creators.com
A SYNDICATE OF TALENT

Government Sinks Teeth Into Apple's Security Core

Debra J. Saunders

February 21, 2016

I view Apple with almost as much loathing as I save for overzealous federal prosecutors. My last Apple phone was a lemon. The "Genius Bar" isn't. When I hear Apple extol its vaunted regard for privacy, I think of all the invasive personal questions my iPhone used to ask before I could download a free app. That was before I switched to Android. Liberated from 1 Infinite Loop -- that's is Apple headquarters' precious Cupertino street address -- I am free of owners' cultish reverence for all things iPhone.

So when I began reading CEO Tim Cook's open letter outlining the reasons why the most valuable corporation in the world would not submit to a judge's order that Apple help break the encryption on a terrorist's iPhone, I was ready to believe that Apple was putting its brand before public safety. But this is no black-and-white controversy. It's not: Apple thinks it doesn't have to obey court orders. And it's not: The government just wants to mess with Apple's encryption. It's more complicated.

The FBI believes that the San Bernardino County Public Health Department-owned work iPhone of Syed Rizwan Farook -- who with his wife, Tashfeen Malik, killed 14 people on Dec. 2 -- may contain important information about other terrorists. Farook may have intentionally disabled a feature that sends data to the cloud on or after Oct. 19 to conceal the identity of confederates. Prosecutors want Apple to override its technology that wipes out phone data after 10 unsuccessful attempts to enter a pass code in order to see what's in Farook's phone.

While critics of national intelligence surveillance like to rail against National Security Agency bulk data collection, this story is not about sweeping surveillance, It is about a judge's warrant for the phone of a known terrorist and mass murderer. San Bernardino County gave the feds permission to tap phone data. It is possible that the phone's contents could save lives. Or not.

Julian Sanchez of the libertarian-leaning Cato Institute, notes that Farook and Malik tried to destroy their burner phones, but not the iPhone. In practical terms, Sanchez argued, the Justice Department wants to risk iPhone security protocols on a bet that Farook hid data in a device he did not bother to destroy.

Cook wrote that if the government forces Apple to bypass its security codes, then "The encryption can be defeated by anyone with that knowledge." The answer to which should be: OK, don't share the knowledge. But to Cook, the exercise is like Pandora's box. You open the lid, all the bad things get out.

Worse, the FBI essentially is demanding that Apple do the FBI's job: criminal investigation. Cook wrote, "The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers." If the government can order a tech company to write a hacking program, can the government force other people to do investigators' chores as well?

Cyber law attorney Catherine Gellis described Apple's position in a different manner. "Apple is trying to deliver an invulnerable product," she told me. If Apple can break its own code, then its new iPhone is "no longer a secure device. It's no longer invulnerable." You could say the government is demanding that Apple disprove its marketing claim that its phones are so secure that even Apple cannot hack into your data.

Cook, Sanchez and Gellis fear that if the government succeeds in using the All Writs Act of 1789 to force Apple to undo its security measures, there's no way the Department of Justice stops with Farook's work phone. Indeed, Sanchez thinks that's the idea. He suspects this effort is less about Farook's phone and "more about finding a high-profile case to push a novel and somewhat unprecedented" use of an 18th century law.

It wouldn't be the first time the feds have used their considerable muscle to pick on the wrong person. In 2007, the government imprisoned videographer Josh Wolf for seven months based on the incorrect belief that Wolf had video that might reveal the identity of a protester who seriously injured a San Francisco police officer.

"I just don't see them doing that to Apple," former CIA spokesman Bill Harlow told me. Harlow doesn't think Uncle Sam would haul such a large corporation into court unless there was no other recourse. For one thing, "These are all senior government lawyers who want to get jobs with Apple" when they leave the government.

The government is still pursuing its investigation. Thursday officials executed a search warrant on Farook's brother's home.

Gellis told me that once Apple admits its pass codes wear no clothes, entrepreneurs and hostile foreign governments will try to create their own backdoor into the iPhone. I have to think others already are trying to hack iPhone security software, because the notion of inviolability sounds too good to be true. But that doesn't mean it's smart to encourage hackers. Or that it's smart to develop anti-encryption software that others can steal. The trade-off: Risk inviting China and freelancers to break iPhone security in the hope that Farook left useful intelligence in his iPhone. The downside may be far worse than the upside is good.