Mondialisation.ca
Centre de recherche sur la mondialisation

« Privacy Crisis »: Why the FBI's Case Against Apple is Falling Apart

Par Shawn Helton
Mondialisation.ca, 04 mars 2016
21st Century Wire 3 mars 2016

Région : USA
Thème: Intelligence, Law and Justice, Police State & Civil Rights

This week a House Judiciary Committee began overseeing details of a US Federal Court case between tech company Apple and the FBI.

On February 16th, Apple CEO Tim Cook publicly rejected a court order to decrypt an iPhone said to be connected to the San Bernardino mass-shooting case from December of 2015.

The House Judiciary Committee listened to the controversial case between tech titan Apple and the FBI a day after Magistrate Judge James Orenstein of New York, struck down a federal court order pressuring Apple to help access encrypted data in a separate case involving illegal drug trafficking.

The landmark decision made by Judge Orenstein stated that the All Writs Act of 1789 (also used as the FBI's main argument in the Apple/San Bernardino case) *"does not permit a court to order companies to pull encrypted data off a customer's phone or tablet, "* according to a recent article from *The Washington Post*.

The *Post* continued by discussing Orenstein's lengthy argument against the FBI's order against Apple in the drug related case:

> "In a 50-page opinion disdainful of the government's arguments, Orenstein found that the All Writs Act does not apply in instances where Congress had the opportunity but failed to create an authority for the government to get the type of help it was seeking, such as having firms ensure they have a way to obtain data from encrypted phones."

In addition, The *Post* outlined some of the social engineering aspects involved in the lead up to the FBI drug case overseen by Judge Orenstein, a case which has arguably been a part of an overarching back drop concerning the larger San Bernardino case:

> "The Brooklyn case began last fall when Orenstein, one of a handful of magistrates across the country who are activists in the surveillance debate, received the government's application to issue an order to Apple."

While Apple has previously helped the federal government with some 70 phone cases since 2008, Judge Orenstein examined several problems with the FBI's use of the All Writs Act:

> "In an Oct. 9 ruling, Orenstein identified what he thought was a problem with the government's argument. Though prosecutors cited a 1985 decision that found that the All Writs Act is a source of authority to issue writs "not otherwise covered by statute," he said they failed to cite another part of the decision that found that the act does not authorize the issuance of "ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate."

The new ruling in the FBI drug case will likely have a heavy impact on the eventual *ruling* in the San Bernardino/Apple court order, as it directly questions the heart of the government's argument to gain easier access to encrypted consumer data.

It's also interesting to note, that it was the FBI who put themselves in this position regarding the San Bernardino phone as they reportedly ordered the password to be reset via iCloud shortly after the apparent mass shooting.

You have to wonder why the agency would have ordered a new password almost immediately following the highly dramatic scene in San Bernardino…

'INVENTIONS OF REALITY?' – Is this latest "privacy crisis" a manufactured drama or a legitimate battle for those in the tech industry?

What's interesting here, is that ABC news reported on December 3rd, a day after the apparent shooting:

> "Sources say mobile phones, hard drives, virtually anything with digital memory that was associated with the alleged shooters — Syed Farook and Tashfeen Malik — was smashed."

Adding to that, we've mentioned a number of times here at *21WIRE*, that none of the eyewitness testimony mentioned seeing a female shooter at the scene of the Inland Regional Center in the aftermath of the San Bernardino shooting.

A Right to Privacy

In our previous article detailing the ongoing encryption saga between Apple and the FBI, we stated that there are no guarantees in the security world, especially if a digital master-key were to be created, as this would potentially make it easier for invaders (either the government, or various hackers) mining for data moving forward into the future.

In a recent *Guardian* article, some of those involved in the technology and security sector offered their thoughts regarding the government's continued encroachment on individual privacy:

Dan Kaminsky, the security expert who made his name with the discovery that one of the most basic parts of the internet, the domain name system, was vulnerable to fraud – disagrees:

> "Feds want final authority on engineering decisions, and their interests don't even align with fighting the vast bulk of real-world crime."

Kaminsky further explained why Apple's security measures already help law enforcement:

> "If my iPhone is stolen, my emails stay unread, my photos stay unviewed, and I don't need to notify anyone that the secrets they entrusted me with are going to show up on the internet tomorrow."

Continuing, *The Guardian* interviewed former FBI agent Michael German, currently at judicial think-tank the Brennan Center. The following is a portion of that interview:

> "After 9/11, you had this concept of total information awareness. The intelligence community was very enamoured of the idea that all information was available. Much like the NSA, they wanted to see it all, collect it all, and analyse it all."

Additionally, there are many who believe weaker encryption may pose an even bigger security risk globally.

In many ways, it appears as though federal agencies are seemingly searching for the right *crisis* to push public opinion in favor of the state when it comes to security.

