New American

Written by **C. Mitchell Shaw** on March 17, 2016

FBI vs. Apple: More Than Meets The Eye

Against the consensus of the leaders of technology, the FBI continues to insist that the courts should force Apple to create a backdoor into the iOS platform to allow the agency to defeat the software safeguards that protect the default encryption. Facebook, Twitter, Snapchat, Microsoft, Google, and other tech companies have issued statements showing support for Apple. These companies have said that creating a backdoor would be dangerous. Some have even filed amicus briefs with the court in support of Apple's position. Yet the FBI persists.

Considering that government backdoors are already responsible for allowing our enemies to carry out a series of data-thefts of American top secret intelligence — of which the hack on the Office of Personnel Management (OPM) is the most glaring, but far from only, example — it would seem the FBI would heed the sage advice of the tech experts. Unless there is more to the FBI vs. Apple encryption battle than meets the eye.

The FBI claims, because of the default encryption of the iPhone 5c used by San Bernardino shooter Syed Farook, that "Apple has the exclusive technical means" to access the data on the phone. So, when Apple refused to create a backdoor, the FBI said it had no choice but to seek a court order to force Apple to comply. But there are some facts of this case that — when seen together — paint a clear picture of the FBI creating and exaggerating the problem it says it can't solve without a backdoor into the iPhone.

When the phone — which is actually owned by the county of San Bernardino and was issued to Farook as his work phone — was recovered by San Bernardino investigators, they were instructed by the FBI to change the password of the iCloud account associated with the phone. This prevented the phone from being able to backup its data to the iCloud service where it would have been accessible to the FBI since Apple does hold the keys to the encryption of that service. In fact, Apple has made all of the data from the iCloud account associated with that phone available to the FBI. But, as the FBI claimed in its petition to the court, changing the password made the data "permanently inaccessible" since Apple does not hold the encryption keys to iPhone and iPad devices.

If the FBI had not directed San Bernardino investigators to reset that password, there is a good chance that simply by connecting the phone to one of its default Wi-Fi networks, it would have sent much, if not all, of its data to the iCloud where Apple would have been able to access it and turn it over to the FBI. In describing the decision to reset the iCloud password during his testimony before Congress, FBI Director James Comey said, "There was a mistake made." It is unimaginable that a computer forensics investigator working for the FBI would make such a "mistake."

Despite the claims of the FBI that the backdoor it demands is the only way to get to the data on the phone, experts in technology and surveillance have said that the FBI has the ability to do a hardware

hack on the phone and retrieve the data without forcing Apple to create a backdoor. NSA data-analyst-turned-whistleblower Edward Snowden responded to the FBI's claim that "Apple has the exclusive technical means" to access the data on the phone by saying "Respectfully, that's bullsh*t." He added that "There are hardware attacks that have existed since the '90's that the FBI can mount" that would give them access to the data on the phone.

The ACLU published an online article that both calls the FBI out for being "fraudulent" in that claim and gives a fairly detailed explanation of one of the "hardware attacks" that would allow the FBI to do what it claims it cannot do without Apple creating a backdoor. The method is similar to that described by John McAfee (the founder of McAfee anti-virus software).

As we mentioned above, the iPhone at the center of the FBI's PR and legal war against Apple was not even Farook's primary mobile phone. He had a personal phone which he destroyed before he and his wife went on their ISIS-inspired killing spree. Let that sink in. Farook had two phones: a work phone and a personal phone. His employer has access to the itemized bill on his work phone which would show every number he called and every number that called him. In fact, Verizon has given the FBI a record of all his calls and texts. He *did not* destroy that phone, but he *did* destroy his personal phone. It doesn't take The Amazing Kreskin to figure out which of those phones he was worried about investigators accessing. It is highly unlikely that anything of any value to this investigation could be found on the phone the FBI is making such a fuss over. So, why all the fuss?

If the FBI can access the data through well-established methods and there is little likelihood that the information it claims to seek is on the phone in the first place, why would the FBI scuttle the easiest method and then ignore the most effective method at its disposal? The simplest answer is that the FBI is not interested in Farook's iPhone; it is interested in setting a precedent in regard to all encryption.

Almost as soon as Apple announced the new default encryption standard on all iPhones running iOS 8 and up and Google followed suit by making better encryption available on Android 5.0 and up, Comey began demanding backdoors, saying "encryption threatens to lead us all to a very, very dark place."

After the deadly terrorist attacks on Paris, elected and appointed officials attempted to blame encryption for those attacks, and leaders of intelligence agencies claimed that the attacks were caused by too little surveillance. The surveillance hawks ramped up their rhetoric in an attempt to use those attacks to push for both and end to the private use of encryption and an increase in government surveillance.

When the San Bernardino shooting happened just a few weeks later, the hawks swooped in. Comey played on the fear and anger in the American mind to point to the encrypted iPhone and say that if the FBI could get into that phone, the shooters' accomplices could be found. He spent weeks claiming that this would be an isolated case: The backdoor the FBI was demanding Apple create could only be used once on this one phone in this one case.

But that's not true. As Apple CEO Tim Cook and other experts in encryption said over and over, once the tool is created, it could — and would — be used over and over. It would be the end of any effective encryption. In an open letter to customers, Cook wrote:

> 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.

Earlier this month, while testifying under oath before Congress, Comey finally admitted the truth. Sort of. House Judiciary Committee Chairman Robert Goodlatte (R-Va.) pressed Comey about the precedent this case might set. During his questioning of Comey, Goodlatte said, "It won't be a one-time request. It'll set precedent for other requests from the FBI and any other law enforcement." Comey's response? "Sure, potentially."

Manhattan Attorney General Cyrus Vance, Jr., was even more forthcoming in his congressional testimony. As *The New American* reported previously:

> Vance's prepared statement included the following glaring admission which directly contradicts Comey's assertion that forcing Apple to help the FBI circumvent the encrypted iPhone used by one of the San Bernardino shooters would be a one-time deal:
>
> > While the San Bernardino case is a federal case, it is important to recognize that 95 percent of all criminal prosecutions in this country are handled at the state and local level, and that Apple's switch to default device encryption in the fall of 2014 severely harms many of these prosecutions.
> >
> > And that is why I am here today as a representative of the thousands of local and state prosecutors around the country: Smartphone encryption has real-life consequences for public safety, for crime victims and their families, and for your constituents and mine. In the absence of a uniform policy, our nation will effectively delegate the crafting of national security and law enforcement policy to boardrooms in Silicon Valley. That is, important responsibilities of our government will be carried out by Apple, Google, and other technology companies, who will advance the best interests of their shareholders, not necessarily the best interests of our nation.
>
> In case that was too ambiguous, Vance also told the committee, "Law enforcement agencies at all levels, as well as crime victims' advocates and other concerned community leaders, are watching this case with great interest." In other words, the surveillance hawks need this case to set the precedent so that they can expand it to other cases.

If the FBI vs. Apple encryption battle were really about the one phone in this one case, the FBI could have had that data by now. Instead, the agency and its director have craftily orchestrated their case and their "mistakes" to create what may be a perfect storm. Fortunately, as the truth continues to come out and tech companies continue to push back, the clouds of deceit and obfuscation appear to be clearing.

There is a lot at stake here. In the digital age — more than ever — there is no line of demarcation between privacy and liberty. Concerned Americans should encrypt all their devices and communications and bring pressure to bear on legislators to reject any bill that threatens that right. And they should pray for the success of Apple in this case. Liberty may well depend on it.