Codes, ciphers, and the Constitution

Patrick G. Eddington

February 19, 2016

What if I told you that right now, senior officials at the Department of Justice were advocating a policy that, if implemented, would make every American more vulnerable to identity theft and cyber crime?
The scenario I've just outlined is playing out right now before a federal magistrate judge in California.

The Department of Justice is demanding that Apple, maker of the iPhone 5c used by one of the ISIS-inspired San Bernardino shooters, make new software that would allow the FBI to bypass the passcode lockout and data-erasure security measures on the phone so the FBI can see if there is any additional evidence relevant to the shooting on the device. On the surface, this sounds perfectly reasonable, even potentially necessary. However, a close look at the judge's order and a little reflection on its down-stream consequences demonstrates the dangers to all of us if the Justice Department gets its way.
Specifically, federal magistrate judge Sheri Pym has ordered Apple to create this encryption "back door" software and that the software "be loaded on the SUBJECT DEVICE at either a government facility, or alternatively, at an Apple facility; if the latter, Apple shall provide the government with remote access to the SUBJECT DEVICE through a computer allowing the government to conduct passcode recovery analysis." In other words, this encryption "back door" software is to be given directly to the FBI, to be stored on FBI computer systems.

As CEO Tim Cook noted in his open letter to Apple customers, "The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, 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."

Cook is right, and the Justice Department will not stop with this case and confine itself to simply getting past iPhone passcode locks.

Many companies make encrypted messaging apps, some of which have been misused by alleged or actual ISIS supporters to plot terror attacks here in the United States. In 2015, A Virginia teen pled guilty to providing material support to ISIS, and one of his primary means of communicating with ISIS overseas was the encrypted messaging app Surespot. If the Justice Department prevails in compelling Apple to create an encryption "back door" for the iOS operating system, it will use that precedent to force companies like Surespot to do the same to their products. Encrypted webmail providers like RiseUp will face similar demands.

A court-mandated encryption "back door" ruling will harm the entire U.S. technology sector. It will not only cost jobs, but it will put the financial security of every American at risk by leading to online products and services that are more vulnerable to hackers and hostile intelligence services.

The amazing thing about this case is that Department of Justice officials cannot possibly be ignorant of these risks. In February 2016, the FBI itself suffered its largest data breach to date, with hackers posting online the contact information for 20,000 FBI employees. If the FBI succeeds in getting court-ordered encryption "back door" software from dozens or hundreds of American companies, how long will it be before cash-for-hire hackers or foreign spies breach the database containing that "back door" software?

Some members of Congress have recently shown a sensitivity to this kind of threat.

A week before Judge Pym issued her order to Apple, a bipartisan group of law makers introduced the ENCRYPT Act, which would prevent state governments from trying to mandate that companies create encryption "back doors" for law enforcement. Representatives Ted Lieu (D-Calif.), Blake Farenthold (R-Texas), Suzan DelBene (D-Wash.), and Mike Bishop (R-Mich.) deserve credit for trying to prevent the balkanization of American encryption policy through their bill.

Unfortunately, their simple, well thought through measure has now been overcome by events. They and their like-minded, liberty-friendly colleagues are now in a race against time to prevent federal courts from compromising the privacy and civil liberties of Americans and the competitive edge U.S. companies still retain in the area of encryption.

Responding to the latest developments in the Apple v. FBI case, Rep. Lieu spoke for many Americans when he said "The San Bernardino massacre was tragic but weakening our cyber security is not the answer – terrorism succeeds when it gets us to give up our liberties and change our way of life."

He's right—and the best way to achieve the goal of defeating the terrorists without trashing the Bill of Rights is to demand that the FBI, CIA, and NSA do what they have been charged with vis a vis ISIS—get inside that organization in Europe and the Middle East and destroy it.

Eddington is a policy analyst in homeland security and civil liberties at the Cato Institute.