this area and will instead place them in a arena in which the government can, legally speaking, effectively dragoon them into helping investigators hack consumer devices.

With all of that as background, now let's turn to Apple's pitchforks and torches position on this matter.

Consider first that Apple is wildly overstating the threat to user privacy. The government has not, in fact, demanded that Apple "build a backdoor to *the* iPhone." It has demanded that Apple build a backdoor—if that's even the proper analogy—to *one* iPhone. If the company is worried about the threat of that "backdoor" leaking, it can destroy the modified operating system immediately. What's more, Apple's argument about this move's setting "a dangerous precedent" is altogether unconvincing. If government access is appropriate here, and demanding technical assistance is appropriate, then setting a precedent for future appropriate uses is not a problem. If the company is worried about the government's asking for hacking aid in future, less important cases, that is a fair concern. But while Apple intones that "[t]his moment calls for public discussion," that kind of careful line-drawing does not seem to be the conversation Apple really wants to

have. Rather, the company is stonewalling and refusing to engage at all. Apple here is not merely privileging the privacy of overseas users over American law enforcement. It's privileging user privacy public relations—as opposed to *actual privacy*—over genuine law enforcement interests.

Now consider that there are only so many ways a company can respond constructively to a problem like this one—and that Apple rejects them all.

The most obvious approach is also the most obvious non-starter for a company which chose to create the problem in the first place: voluntary cooperation. Technology companies can sit down with government officials and come to a mutual understanding regarding the capacity and obligations to give aid in such situations. In his testimony before the SSCI last week (at the same hearing, linked to above, at which Comey spoke), DNI Director Clapper said that he hoped the possibilities for voluntary cooperation were not yet exhausted. We think it is safe to say from Apple's point of view, however, that the notion of voluntary cooperation is unacceptable. Apple has developed a conscious public relations strategy tied to its committed opposition to law enforcement on data access. Because Apple is a global corporation with customers and stakeholders in many nations, this may not be an irrational approach. The patriotic merits of cooperating with US law enforcement—notwithstanding the company's professed "love" of country—just is not a message that plays well in countries where love of America is not a civic value. And the company clearly has sincere desires to maximize user cybersecurity too. So voluntary cooperation has limits, as reflected in Apple's own statement on this matter:

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

In the absence of voluntary cooperation, Apple could work to shape legislation setting—and presumably limiting—the terms under which the law compels it to provide assistance. This would allow the company to have a voice in shaping appropriately scoped legislation, while simultaneously giving it worldwide cover for compliance. In situations like the one at hand, the company could then argue that it is only doing what it has to under the law. Apple could even contrive to be perceived as being dragged, kicking and screaming, into cooperating if that helps the company's international reputation and, therefore, its bottom line.

But Apple has obstructed legislative efforts at every turn, both here and in the UK. As Tim Cook has made clear, the company's view is that "the reality is if you put a backdoor in, that backdoor's for everybody, for good guys and bad guys." The problem is the "backdoor" Cook refers to here is *any* form of law enforcement access to content because that would "aid both law-enforcement agencies and the terrorists they are working to stop."

And when you think about it, why shouldn't Apple oppose all legislation? Working towards legislation is really just a different form of voluntary cooperation; it's voluntary cooperation at the congressional level, instead of the investigative level. And if one's goal is device security uber alles, well, that's hardly any better.

Traditionally, in the absence of legislation, the All Writs Act functions as a gap-filling measure. Under 28 USC 1651, "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." Put simply, federal courts can compel individuals and companies to assist in carrying out its orders. All Writs functions as a stopgap that applies where there is no other law directly on point under which a court can act. It is intended to ensure that courts are empowered to give practical effect to "the proper administration of justice"—for example, by requiring companies to help execute search warrants where the government otherwise cannot. Without the power of All Writs, many court orders are worth little more than the paper they are printed on. So an Apple that actually wanted to do business might take the position that in the absence of legislation (which it opposes) and in the absence of voluntary cooperation (which it won't grant), the All Writs Act allows it to be forced to help unlock a shooter's phone.

But Apple objects to the application of All Writs wherever it finds it. This actually isn't the first time the company has fought a technical assistance request under the law. Back in October 2015, federal authorities in the Eastern District of New York obtained a warrant to search the phone of Jun Feng, relating to his indictment on charges of possessing and distributing methamphetamine. As is common practice, the government also secured a court order directing Apple to assist in the execution of the search warrant by unlocking the defendant's phone, which was in the possession of law enforcement. There was no reason to anticipate any kind of controversy in this case; the phone in question ran iOS7, a system which Apple retains the technical capacity to unlock. And the government complied with Apple's published guidelines to law enforcement. Initially, Apple indicated that it intended to comply, as indeed it had some 70 times prior in other cases.

But then, rather unexpectedly, Apple changed its mind. The company challenged the court order, claiming that it constituted an improper application of the All Writs Act.

