Written by **C. Mitchell Shaw** on March 18, 2016

Obama Ignores Experts; Calls for Backdoors for Encryption

As the FBI and Apple wage battle over the rights of private citizens to protect their data and communications by using encryption, both the FBI and the White House have said the FBI has "the full support of" the president. Last week, President Obama made that support clear in a speech in Texas.

His comments were made during a speech at the South by Southwest Festival in Austin, Texas. In what Reuters called Obama's "most expansive [remarks] on the subject since the dispute," the president "made clear that, despite his commitment to Americans' privacy and civil liberties, a balance was needed to allow some intrusion when needed." As is almost always the case when heavy handed politicians speak of "a balance" between liberty and security, what President Obama meant was that Americans will be expected to give up privacy for an empty promise of security.

Also par for the course, the president trotted out those two favorite beasts of burden for the surveillance hawks: children and the fear of terrorism. He told the crowd:

> If technologically it is possible to make an impenetrable device or system where the encryption is so strong that there is no key, there's no door at all, then how do we apprehend the child pornographer, how do we solve or disrupt a terrorist plot?

This is the most common argument of the surveillance hawks. Encryption, they claim, is a tool of terrorists and other terrible criminals. Never mind that many more law-abiding citizens use encryption for legitimate purposes all the time. Yes, terrorists and other criminals use encrypted devices and communications. They also use cars, houses, doors with locks, baseball bats, knives, rope, PVC pipe, guns, and thousands of other things that ordinary law-abiding people use. But that is no reason to ban any of those things.

Actually, the similarity in the way the elites in government treat guns and encryption is a topic *The New American* has addressed previously:

> For all the ostensible reasons that the intelligence and law-enforcement communities give for wanting to limit the ability of ordinary citizens to encrypt their data and communications, the real reason is that those in power love power and want a monopoly on it. Government officials — who

> use encrypted systems for both data storage and communications — don't want private citizens to use that same technology. These are the same individuals who go about their daily lives surrounded by armed police officers, military personnel, and private security guards while decrying the evils of an armed society. This double standard is more than mere hypocrisy; it is tyranny.

Another striking similarity is that the elites who would disarm all ordinary Americans while surrounding themselves with armed personnel typically know almost nothing about guns. Those same elites — while seeking to put and end to encryption in the hands of the people they have sworn to serve — prove almost every time they address the subject that they don't have even a rudimentary understanding of technology.

The president's inane claim that "it is possible to make an impenetrable device or system where the encryption is so strong that there is no key, there's no door at all" deserves a little attention. As a self-professed crypto-nerd, I could find such a statement funny if it weren't coming from the bully pulpit occupied by the supposed "leader of the free world."

Let me make this clear: Any device where there "is no key, there's no door at all" is a broken or "bricked" device. It is worthless to the owner. I have personally bricked several Android phones when I was first learning the skills necessary to "root" those devices in order to unlock their full potential. Encryption does not "make an impenetrable device or system where the encryption is so strong that there is no key, there's no door at all." It makes the device accessible to the person who holds the key and can open the door.

Allow me to self-identify as one of those people that encrypts everything. I am writing this article on a laptop that has three hard-drives. They are all encrypted using different keys. Only I know the pass-phrases that can access those keys and gain access to the data stored on those drives. My pass-phrases are sufficiently long and random that www.howsecureismypassword.net estimates that it would take a desktop computer 49 quindecillion (that's 48 zeros) years to crack them. While no one but me can access that data, the data is easily accessible by me.

Perhaps the president should spend a little time reading up on encryption before he demonizes it.

With the two most striking similarities of the elitists' mentality toward firearms and encryption noted, it is important to point out that there at is least one major difference which the surveillance hawks always fail to recognize. While it takes a factory to create a modern firearm, anyone with a good understanding of cryptography can write the code necessary to create unbreakable encryption using nothing but a $200 laptop while sipping a cup of Zen tea at Starbucks. Trying to stop encryption is ridiculous. They may as well outlaw mathematics.

In fact, it is a well known fact that terrorists do not use Apple's iCloud service or WhatsApp, or other readily available and popular tools for planning and carrying out their evil deeds. As *The New American* reported when the surveillance hawks tried to blame the Paris attacks on the use of encryption:

> It is common knowledge that terrorists tend to keep their tools to themselves. Their cryptography is no different. Rather than use the same cryptographic tools as the public, such as Tor or GPG, they typically develop their own. It makes logistical sense for them to do it that way, because they don't need software that will scale to millions or even hundreds of users. If they develop their own proprietary encryption software that they scale to a dozen (or even a few dozen) users, it is better for their purposes.
>
> In fact, a newly released study by Flashpoint Global Partners shows that not only are terrorists

creating their own tools for encrypted communications, they were doing so *before* Snowden's revelations. More importantly, their use of cryptographic tools has not increased in the more than two years since those revelations. As the report explains:

> For many years, the jihadi community has been cognizant of the benefits of encrypted communications and, as such, has developed its own proprietary cryptologic software in order to meet this demand. In October 2010, Al Qaeda in the Arabian Peninsula (AQAP) dedicated an entire sub-section of its English-language *Inspire* magazine to help teach would-be AQAP recruits about the need for digital encryption.

As The Daily Dot reported:

> In 2007, well before the Snowden revelations in 2013, software called Asrar al-Mujahideen (Secrets of the Mujahideen) was released on an Al Qaeda Web forum known as "al-Ekhlaas." This software is used to encrypt "messages and files between users and is promoted as a trusted and secure avenue for terrorist groups," according to Flashpoint.

But last week the president ignored all that and advocated for a "solution" about which there is nearly universal negative consensus within the tech community. Reuters reported:

> He acknowledged skepticism about the government in the wake of the revelations about U.S. surveillance programs by former National Security Agency contractor Edward Snowden.
>
> But he pressed his point that a compromise that respected civil liberties and protected security had to be found. That solution would likely be a system with strong encryption and a secure "key" that is accessible to the "smallest number of people possible" for issues that were agreed to be important.

What the president is describing is a backdoor. The problem is that there is no way to create a key that can be used by only certain people. That's not how keys work and it's not how encryption works. Almost two years ago, more than 140 tech companies came together and addressed this issue. As *The New American* reported at the time:

> More than 140 tech companies, trade associations, computer security and policy experts, and civil society organizations signed a letter addressed to President Obama urging him "to reject any proposal that U.S. companies deliberately weaken the security of their products," and to "instead focus on developing policies that will promote rather than undermine the wide adoption of strong encryption technology." The signers of the letter argue that "such policies will in turn help to promote and protect cybersecurity, economic growth, and human rights, both here and abroad."
>
> The letter, dated May 19, calls strong encryption "the cornerstone of the modern information economy's security," and says "Encryption protects billions of people every day against countless threats — be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies' most valuable trade secrets, repressive governments trying to stifle dissent, or foreign intelligence agencies trying to compromise our and our allies' most sensitive national security secrets."
>
> The letter's signatures take up almost four of its six pages and include some significant names in the tech world. Many of the people and organizations listed have been supporters of President Obama. Hopefully he will heed their wise advice.

It appears that in his waning days in office, President Obama has decided to ignore these experts.

Photo of President Obama at South by Southwest Festival in Austin, Texas: AP Images