THE PATRIOT POST®
VOICE OF ESSENTIAL LIBERTY

Counterterrorism Logjam: FBI vs. Apple

February 19, 2016

"They that can give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety." —Benjamin Franklin

The attempt to find balance between Liberty and security is the primary challenge facing our efforts to fight terrorism in modern America. That debate is now playing out between the FBI and Apple over the iPhone that belonged to San Bernardino terrorist Syed Farook.

U.S. Magistrate Judge Sheri Pym gave tech giant Apple until Feb. 26 to decide whether to help unlock Farook's iPhone (bypass the 10-attempt limit on the passcode) so that investigators can look for evidence of connections with other terrorists. "Despite … a warrant authorizing the search," said prosecutors, "the government has been unable to complete the search because it cannot access the iPhone's encrypted content. Apple has the exclusive technical means which would assist the government in completing its search, but has declined to provide that assistance voluntarily."

When a warrant is served, a locked door shouldn't stand in the way. The national security arguments for actually being able to serve this of all warrants are obvious. No one wants terrorists to succeed in killing innocents, and if the information contained on the phone could thwart future attacks, lives could be saved. And Apple notes it has already "worked hard to support the government's efforts to solve this crime." Apple provided all of Farook's data in its possession and had its own engineers advise the FBI.

But Apple has refused to create a way to unlock this phone. Why? It has, on 70 prior occasions since 2008, helped investigators access other iPhones. Why, as Sen. Tom Cotton (R-AR) put it, has "Apple chose[n] to protect a dead ISIS terrorist's privacy over the security of the American people"?

In a public letter, the company explained why Cotton's is a false choice — because this locked door is different:

[T]he 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.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during

the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.
The letter goes on to explain the technical details. Here's the gist of it: One of the major security initiatives of iOS 8 and iOS 9 (and several other recent operating systems like Windows 10) is to ensure that an OS update can't be forcibly installed that would allow the system to be compromised. Despite its claims, the FBI isn't just asking Apple to do this one thing for this one phone this one time. It is effectively asking Apple to undo some of its most important security efforts over the last several years. Those 70 phones Apple already unlocked were previous generation technology, and thus a different matter.

According to Apple, "Once created, the technique could be used over and over again, on any number of devices." Building a "backdoor" to one iPhone builds one for all iPhones. The warrant wouldn't just provide agents the key to one door, but a master key to all of them.

Apple argues, "We can find no precedent for an American company being forced to expose its customers to a greater risk of attack."

The company has largely staked its reputation in recent years on this very security. If it were to break its security promises, the blow to the company would be enormous. It's not for nothing that the company pleaded, "This reputational harm could have a longer term economic impact beyond the mere cost of performing the single extraction at issue." Would you buy a safe from a company that could easily crack it open?

Moreover, the U.S. is not the only large consumer of Apple's products. So if Apple creates a backdoor for the U.S., what's to stop China or Russia from demanding the same thing to use against political opponents, underground churches, etc.?

Can you say Pandora's Box?

The FBI already has loads of information on Farook and his wife. Farook used cloud backups until about six weeks before the attack, and Apple has already turned over that data. Prior to the attack, the warning signs were already there — via unencrypted information on Facebook, for example. With proper vetting, the couple could have been kept out of the country in the first place.

But by the FBI's own admission, this is just the kind of case they've been looking for to argue for a backdoor to encrypted devices, which they will then use to set precedent — not just for solving terrorism cases, either. And what better case than San Bernardino? Two Islamist dogs murdered 14 Americans, and the FBI has painted Apple as unwilling to help complete the investigation. Some will indeed look askance at Apple as a result, whether the company prevails or not.

Perhaps more important than the technology is the precedent. “The law operates on precedent, so the fundamental question here isn’t whether the FBI gets access to this particular phone,” said Julian Sanchez, a surveillance law expert at the Cato Institute. “It’s whether [the All Writs Act] from 1789 can be used to effectively conscript technology companies into producing hacking tools and spyware for the government.”

Fighting terrorism is a notch above other crimes in importance, but along with the NSA’s surveillance program and other intrusive counterterrorism measures, is creating this major security vulnerability worth it?

Finally, the underreported fact is that Farook’s iPhone 5c belonged to San Bernardino County, for which he worked, not to Farook. The county doesn’t object to unlocking the phone; Apple does. There is almost surely a “cover-your-rear” angle for the county, however, and that’s even less reported than the phone’s ownership. iOS has “enterprise” functionality, and the county could have set up Farook’s phone in such a way as to allow clearing the passcode lock — which again is the specific barrier for the FBI. But bureaucratic ineptitude being what it is, the county didn’t set it up that way. In other words, if the county had set up Farook’s phone correctly in the first place, we might not even be having this debate.