New American

Written by C. Mitchell Shaw on February 19, 2016

Fighting for Privacy: Apple Resists Order to Decrypt Terrorist's iPhone

Earlier this week, a district court judge ordered Apple to build a backdoor into the encryption software used in the iOS platform. The FBI wants the backdoor so that it can access the data stored on an iPhone used by one of the terrorists responsible for the San Bernardino shooting in December 2015. Apple is fighting the order, claiming it threatens the privacy of everyone who uses a smartphone.

The case revolves around the use of encryption in smartphones and whether or not government agencies can compel the companies — such as Apple and Google — which write the encryption software for mobile devices to circumvent the encryption. In late 2014, Apple announced that — starting with iOS 8 — users' data, including that which is stored on the device as well as e-mails, contacts, and photos would be fully encrypted by default. Apple also said the encryption process would happen on the device itself and that the company would not have access to the keys, meaning that Apple would not be able to access the encrypted data. Google followed suit by making better encryption available starting with Android 5.0, though it is not turned on by default. Now millions of Americans and others around the world use encrypted devices to protect their communications and data.

Since these encrypted devices are secure against hacking — even by those methods used by the NSA and other government agencies — the users of the devices are in control of their data. The surveillance hawks responded immediately by claiming that encrypted phones are the tools of terrorists and criminals. Ignoring the fact that the vast majority of people who use encryption to protect their data are law-abiding citizens, legislators began proposing bills to limit the types of encryption available to ordinary citizens. No anti-encryption bills made it very far, since the White House was hesitant to support the legislation.

Then came the San Bernardino shootings. An iPhone belonging to one of the shooters, Syed Rizwan Farook, was seized by police and turned over to the FBI. Since FBI agents were unable to get into the phone, they asked Apple to help. As Apple CEO Time Cook explained in an open letter to customers:

> We were shocked and outraged by the deadly act of terrorism in San Bernardino last December. We mourn the loss of life and want justice for all those whose lives were affected. The FBI asked us for help in the days following the attack, and we have worked hard to support the government's efforts to solve this horrible crime. We have no sympathy for terrorists.
>
> When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

As the investigation proceeded, the FBI demanded that Apple do more than provide technical assistance. The agency wanted Apple to create a fake iOS update and sent it to Farook's iPhone, fooling

the device into accepting a software package that would allow the agents to bypass the password protecting the encryption. Apple called that what it is — a backdoor — and refused. In the open letter to customers, Tim Cook wrote:

> We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the 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.

Apple's decision to refuse the FBI's demands is based in the basic principles that make encryption both necessary and effective.

Encryption is necessary because users need to protect their data from surveillance by overreaching government agencies, data-mining by nosy companies, and theft by hackers. As this writer said in a previous article:

> In the digital age, people do nearly everything on their computers and mobile devices. They talk, text, e-mail, and use video chat. They manage their businesses, transact their banking, shop, and pay their bills. They manage their social media accounts and search for needed — and sometimes frivolous — information. By using the various types of encryption available, they can do all these things with privacy and security.

Tim Cook addressed this same need in his open letter to customers:

> Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going.
>
> All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data.

Encryption is effective because the keys to unlock it are kept private. As this writer also wrote in that same article quoted above:

> The problem with "backdoors" is that that is just not the way cryptography works. The most powerful form of cryptography is "public key encryption," such as the popular GPG encryption used by millions, including Snowden. The way it works is that each user has a public key (which they share with others) and a private key (which they keep secret). The communication is encrypted

> using the sender's private key and the recipient's public key. The recipient then decrypts the message using his private key. Since the only keys that can unlock the communication are private, the communication is private. Providing "another key" that only government can use is a farce. Any such key would inevitably be exploited by hackers and foreign governments. Experts in cryptography agree: There is simply no way for it to be "kept safe."

Again, Tim Cook says essentially the same thing in his open letter to customers:

> Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.
>
> In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.
>
> The government suggests this tool could be used only 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.

While "no reasonable person would find that acceptable," the FBI, the Justice Department, and Magistrate Judge Sheri Pym of the Federal District Court for the District of Central California seem to think it makes perfect sense. In their unbalanced view of security vs. liberty, the surveillance hawks always lean toward promising security, though they often fail to deliver on that promise.

So, Judge Pym has ordered Apple to undermine the security of millions of smartphone users in the hopes that something useful will be found on Farook's iPhone. As Tim Cook put it, "The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe." Apple is fighting the order and the case may wind up in the Supreme Court.

There is more at stake here than the outcome of one investigation. The privacy of millions — not just in the United States, but around the world — will be determined by how this case turns out. As *The Guardian* wrote, "Authoritarian governments including Russia and China will demand greater access to mobile data should Apple lose a watershed encryption case brought by the FBI, leading technology analysts, privacy experts and legislators have warned."

There was a time when the United States set an example of liberty for the world to follow, and oppressive nations felt the weight of that example. Now, the "city on a hill" is known for setting an example of mass surveillance and brooking no opposition. The outcome could well be that nations such as China, Russia, and others will be emboldened to not only continue their practices of oppressing and spying on their citizens, but to expand those practices. If the United States can force an American company to provide a backdoor, these authoritarian nations will certainly demand the same. As *The Guardian* wrote:

> Senator Ron Wyden of Oregon, a leading legislator on privacy and tech issues, warned the FBI to step back from the brink or risk setting a precedent for authoritarian countries.
>
> "This move by the FBI could snowball around the world. Why in the world would our government

want to give repressive regimes in Russia and China a blueprint for forcing American companies to create a backdoor?" Wyden told the *Guardian*.

"Companies should comply with warrants to the extent they are able to do so, but no company should be forced to deliberately weaken its products. In the long run, the real losers will be Americans' online safety and security."