Written by **C. Mitchell Shaw** on October 21, 2020

Privacy at Stake in New Crypto Wars

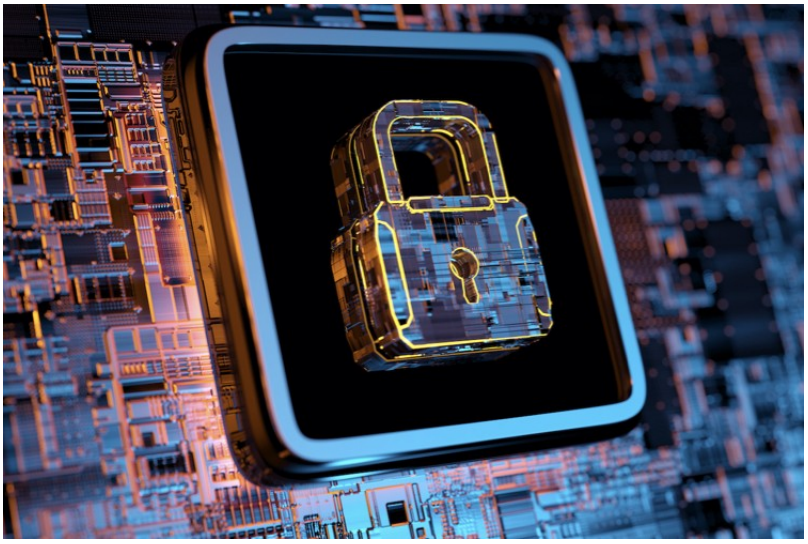

Image: MF3d / E+ / Getty Images Plus

The Crypto Wars are heating back up. As Ed Snowden's revelations about mass digital surveillance caused citizens in America and around the world to realize just how much governments spy on their own people, encryption — which had been difficult to achieve (and therefore not used by the masses) — became commonplace thanks to simple apps and services. As more and more private citizens have adopted encryption to protect their data, governments have pushed back more and more.

While one common thread in that push-back has been demands by government for "backdoors" into encrypted apps and services, the tactic for achieving that end has shifted lately. Previously, government agencies — such as the NSA and FBI in the United States and GCHQ in the United Kingdom — have attempted to *force* software and hardware companies to build those backdoors. Now, along with several other nations, the United States and the United Kingdom are "asking" them to do so.

The sudden shift is alarming. As someone who grew up enjoying the thrill of jumping out and scaring friends and family members, this writer can tell you that shouting "Boo!" as you jump out from behind a door is effective, but *whispering* it from behind the door while you gently reach out and touch someone's arm is *terrifying.* In this shift, spying governments around the world have gone from shouting to whispering.

The core group of nations now "asking" for backdoor access to the encryption that protects the privacy of millions are the five nations historically known as the Five Eyes — the United States, the U.K., Canada, Australia, and New Zealand. The origins of the Five Eyes can be traced to agreements between the Allies in the wake of WWII as part of the surveillance efforts of the Cold War. Though initially begun as a way to monitor communications between Communist Bloc nations, it was eventually expanded to capture all communications of everyone everywhere.

The Five Eyes nations have — for decades — assisted each other in skirting their own internal laws about surveillance of their own citizens. The tactic is simple. Since the United States could not legally spy on U.S. citizens, U.S. agencies spied on citizens of other Five Eyes nations. The intelligence agencies of those nations in return spied on U.S. citizens. Then each nation made the data available to the other nations.

In a 2016 article for the print version of this magazine (which was later published online), this writer laid out the history of the first round of the Crypto Wars. In short, as late as the 1990s, encryption powerful enough to actually work (and therefore protect communications) was classified as a "munition" and was illegal to import or export.

After lengthy legal battles, a 37-year-old software engineer named Phil Zimmermann outplayed the U.S. government by releasing the source code to his encryption program, PGP (Pretty Good Privacy), as a printed book. This made the case an issue of *free speech* and forced the government to back down. In 1996, President Clinton issued Executive Order 13026, essentially removing encryption from the munitions list.

But even though encryption was no longer illegal, it was still not widely used by individuals. While businesses adopted it as a standard (can you even *imagine* logging into your bank account online to transfer funds without that transaction being encrypted?), private individual citizens were not using it to protect their communications.

