Written by C. Mitchell Shaw on February 22, 2016
Published in the February 22, 2016 issue of the New American magazine. Vol. 32, No. 04

Correction, Please!

Cryptic Encryption Policies

Item: Senator Richard Burr (R-N.C.), chairman of the Select Committee on Intelligence, wrote an article for the Wall Street Journal *on December 23, 2015 in which he claimed that "Encrypted devices block law enforcement from collecting evidence. Period." Burr went on to say that encrypted devices and communications enable "murderers, pedophiles, drug dealers and, increasingly, terrorists." He repeated the oft-recited claim that terrorists are using encryption to "go dark":*

Unfortunately, the protection that encryption provides law-abiding citizens is also available to criminals and terrorists. Today's messaging systems are often designed so that companies' own developers cannot gain access to encrypted content — and, alarmingly, not even when compelled by a court order. This allows criminals and terrorists, as the law enforcement community says, to "go dark" and plot with abandon.

Burr ended his article by calling for new laws banning the type of encryption offered by Apple and Google on the iOS and Android platforms, saying, "It's time to update the law."

Item: As a result of the growing number of people using encrypted devices and communication methods, Assistant Attorney General Leslie Caldwell called for "back doors" to be written into the encryption software to allow law-enforcement agencies to access those devices and communications. As reported by The Hill *on January 26, 2016, she — like Burr — touted the idea of backdoors as a solution to the problem of terrorists "going dark."* The Hill *reported, "Her remarks come the day after a newly released video from the Islamic State in Iraq and Syria (ISIS) indicated those behind the Paris massacre last year were using encryption to hide their communications," leading readers to the conclusion that popular encryption methods are tools of terrorism.*

Item: The New York Times *reported in November 2015 that both FBI director James Comey and Manhattan district attorney Cyrus Vance, Jr. are seeking "to reopen the argument that law enforcement and intelligence officials need to have access to encrypted information on smartphones with court approval." From that report:*

In a speech at a cybersecurity conference in New York, James B. Comey, who since taking over the F.B.I. has been the most vociferous about the "going dark" problem facing investigators, warned that "we're drifting to a place" where court orders to gain access to text messages or computer communications "are ineffective." Both devices and data in transmission are often encrypted so well that the law enforcement and intelligence agencies cannot crack the coding — and their makers have designed the system so they do not hold the key.

The Times *also quoted a white paper released by Manhattan DA Vance — whose father was President Carter's secretary of state, as well as serving under Presidents Johnson and Kennedy as deputy secretary of defense and secretary of the Army — as saying, "Last fall, a decision by a single company changed the way those of us in law enforcement work to keep the public safe and bring justice to victims and their families," referring to Apple. "We risk losing crucial evidence in serious cases if the contents of passcode protected smartphones remain immune to a warrant."*

Correction: As many computer experts have repeatedly said, all calls for weakening encryption standards are technologically backward. Those making the calls either ignore or are unaware of the fact that that is simply not how encryption works. Any backdoor approach would require that the software have a "master key."

Take encrypted communications as an example. The most powerful encryption is "public key encryption," such as the popular PGP encryption (or its open-source counterpart, GPG) used by millions, including NSA whistleblower Edward Snowden. The way it works is that each user has a public key (which is shared with others) and a private key (which is kept 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."

Likewise, calls for weakening encryption standards are a threat to privacy, and by extension, liberty. The growing use of strong encryption by private citizens is the result of an overreaching government that has abused its power by spying on all citizens — the innocent and the guilty alike. Remember that before the Snowden leaks, government officials at every level denied that blanket surveillance was taking place. Many of them even denied it in sworn testimony before congressional committees.

Strong encryption is vital to privacy precisely because government agencies abuse their power.

Private citizens did not start the Crypto Wars, but since technology is — thankfully — an equal-opportunity tool, they are better equipped to protect their privacy against a growing surveillance state. Government officials — who use encrypted systems for both data storage and communication — 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. And as usual, the surveillance hawks put their two favorite beasts of burden — children and terrorism — into play when they call for limits and bans on the use of encryption. It's an emotional appeal designed to manipulate the people into sacrificing privacy — and liberty — in the name of security.

As for the claim that terrorists are using popular encryption tools to "go dark" and plan their evil deeds under the cloak of secrecy, it is a lie wrapped inside another lie.

First of all, given the ubiquitous surveillance conducted by the various three-letter U.S. government agencies and their counterparts in the other "Five Eyes" nations (Australia, Canada, New Zealand, and the U.K.), there is no such thing as "going dark" for those who have — by their terrorism — gained the undivided attention of government agencies with nearly limitless budgets to finance their surveillance. Even when they use encrypted communications, terrorists cannot hide from satellite photography, spy planes, parabolic and laser microphones, agents who infiltrate their ranks, and a plethora of other "targeted" surveillance techniques.

The second part of the lie is that popular encryption tools — such as the full-disk encryption of iOS and Android and communication apps such as WhatsApp, Signal, ProtonMail, and others — are the work-a-day tools of terrorists. The fact is that terrorists *are* encrypting their data and communications, but they *are not* using commercially available tools to do it. They create their own tools for encrypted communications and data storage. After all, they don't need encryption tools that can scale to millions (or even thousands) of users; they work in small, tight-knit cells. The use of home-baked encryption tools by terrorists is nothing new, either. As *The Daily Dot* reported last November,

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, the reality is that the genie is already out of the bottle. There is no going back. Encryption is here to stay and the only question is whether law-abiding citizens will continue to have legal access to it. If encryption is outlawed, only criminals and government agencies will have encrypted data and communications. The difference is that there is literally *no way* to regulate the technology on which encryption is built. Terrorists and other criminals are already writing their own programs and will certainly continue to do so.

That is all the more reason for private citizens to have access to the same types of tools to protect their data and communications.

— C. Mitchell Shaw