This is at the core of the perpetual privacy and security battle post 9/11…

'TARGETING PRIVACY' – FBI Director James Comey speaking at the Brookings Institution in October of 2014 about Going Dark. (Photo link brookings)

Shining a Light on the FBI 'Going Dark'

Last September, *The Washington Post* published an article entitled,**"Obama faces growing momentum to support widespread encryption**, " and within its contents, perhaps the true nature of the security/privacy issue was laid bare (hat tip saperetic):

> "Privately, law enforcement officials have acknowledged that prospects for congressional action this year are remote. Although "the legislative environment is very hostile today," the intelligence community's top lawyer, Robert S. Litt, said to colleagues in an August e-mail, which was obtained by The Post, "it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."
>
> « There is value, he said, in keeping our options open for such a situation."

Interestingly, in October of 2014, FBI Director James B. Comey, explained while speaking at the Brookings Institution he was *"focused on trying to get the law changed"* so that tech companies would have to *comply* with law enforcement to unlock data on various devices.

Continuing, he outlined the current security agenda concerning the FBI:

> "We have the legal authority to intercept and access communications and information pursuant to a court order, but we often lack the technical ability to do that."

The Brookings speech from 2014, appeared in stark contrast with a recent emotionally driven op-ed Comey wrote for *Lawfare* entitled **"We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead."** Here's a passage from that piece, that clearly displays the conflicting message of the FBI director:

> "We simply want the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it. We don't want to break anyone's encryption or set a master key loose on the land."

The *Guardian* refers to this as a "two-pronged approach" on the public's senses – as one tone from the FBI comes across as caring and the other seems more focused on the greater, nationalistic implications of encryption.

Think *good cop/bad cop* hovering over you in an interrogation room and you'd be getting very warm.

This is the kind of psychological drama that has prompted some in media to think that the law enforcement agency has been exploiting the public in the wake of tragedy, in order to increase security measures.

This is absolutely something to watch.

So, what are we to make of the FBI's claims of going dark in the digital age?

It has long since been claimed that intelligence agencies fear *going dark* in the age of high-tech gadgetry. This idea is vastly overblown and not rooted in reality, especially when you consider the many revelations concerning NSA spying, collection of bulk metadata and other tracking programs such as the IMSI catcher, otherwise known as **Stingray** (Stingray acts as cell tower locking onto all devices in a certain area) intercepts phone calls, texts, as well as your location.

The very notion that law enforcement will somehow be condemned eternally to outdated methods to catch criminals in the future – is patently absurd.

Furthermore, the concept and presentation of the FBI's "going dark" scenario is nothing more than a talking point used to increase a police state apparatus within the United States.

Don't Panic

On February 1st, a group of experts published report regarding the current status of law enforcement and their ability to keep up with the demands of crime solving in the world today. The lengthy report entitled **"Don't Panic"** was compiled by The Berkman Center for Internet & Society at Harvard University.

Here's a passage below examining the FBI's catchy mantra, 'Going Dark':

The U.S. intelligence and law enforcement communities view this trend with varying degrees of alarm, alleging that their interception capabilities are "going dark." As they describe it, companies are increasingly adopting technological architectures that inhibit the government's ability to obtain access to communications, even in circumstances that satisfy

the Fourth Amendment's warrant requirements.

Encryption is the hallmark of these architectures. Government officials are concerned because, without access to communications, they fear they may not be able to prevent terrorist attacks and investigate and prosecute criminal activity. Their solution is to force companies to maintain access to user communications and data, and provide that access to law enforcement on demand, pursuant to the applicable legal process.

However, the private sector has resisted. Critics fear that architectures geared to guarantee such access would compromise the security and privacy of users around the world, while also hurting the economic viability of U.S. companies. They also dispute the degree to which the proposed solutions would truly prevent terrorists and criminals from communicating in mediums resistant to surveillance.

While the report states that encryption is a difficult issue for law enforcement, all sorts of digital data is unencrypted and therefore can be accessed via a search warrant if there is cause – not to mention the spying capabilities of a plethora of smart devices also available for review.

Below is FBI Director (former Senior Vice President at Lockheed Martin) discussing the idea that the government is Going Dark…

In an article entitled "**Here's Why the FBI Went After Apple When It Did**," Fortune magazine revealed that on February 9th, DOJ head **Loretta Lynch** requested *"an extra $38 million to help the FBI development workarounds on data encryption, bringing the total budget of what it calls "project Going Dark" to $69 million."*

Will the FBI continue to develop "encryption workarounds" in the event that they lose their battle with Apple over the San Bernardino case?

In Summary

Regardless of how you shape the court battle between Apple and the FBI, this is about the government wanting a more direct route into personal devices moving ahead.

For Apple, this is a very important issue as a dip in consumer confidence, could be a crushing blow to the tech company's overall brand.

It's important to remember anomaly ridden events such as the San Bernardino shooting and the suspicious events in Garland, Texas, of last year, in addition to other *inconvenient truths* concerning the government's role in manufacturing its own terror plots – which have ironically prompted calls for greater national security, while continuing to appropriate large funds to federal agencies.

You have to wonder, has the FBI's case against Apple fallen apart?

Articles Par : **Shawn Helton**