CITY NEWSPAPER

FBI vs. Apple case isn't just about one iPhone

Mary Anna Towler

March 1, 2016

Words have a lot of power. And since the September 11 attacks, one of the most power-packed words for Americans has been "terrorism." All anybody in government has to do is say that word, and we're ready to put our skepticism and, sometimes common sense, in a drawer and close it.

I don't mean to be flippant; while some politicians like to exaggerate terrorism's threat, it would be naïve and irresponsible to deny that the country needs to be vigilant. And we tend to give government officials the benefit of the doubt when they say they need to do something to protect us - especially when that something is a "just this once" action related to someone who shot up a social-services center, killing 14 people, wounding 21 others, and surely traumatizing everybody else in the area.

And so we have the conflict between the FBI and Apple. The FBI wants to know whom Syed RizwanFarook was in contact with on his iPhone in the hours before his San Bernardino attack. That information is still on Farook's cellphone, and the phone is in the FBI's possession. But thanks to the encryption that Apple builds into its iPhones, the FBI can't access it. Nobody can. Not even Apple.

Apple could create something that would let the FBI get past the encryption, but it's refusing to. The company believes it's "too dangerous" to do it.

"The only way to guarantee that such a powerful tool isn't abused and doesn't fall into the wrong hands is to never create it," Apple CEO Tim Cook said in a letter to Apple customers.

Despite the government's insistence, this issue won't be limited to this one request for this one phone this one time. "Once created," Cook wrote, "the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks - from restaurants and banks to stores and homes. No reasonable person would find that acceptable."

And if the government is able to require Apple to create something that will unlock this specific iPhone, that will set a dangerous precedent.

"For starters," writes Timothy Lee on Vox, "although the hassle involved in complying with the FBI's request is considerable, once Apple engineers have done the necessary work of creating the custom software it will be much easier to comply with other law enforcement requests for the

same service. Today's extraordinary request for an extraordinary suspect, in other words, could be tomorrow's routine request."

If the FBI prevails in this case, writes the Wall Street Journal's technology columnist, Christopher Mims, "Apple can be forced to make the data on any iPhone available to any law-enforcement agency that demands it."

In fact, the Farook iPhone isn't the only one Apple has been asked to provide access to. ABC News reports that Apple "has received at least 15 court orders compelling the company to assist in extracting data from an iPhone over the past five months."

And Julian Sanchez, a senior fellow at the Cato Institute, adds this, on the online forum Just Security: "The Manhattan DA's office alone has at least 175 iPhones that they'd like Apple to help them break into, and DOJ itself [the Department of Justice] has 12 other ongoing lawsuits seeking access to iPhones."

If you have a smartphone of any kind, you know what information it contains: personal and business e-mail correspondence, contact information for friends and family members, your purchases, your reading material, your idle online searches, personal health information. Your plans for today, for tonight, for your vacation. Your location right now and where you've been recently.

You don't have to be a conspiracy theorist to believe that there are many things that government - whether liberal or conservative, federal or local - has no business knowing about you.

Nor is the Apple case a concern only to smartphone users in the US. "Authoritarian regimes around the world are salivating at the prospect of the FBI winning this order," the Electronic Frontier Foundation's Nate Cardozo said in a PBS NewsHour interview. "If Apple creates the master key that the FBI has demanded that they create, governments around the world are going to be demanding the same access."

The issue, says the Wall Street Journal's Christopher Mims, is "simply this: Do we want our government, and the governments of other countries, to have the ability to compel Apple - or any technology company - to grant access to any of our data they request?"

"Most ominously," the Cato Institute's Julian Sanchez wrote in Time magazine, "the effects of a win for the FBI in this case almost certainly won't be limited to smartphones."

"Don't just think of the webcam and microphone on your laptop," wrote Sanchez, "but voice-control devices like Amazon's Echo, smart televisions, network routers, wearable computing devices and even Hello Barbie."

This isn't a case of getting into one terrorist's cellphone; it's "whether technology companies can be conscripted to undermine global trust in our computing devices," Sanchez warned. "That's a staggeringly high price to pay for any investigation."

And it's a staggeringly big attack on privacy - an attack, as Tim Cook said in his letter to Apple customers, on "the very freedoms and liberty our government is meant to protect."

The FBI's request related to Farook's cellphone is expected to end up before the Supreme Court. But Apple and other critics say that Congress, not the courts, should define the line between national security and individual privacy.

Given the conservatism of Congress and the national obsession with security, though, I'm not sure that offers much consolation. And can't you just see what a Donald Trump administration would do on this issue.