techdirt

How Apple Could Lose By Winning: The DOJ's Next Move Could Be Worse

Julian Sanchez

March 17, 2016

Since the conflict over smartphone security, long simmering between Apple and the FBI, **burst into the headlines** last month, many of us who advocate for strong encryption have watched the competing legal arguments advanced by the parties with a certain queasiness. Many of the arguments on Apple's side—whether offered **by the company itself** or the **myriad groups** who have weighed in with friend-of-the-court briefs—have turned critically on the government's unprecedented invocation of the hoary All Writs Act to compel the company to write and authenticate a novel piece of software effectively dragooning Apple engineers into government service.

But there has always been an obvious alternative—a way to achieve the FBI's aim of circumventing iPhone security features without requiring any Apple employees to write a line of new code: the **Lavabit** Option.

That is, **instead of asking Apple to create a hacking tool that would permit the FBI to attempt to brute-force a phone's passcode without triggering escalating delays between guesses or deletion of encrypted data, they could simply demand that Apple turn over the source code and documentation the FBI would need to develop its own custom version of the iOS boot ROM, sans security features**. Then, they require Apple to either cryptographically sign that code or provide the government with access to its developer credentials, so that the FBiOS can run on an iPhone.

That hypothetical possibility is raised explicitly by the Justice Department in a footnote to its most recent motion in its ongoing litigation with Apple, which explains that the FBI had not gone that route because it "believed such a request would be less palatable to Apple." Having tried it the easy way, the FBI suggests it's happy to do things the hard way: "If Apple would prefer that course, however, that may provide an alternative that requires less labor by Apple programmers."

[7] For the reasons discussed above, the FBI cannot itself modify the software on Farook's iPhone without access to the source code and Apple's private electronic signature. The government did not seek to compel Apple to turn those over because it believed such a request would be less palatable to Apple. If Apple would prefer that course, however, that may provide an alternative that requires less labor by Apple programmers. *See In re Under Seal*, 749 F.3d 276, 281-83 (4th Cir. 2014) (affirming contempt sanctions imposed for failure to comply with order requiring the company to assist law enforcement with effecting a pen register on encrypted e-mail content which included producing private SSL encryption key).

The government follows up with a citation to the **Fourth Circuit's ruling** in the now-infamous Lavabit case. Because the secure e-mail service Lavabit maintained minimal logs of user metadata, the government had **obtained an order** to install a "pen register"—a mechanism for recording metadata in realtime—on the company's systems in order to monitor a particular user, widely believed to be Edward Snowden. In order to make that data intelligible, however, **it also demanded the use of the SSL keys** used to encrypt all users' traffic. When the Fourth Circuit upheld that demand, CEO Ladar Levinson **chose to shutter** the site entirely.

Apple's **latest reply brief** clearly registered the company's dismayed response to this legal shot across the bow:

> The catastrophic security implications of that threat only highlight the government's misunderstanding or reckless disregard of the technology at issue and the security risks implicated by its suggestion.

Such a move would signal a race to the bottom of the slippery slope that has haunted privacy advocates: A world where companies can be forced to sign code developed by the government to facilitate surveillance. In this case, that means software to brute force a passcode, but could as easily apply to remote exploits targeting any networked device that relies on developer credentials to authenticate trusted updates. Which is to say, nearly any modern networked device. It entails, quite literally, handing the government the keys to the kingdom.

What's particularly worrying is that, while this approach is massively more troubling from a security perspective than funneling such requests through the company itself on a case-by-case basis, it would likely stand on a less shaky legal foundation.

Apple's arguments throughout this case have stressed the unprecedented nature of the FBI's attempt to conscript the firm's engineers, noting that the All-Writs Act invoked by the government was meant to enable only the particular types of orders familiar from common law, not grant an all-purpose power to "order private parties to do virtually anything the Justice Department and FBI can dream up." The trouble is, an order to turn over information in the "possession custody or control" of a private party is just such a traditional order. Such demands are routinely made, for instance, via a subpoena duces tecum requiring a person or company to produce documents.

It's likely that Apple's developer keys are stored in a Hardware Security Module that would make it difficult or impossible to produce a copy of their firmware signing key directly to the government. But that might not be much legal help. In a separate iPhone unlocking case in New York, magistrate judge James Ornstein recently **rejected the government's argument** that a previous All-Writs Act case, *New York Telephone Co.*, required Apple's compliance. In that case, Ornstein noted, the government's

> agents would normally have been able to install the authorized pen register without the company's assistance but for the fact that the subject telephone's wires were so placed as to prevent the agents from gaining surreptitious access. The agents thus needed the telephone company not to provide technical expertise they lacked, but only to step out of the way and let them perform their authorized surveillance on company property.

But that sounds much closer to what would be involved in a case where Apple is required to authenticate government-written code: Just "step out of the way" and let the FBI access the HSM containing the keys used to sign updates.

Similarly, many of the First Amendment arguments raised by Apple and the Electronic Frontier Foundation—to the effect that "code is speech" and the requirement that Apple create new software amounts to "compelled speech"—would also fall by the wayside. They might still advance such arguments with respect to the "endorsement" implicit in using company credentials to sign software, but a court may not find that as intuitive as the idea that "compelled speech" is involved in requiring engineers to devise wholly novel and potentially complicated software.

Many of Apple's other arguments, of course, would remain untouched: There's the idea that Congress has established a comprehensive statutory framework specifying the means of law enforcement access to digital content via laws like the Communications Assistance for Law Enforcement Act and the Electronic Communications Privacy Act, making the All-Writs Act an inappropriate mechanism to seek authority withheld by Congress. Nor would a "sign our code" approach affect any of Apple's claims about the broader security harms inherent in the creation of developer-authenticated tools to break security. But the long list of legal barriers to the FBI getting its way would surely be significantly reduced.

That means it's not just important that Apple win in this case—*it matters how it wins*. If the company emerges victorious on grounds fundamentally tied to the mandate to create software rather than the demand to authenticate it, it could prove a pyrrhic victory indeed, opening the door for the government to insist on doing things the "hard way," and inaugurating an era of government scripted malware signed to look like genuine updates.

Julian Sanchez is a senior fellow at the Cato Institute and studies issues at the busy intersection of technology, privacy, and civil liberties, with a particular focus on national security and intelligence surveillance.