New American

Written by C. Mitchell Shaw on March 30, 2016

FBI v. Apple Case: Government Smoke and Mirrors

After a month of claiming — in court documents, sworn testimony, and public statements — that "Apple has the exclusive technical means" to access the data on the encrypted iPhone 5C used by one of the San Bernardino shooters, the FBI has now dropped the case. The agency claims it "discovered" a "new" method that allowed investigators to access that data without forcing Apple to build a backdoor into the iOS platform.

During the month-long showdown between the FBI and Apple over the issue of encryption, one expert after another came forward to debunk the FBI's claim that the only way into Syed Farook's phone was for Apple to build a backdoor.

NSA whistleblower Ed Snowden called it "bulls**t," and said that "There are hardware attacks that have existed since the '90s that the FBI can mount" that would give them access to the data on the phone. Daniel Kahn Gillmor, writing for the ACLU, called the FBI's claim "fraudulent," and laid out a method for extracting the data from the phone without creating a backdoor and weakening the privacy of everyone else who uses encrypted devices. John McAfee, famous founder of McAfee Antivirus, offered to decrypt the phone himself without a backdoor. He also said that backdoors — far from being a solution — actually endanger national security.

And now the FBI has asked the federal court to vacate the order and the court has agreed, since — as it turns out — the FBI's claim that "Apple has the exclusive technical means" to circumvent the encryption was false. The FBI claims it has accessed the phone with the help of a "third party" and does not need Apple's help after all.

The FBI's claim that it "discovered" a "new" method is as bogus as its initial claim that only an Apple-created backdoor could help the agency get into the phone. As the experts cited above have said, these methods are well established and well known within computer security and computer forensics circles. So, if the FBI never needed to force Apple to create a backdoor to access Farook's iPhone, what was this case really all about?

As this writer said in a previous article:

> 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.

If the FBI wanted to access only this one phone, it never needed a backdoor. What the FBI — and for that matter all the surveillance hawks — really wanted was a chance to set a precedent to allow the circumventing of *all* encryption on *all* devices. The San Bernardino case was picture perfect. Two terrorists killed dozens of people and the FBI suspected ISIS connections. An encrypted iPhone was

recovered and — par for the course — FBI Director Comey claimed that the encryption was protecting the terrorists' accomplices.

So, The FBI played a rousing game of Keystone Cops and made "mistakes" which would make a tech rookie blush. For example, the FBI ordered San Bernardino investigators to change the password on Farook's iCloud account, assuring that the iPhone could no longer back up its data. This meant that the only way to get that data was to get past the encryption.

But, the iPhone — which has a four-digit pin — allows only 10 wrong guesses before it resets and makes the data permanently inaccessible. A four-digit pin has 10,000 possible combinations, so the FBI had what it was looking for: an opportunity to try to force Apple to create an "update" that would leave the encryption in place, but remove the 10-strikes-and-you're-out element. With that tool, the FBI claimed, its investigators could keep trying until they got into the phone. The agency got a court to order Apple to comply and Apple resisted.

Even as the FBI and the Justice Department were arguing that the All Writs Act of the horse-and-buggy era somehow applied and could be used to legally justify forcing a company to weaken its own product, a federal judge in a similar, but unrelated, case ruled that the FBI could not use the All Writs Act to force Apple to break into the phone of a suspected drug dealer in New York.

With the hearing to decide the validity of the court order approaching, Comey apparently read the writing on the wall and decided this was not the picture-perfect case after all. The day before the hearing, the FBI asked the court to postpone the proceedings and to set the order aside, claiming that a new method had been found.

Apple has sought to find out what this "new method" is, but the FBI and Justice Department have classified it. This writer will need to be forgiven his skepticism if he fails to take the FBI at face value in any of this.

While mainstream media reports that the FBI vs. Apple case is over, little could be further from the truth. The real battle for the rights of private citizens to protect their communications and data by using strong encryption is just beginning.