Then, Ed Snowden revealed to the world what many had long suspected: Our government routinely spies on us all.

Almost immediately after the Snowden revelations, Apple made full disc encryption standard in iOS and Google followed close behind with full disc encryption by default on all devices running Android. Encrypted apps and services — such as Signal for encrypted texts and phone calls and ProtonMail for encrypted e-mails — became available and quickly became popular.

Governments responded with wave after wave of attempts to pass legislation forcing companies to build their software in such a way that government agencies could access it. These "backdoors" would — government said — allow police and investigators to slip in while keeping "bad guys" out. The tech world was quick to point out the obvious: That is impossible. Any door that police can come through can be accessed by anyone else. Period.

Surveillance Hawks decried encryption that could keep out the government as the hiding place of bad people. The tired old line is that pedophiles, terrorists, and criminal gangs use encryption to "go dark" and hide their activities and communications. Good people — those who have nothing to hide — shouldn't have anything to worry about. After all, all they are asking for is unhindered access to all your private files and communications.

This illustrates the point that many privacy advocates have made: Even if a "good guys only" backdoor were possible, it misses the point. Joe Everyman began encrypting his communications and hard drives as a direct result of government overstepping its boundaries and spying on all of us. That does not exactly garner trust.

At any rate, government efforts in the United States to break encryption have failed time and again: They introduce the legislation and it gets shot down. They introduce it again and it gets shot down again.

But now, the Five Eyes are doing something different. Joined by India and Japan, the Five Eyes have released a statement about how the use of end-to-end encryption makes it impossible for tech

companies to identify dangerous content — such as terrorist propaganda and attack planning — and makes it harder for police to investigate serious crimes and protect national security.

The statement begins with disingenuous lip service to the protection of privacy, saying:

> We, the undersigned, support strong encryption, which plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security. It also serves a vital purpose in repressive states to protect journalists, human rights defenders and other vulnerable people, as stated in the 2017 resolution of the UN Human Rights Council. Encryption is an existential anchor of trust in the digital world and we do not support counter-productive and dangerous approaches that would materially weaken or limit security systems.

So far, so good. But wait; there's more. Having gotten the niceties out of the way, the second paragraph gets in to the real purpose of the statement:

> Particular implementations of encryption technology, however, pose significant challenges to public safety, including to highly vulnerable members of our societies like sexually exploited children. We urge industry to address our serious concerns where encryption is applied in a way that wholly precludes any legal access to content.

The statement goes on to "call on technology companies to work with governments to take the following steps" which the statement claims are "focused on reasonable, technically feasible solutions." Of course, those steps include things — such as "Enable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate" (read: "Good Guys Only Backdoors") — which are neither "reasonable" nor "technically feasible."

The subtle shift here is found in the move away from demanding to asking. This statement attempts to shift the blame for the next crime against a child or the next terrorist attack and to place it squarely on the shoulders of the tech companies that protect the privacy of hundreds of millions of law-abiding people around the globe. The message is clear: "Give us the keys to the kingdom, or the blood is on your hands."

What needs to be understood is that encryption is just math. It is made possible by powerful algorithms that scramble data in such a way that it can only be unscrambled by the correct key. Sure, Apple, Google, Signal, ProtonMail, SpiderOak, and a thousand other companies make software using it, but *anyone* can. A terrorist cell is not likely using Signal and ProtonMail. First, they likely don't trust it. Second, they can make their own encryption that does not need to scale to millions of users; it only needs to work for the two dozen of them.

This means that if the government were ever successful in making encryption illegal, only criminals would continue to use it while everyone else would be an open book for tyrannical power-mongers to read. Ditto if companies such as Apple, Google, and Microsoft comply with the guilt-laden pablum of statements such as this.

But since the best encryption softwares available are all open source, there is little to worry about. Open source software is software for which the actual source code is available for anyone to see. Because of this, a backdoor would be discovered and reported immediately. That feature is one reason this writer only uses — and only recommends — open source software.

This new wave of the Crypto Wars is in the hands of the people. Two things are needed to win it: First, use open source encryption to protect *all* of your data and communications. Second, never let up on pressuring your legislators at all levels to pass legislation protecting privacy and to vote against all legislation that would threaten it.