Why an *improper* application of All Writs? In United States v. New York Telephone Co., 434 US 159 (1977), the Supreme court held that courts have authority to order third parties to facilitate the execution of search warrants subject to a three-part test. First, the third party—in that case a phone company installing a pen register device—cannot be "so far removed from the underlying controversy" that it would be unreasonable to compel assistance. Second, the order cannot place an "undue burden" on the third party. And third, the assistance must be necessary to effectuate the warrant.

Apple's first argument in that case is a bit hard to track, but bear with us. The company argued that it is an "information services provider" as defined in CALEA, the law that requires telephone companies to preserve law enforcement's ability to wiretap. Apple claims that as an information service provider, it is expressly *excluded* from CALEA (by virtue of being named but not directed to assist), which only applies to "telecommunications carriers." Therefore, the company argued, All Writs cannot apply; there's no gap in the law, after all, since CALEA defines the company. On the other hand, CALEA also defines the company as something other than the telecommunications carrier obliged to help out. Voila! There is both a law, which cannot be used to force Apple to assist, and then the very existence of said law means that no *other* mechanisms to compel assistance apply. It's a neat trick.

More importantly (and more revealingly), Apple claimed that complying with the order represented an undue burden because it would cause "reputational damage" that would tarnish its brand:

[P]ublic sensitivity to issues regarding digital privacy and security is at an unprecedented level. This is true not only with respect to illegal hacking but also in the areas of government access—both disclosed and covert. Apple has taken a leadership role in the protection of its customers' personal data against any form of improper access. Forcing Apple to extract data in this case, absent clear legal authority to do so, could threat the trust between Apple and its customer and substantially tarnish the Apple brand. This reputational harm could have a longer term economic impact beyond the mere cost of performing the single extraction at issue.'

Susan analyzed Apple's positions in detail in this post. For present purposes, however, the point is simply that Apple's position is that neither CALEA nor All Writs obligate it to provide technical assistance. And while the company actively opposes legislative approaches to the Going Dark problem, in court it insists that without one, judges can't touch it. Apple argued in EDNY: "This is a matter for Congress to decide. And whatever its reasons, Congress has affirmatively decided not to enact legislation requiring Apple to perform the types of services the government demands here." The brief fails to mention Apple's own crusade against legislation.

To summarize, then, the problem is not just that Apple is refusing all possible solutions—though the company is certainly doing that. The problem is that Apple is actively—and we think somewhat duplicitously—using its various positions in different fora to map out a zone of immunity for itself, a kind of legal black hole in which nobody can force it to do anything. Having created technical conditions such that it cannot comply with legal process, Apple then fights all legislative efforts to force it to change those technical conditions while also rejecting the application to itself of both the traditional mechanism used to compel assistance in the absence of legislation and the application of other existing statutory requirements.

FBI and Justice Department officials, we think, can be forgiven if they're a touch cynical about all of Apple's elaborate legal argumentation and suspect that this all just masks what appears to be Apple's genuine litigating posture towards the government: You can't make us do anything, because we are immensely politically powerful, our CEO is on the phone with the President regularly, we are too big and way too cool to fail, and people around the world like us more than they like you. So what about that dead woman in Louisiana? Sorry, but bringing her killer to justice—and preventing his or her future violence—just isn't as important as the data security of our devices. And about protecting people from ISIS? We'll help out if it's not too much trouble, but don't ask us—ever—to do something that will make us look bad to the ACLU, even if there's a very good legal argument that you can.

As the company's statement makes very clear: the government's concerns—terrorists, mass shooters, some poor dead mother and her unborn child whose family may never see justice—all come before the "But."

So here's the question: Does the public accept this heroic self-presentation? Or does the public come to see Apple's posture here as fundamentally self-serving and anti-communitarian? Is Apple not adopting the position of gun manufacturers towards Second Amendment rights? Or the strategy of Big Tobacco as it worked to fight regulation while invoking the lack of regulation as a liability shield? Following this well-trod path is Apple's right, of course. And perhaps it is a rational call by one of the corporations with one of the world's largest market capitalizations.

But the final decision here doesn't belong to Tim Cook. It belongs to the people—and it's time for Congress to act.

Susan Hennessey is the Executive Editor of Lawfare and General Counsel of the Lawfare Institute. She is a Brookings Fellow in National Security Law. Prior to joining Brookings, Ms. Hennessey was an attorney in the Office of General Counsel of the National Security Agency. She is a graduate of Harvard Law School and the University of California, Los Angeles.

@Susan_Hennessey

Benjamin Wittes is editor in chief of Lawfare and a Senior Fellow in Governance Studies at the Brookings Institution. He is the author of several books and is co-chair of the Hoover Institution's Working Group on National Security, Technology, and Law.

@benjaminwittes