Written by **C. Mitchell Shaw** on June 4, 2015

Tech Industry Urges Obama: Don't Weaken Encryption

With recent news of the off-again, on-again status of some of the the worst provisions in the PATRIOT Act, it is important to note that Capitol Hill is not the only — or even the most important — battlefield in the fight for privacy and liberty. As the drama plays out in the halls of Congress, more and more people are discovering the value of strong encryption to protect their privacy and liberty from oppressive government agencies that would spy on them.

Not surprisingly, the same government agencies doing that spying are also publicly attacking the right of individuals to encrypt their smartphones and make them essentially "NSA-proof." When Apple announced last year that iOS 8 would be released with full encryption activated by default and Google followed suit by beefing up the encryption in Android 5.0, FBI Director James Comey accused the companies of "market[ing] devices that would allow someone to place themselves beyond the law," adding that it troubled him "a lot." Of course, he trotted out the surveillance state's two favorite beasts of burden: children and terrorism. "The notion that people have devices, again, that with court orders, based on a showing of probable cause in a case involving kidnapping or child exploitation or terrorism, we could never open that phone? My sense is that we've gone too far when we've gone there," he told CBS News.

The crux of the issue is that the new encryption standards used in modern smartphones leave control in the hands of the user — not the manufacturer, the carriers, or government agencies. When encryption is properly set up with a strong password, the data on the phone cannot be accessed except by entering the correct password.

Comey argues that this will make it impossible for law-enforcement agencies to do their jobs. There are two points that need to be made here. First, Apple and Google are simply responding to consumer demands for greater control over their data in the wake of the Snowden revelations. If government agencies had not gone so far in their intrusion into everyone's privacy, the demand would not have existed in the first place. Second, Comey's claim is false. Encryption does not make it impossible for law-enforcement agencies to do their jobs. If probable cause exists, a suspect could be ordered by a court to unlock the device so that a duly issued search warrant could be served. If the suspect refuses, he would be in contempt of court and could be jailed until he complied.

Apple and Google are not alone in offering software solutions that thwart snooping and surveillance. *The New American* reported last year on a variety of technologies that individuals can use to make their communications nearly impervious to these invasions of privacy. As more and more people use these tools, it becomes less and less worthwhile for government agencies and nosy corporations to spy on people. A culture of privacy and digital liberty is beginning to take hold.

Because these tools are so effective, Big Government wants to force companies to install "back doors" in the encryption software so that government agents can unlock the devices without the users'

cooperation. Of course, those agents would do it only when it was necessary. Unfortunately, that is the same line Comey and his ilk use when discussing the unconstitutional surveillance that brought us to the place where users feel the need to encrypt their phones in the first place. Those back doors would be more like revolving doors.

Setting aside the certainty that the myriad of three-letter agencies that have been spying on all of us would abuse the back doors, the simple fact is that there is no secure way to create a back door that can be used only by government agencies. The very existence of a back door would create vulnerabilities that hackers would be able to exploit.

NSA director Admiral Michael Rogers thinks the solution is to have the encryption key broken into parts and held by multiple parties. That way, no one agency could use it to unlock a phone. He considers that a separation of powers. But in light of the complicity and cooperation between agencies spying on us already, breaking the key up and distributing it to multiple agencies wouldn't solve the problem. It would boil down to a matter of trust, and employees in those agencies don't deserve that trust. No one does. Especially when they have spied on everyone just because they could.

The tech industry is not sitting idly by. 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.