NEW YORK POST

Can an 18th-century law force Apple into hacking killer's phone?

Julian Sanchez

February 18, 2016

Can Apple be forced to hack its own iPhones? That question is at the heart of the latest skirmish in the war between Silicon Valley and law enforcement over smartphone encryption — and the answer may depend on an 18th-century law you've never heard of.

This week, the FBI obtained a court order demanding Apple's help breaking into the iPhoneused by Syed Rizwan Farook.

Killed in a shootout with police in the aftermath of the San Bernardino terror attack, Farook obviously can't unlock the phone, so the bureau wants Apple to write custom software that will help it do so.

In a blistering letter, Apple CEO Tim Cook pledged to fight the demand, warning that the court order would set a "dangerous precedent" threatening the security of millions worldwide.

The government wants Apple to create for it a phone-hacking app keyed specifically to Farook's device, but similar demands from other agencies would surely follow, and Cook fears that the digital "skeleton key" would eventually fall into the wrong hands.

This dust-up is only the most recent battle in the "Crypto Wars" — a long-running debate over how to deal with strong encryption technology.

But Farook was no Edward Snowden — he only locked his phone with a simple numerical code. So the FBI could easily run through all the possible combinations in a few hours or days — if only the phone weren't programmed to wipe itself after too many wrong guesses.

That's where Apple comes in: The feds want the tech titan to build them a custom iPhone operating system, minus security features like auto-wipe.

The tech may be cutting-edge, but the legal issues are old-school. To persuade a judge to compel Apple's assistance, the feds turned to a 1798 law, the All-Writs Act — in essence, a catchall empowering courts to issue orders that are necessary to carry out other legal functions. A search warrant for an apartment, for instance, might come with an order compelling the landlord to produce the key.

Make no mistake, though: What the government is trying here (and in at least one other similar recent case) is unprecedented. Traditionally, the All-Writs Act has been used to force companies to cough up information they already have about their own customers, like a phone company ordered to turn over a criminal suspect's billing records.

Here, Apple engineers are effectively being conscripted to build forensic software — a hacking app — for the FBI. That's more like ordering a locksmith to help crack a safe, or a linguist to make sense of a suspect's diary, against their will, if necessary. Instead of being asked to hand over its own information, Apple is being instructed to help hack into someone else's — someone whose only connection to the company was owning a phone that Apple produced.

That's a particular stretch because (as Apple argues in another ongoing case) Congress has already passed a federal law outlining exactly what companies must do to help police spy on digital messages: the Communications Assistance for Law Enforcement Act of 1992.

Nothing in that law obliges companies to help crack encryption, and despite increasingly loud calls from the FBI for an encryption "update," Congress has declined to go along.

The FBI, in other words, is relying on an 18th-century law to grant it powers that our 21st Congress won't.

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. Sanchez has written on privacy and technology for a wide array of national publications, ranging from the National Review to The Nation, and is a founding editor of the policy blog Just Security.