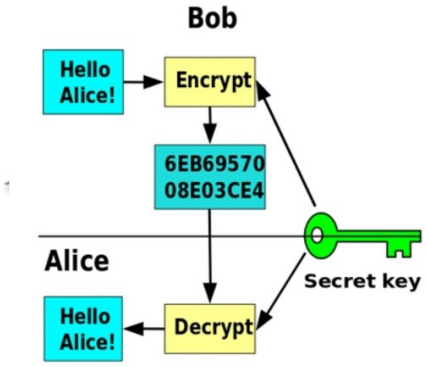
Written by **C. Mitchell Shaw** on November 19, 2015

Surveillance Hawks Blame Cryptography for Paris Attacks



Unsurprisingly, in the wake of last week's deadly attacks in Paris, there has been an escalating demand — by those always in favor of such things — for an increase in surveillance. There has also been a call for limitations to technology that permits encrypted communications. The surveillance hawks seem to believe that liberty and security cannot coexist. Given the choice, they opt for sacrificing liberty for the sake of security.

There are serious problems with that way of viewing the balance of power, though. First, liberty and security are not mutually exclusive. Second, sacrificing liberty does not result in security. Finally, Benjamin Franklin was right when he wrote, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." History has indeed shown that they wind up with what Franklin said they deserve: neither.

But none of that has stopped the surveillance hawks from calling for an end to cryptography. In the few short days since the attacks in Paris left 129 dead and hundreds more injured, there have already been repeated demands for companies that offer encrypted services to provide "back doors" to government agencies. These "back doors" would allow encrypted communications to be intercepted and decrypted by government agents. This, they claim, is necessary to fight terrorism and prevent other attacks such as the ones in Paris.

One such call appeared in *Foreign Policy*, which always sides with the hawks. An article entitled "Paris Attacks Reopen Crypto Wars" stated:

> For months, U.S. intelligence officials have warned that the proliferation of strong encryption technologies has hampered their ability to detect terrorist plots — including last week's deadly attacks in Paris. The question now is whether Washington and its allies will force Silicon Valley to give law enforcement agencies a way around those technologies.
>
> The bloody attacks in Paris that killed 129 have prompted searing questions over how the intelligence services of multiple countries failed to detect what was an organized plot involving multiple individuals and extensive planning in at least three countries. One answer, according to the top law enforcement official in the United States: the ease with which militants can use encrypted messaging tools, such as Apple's iMessage, WhatsApp, and Signal, that have such strong security measures that Western intelligence services can't unscramble communications.

In the midst of all the insinuation, what is missing is any reference to real cases where this is true. Saying that "officials have warned that the proliferation of strong encryption technologies has hampered their ability to detect terrorist plots — including last week's deadly attacks in Paris" is easy. Backing it up, however, proves more difficult. Especially since this same article admits, "It is still unclear whether the Paris attackers actually used encrypted communications technology in their planning."

None of that lack of evidence has kept pandering politicians and uncountable bureaucrats from making wild claims and placing the blame squarely on the shoulders of cryptography and those — such as Ed Snowden — who promote its use.

Senator Dianne Feinstein, who sits on the Senate Intelligence Committee, told MSNBC on Monday, "Silicon Valley has to take a look at their products. Because if you create a product that allows evil monsters to communicate in this way, to behead children, to strike innocents, whether it's at a game in a stadium, in a small restaurant in Paris, take down an airliner — that's a big problem." Except she doesn't show that it is "a big problem" because she doesn't even show that it exists. She simply alludes to it, and in doing so muddies the water.

Attorney General Loretta Lynch played the same gambit in her testimony before the House Judiciary Committee on Tuesday. As *Foreign Policy* reported:

> Lynch said that the use of such advanced encryption technologies has hampered investigations of individuals plotting violence in the United States. Citing unspecified investigations, Lynch said that terrorist suspects have switched from traditional communications tools to ones with end-to-end encryption, which even providers can't unlock when served with court orders to do so. By using such tools, suspects ensure that officials "no longer have visibility into those discussions" about plots, Lynch said.

It's an interesting accusation, but where is the evidence? "Citing unspecified investigations" is not convincing to anyone who did not already want to be convinced.

Senate Armed Services Committee Chairman John McCain is obviously reading the same playbook, because he did not vary from the status quo one iota. He told MSNBC that companies providing these encrypted services should be forced to provide a "back door," adding, "It's time we had another key that would be kept safe and only revealed by means of a court order." As if the government that has moved heaven and earth to spy on ordinary citizens could be trusted not to abuse that power. Again. McCain continued, "Recruitment and training and equipping can go on on secure sites, and we cannot let that continue to happen, in all due respect to my friends in Silicon Valley." Like his fellow surveillance hawks, he failed to offer any evidence of his claims.

The problem with "back doors" is that that is just not the way cryptography works. The most powerful form of cryptography is "public key encryption," such as the popular GPG encryption used by millions, including Snowden. The way it works is that each user has a public key (which they share with others) and a private key (which they keep secret). The communication is encrypted using the sender's private key and the recipient's public key. The recipient then decrypts the message using his private key. Since the only keys that can unlock the communication are private, the communication is private. Providing "another key" that only government can use is a farce. Any such key would inevitably be exploited by hackers and foreign governments. Experts in cryptography agree: There is simply no way for it to be "kept safe."

Furthermore, all of this is for nothing since terrorists don't use Apple's iCloud service or WhatsApp, or other readily available and popular tools to conduct their secret hellish plans, anyway. 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.

So, if terrorists are not increasing their use of cryptography and if the tools they are using are proprietary tools developed in-house, why is the American intelligence community demanding that the tools Americans use be weakened? Is it about security or is it about control? Considering that they are using the deaths of 129 ordinary citizens and the the wounding of hundreds more to perpetuate their myths about the use of cryptography, the answer is evident.

Americans who are concerned about privacy and liberty need to increase their use of these tools and demand that government agencies cease their war on cryptography.