New American

Written by **C. Mitchell Shaw** on April 21, 2016

Real Reason Behind Apple Case: War on Encryption

After months of legal battles, a public relations war, and congressional testimony on whether Apple should be forced to help the FBI break into an iPhone used by one of the San Bernardino shooters, the FBI accessed the iPhone without Apple's assistance. And — as *The New American* predicted — the agency has now admitted that nothing of value was found on the phone. But, as has become increasingly clear, the U.S. government viewed its case against Apple as merely one salvo in a broader war against encryption.

CBS News reported last week that "nothing of real significance" was discovered on the phone after the FBI managed to circumvent the encryption of the iPhone 5C used by Syed Farook:

> A law enforcement source tells CBS News that so far nothing of real significance has been found on the San Bernardino terrorist's iPhone, which was unlocked by the FBI last month without the help of Apple.

FBI Director James Comey claimed — in sworn testimony before Congress — that "Apple has the exclusive technical means" to access the data on encrypted iPhones. He also claimed that his agency could not gain access to the valuable data on the phone that might lead investigators to Farook's accomplices unless Apple created a backdoor into the iPhone. Because Apple refused to cooperate, the FBI persuaded a federal court to issue an order forcing the company to weaken its own product. Apple fought the order and asked for its day in court.

As the date of the hearing was approaching, another federal judge in a separate, but related, case ruled against the FBI and said that the agency could not force Apple to access an iPhone used by an accused drug dealer in New York. Since the FBI's claims in both cases relied on the same (mis)interpretation of the All Writs Act, it seemed likely that the FBI would receive the same answer in the San Bernardino case.

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.

It should be obvious by now that the many of the FBI's claims were false. Others were simply far reaches. Not one — it seems — was realistic.

Since the FBI somehow managed to access the phone without forcing Apple to create a backdoor, it is demonstrably false that "Apple has the exclusive technical means" to circumvent the encryption on the iPhone. In fact, when the FBI made that claim, NSA whistleblower Ed Snowden called it "bulls**t." He added that "there are hardware attacks that have existed since the '90s that the FBI can mount" to gain access to the data on the phone.

As this writer wrote at the time:

> 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.

The FBI's claim that accessing the data on the phone could lead investigators to Farook's accomplices was — while *theoretically possible* — so thin as to be little more than a pipe dream. There was never any realistic chance that the phone would yield any valuable information. As this writer said in a previous article:

> 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?

Now that it is known that the phone does not contain anything of value, the question, "Why all the fuss?" stands in even sharper contrast. The answer is simple: The FBI — and other surveillance hawks — were never really interested in Farook's phone in the first place. They certainly knew it would not likely provide ground-breaking intelligence. The real goal all along was the setting of a precedent.

If FBI investigators had simply wanted the data from Farook's phone, they could have gotten it without demanding that Apple circumvent its own encryption software. Instead, the FBI made a series of "mistakes" that would make a technology rookie blush. As this writer also said in the article quoted above:

> 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 an end to the private use of encryption and an increase in government surveillance.

The end-game of this play by Comey and his fellow surveillance hawks is the end of encrypted data storage and communications in the hands of private citizens. The FBI vs. Apple case was one attempt at

accomplishing that end. Now that it has failed, the next attack has been launched.

No sooner had the FBI dropped its case against Apple than the surveillance hawks in Congress introduced a bill to essentially ban all encryption. The Compliance with Court Orders Act of 2016, also known as the Feinstein-Burr Decryption Bill, was introduced in the U.S. Senate earlier this month. The bill requires that "all providers of communications services and products (including software)" provide "data in an intelligible format to a government pursuant to a court order, and for other purposes." Running more than nine pages, the bill spells out in clear detail the requirements of "any entity" that provides encryption for either data storage or communications. In short, the U.S. government wants a backdoor.

It should come as no surprise that Senators Richard Burr and Dianne Feinstein would co-author a bill to end any encryption worthy of the name. Both Burr and Feinstein have long made known their disdain for the use of encrypted devices and services in the hands of private citizens.

While the bill is not expected to pass (even the White House has distanced itself from the bill), it does demonstrate that the new Crypto Wars are not over just because the FBI dropped its case against Apple. In fact, the war has really just begun.