Encryption fight: A loss for Apple is a loss for American civil liberties

Anthony Hennen

February 17, 2016

The federal government wants to force Apple to develop a backdoor to subvert the security of its products, and the result can set a strong precedent for privacy or a dangerous subversion of it.

On Tuesday, a federal judge ordered Apple to unlock an iPhone connected to the San Bernardino terrorist attacks for the FBI, according to *Buzzfeed*. Specifically, the FBI wants Apple to develop a backdoor to bypass encryption so they can extract data. They want Apple to disable an "auto-erase" function that happens when too many incorrect passcodes have been entered so the FBI can unlock the iPhone.

Some experts have declared that the FBI's request is technically possible, but Apple published an open letter strongly opposed to the order.

"The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge," Tim Cook wrote.

As Julian Sanchez, a senior fellow at the Cato Institute said, "This isn't even REALLY about crypto. It's about whether developers can be conscripted to write spyware."

The grave concern is that, like many other instances, the federal government will use a terrorism case to set a precedent. As with the use of cell-phone trackers, or stingrays, the government violates privacy norms for terrorism suspects, then expands it beyond to the general public and even to find missing persons. Give them an inch and they take a mile in the name of safety, regardless of reality.

Politicians have demanded tech companies do more for the government in fighting terrorism, from John McCain to Hillary Clinton to Donald Trump. After every act of terrorism, authorities are quick to advocate for more power to subvert encryption and privacy protections. The grave threat that the government poses to privacy and civil liberties have not yet been learned, even after the grave abuses since 9/11, empowered by the so-called PATRIOT Act.

Demands for tech companies to subvert privacy protections for the government, and for the American people to submit to further violations of their civil liberties, are un-American. They invite government abuse of power, and they run roughshod over the very idea of liberty the government supposedly upholds.

“I don’t want a door, I don’t want a window, I don’t want a sliding glass door,” FBI Director James Comey said last week when he addressed a Senate committee on difficulties investigating the San Bernardino attack.

A sliding glass door can be opened by law enforcement as well as criminals and terrorists. Encryption is not a threat to American safety. Hollow promises from the federal government threatens the safety and security of Americans more than terrorists. If Apple loses the court battle, it will be another loss in the 15-year battle of civil liberties against government abuse of power. The result will be an American public more exposed to the abuse of governments and terrorists alike.