New American

Written by C. Mitchell Shaw on September 23, 2021

FBI Director Calls on Congress to Restrict Encryption for Americans

AP Images
Christopher Wray

FBI Director Christopher Wray asked the Senate Committee on Homeland Security Tuesday to restrict the private use of encryption so that intelligence agencies can better combat terrorism and domestic extremism. His remarks were made during the committee's counterterrorism hearing.

Every few months, it seems the surveillance hawks come swooping in on the simple tools everyday Americans use to protect their privacy. Chief among those tools is the encryption used to turn data into unintelligible strings of nonsense until the correct key is used to decrypt the data. Default encryption — such as that found on iOS and Android devices — has been a thorn in the side of the Surveillance State for year now. Add to that a list of applications and services — such as Signal, Telegram, ProtonMail, StartMail, ProtonDrive, and others — and the surveillance hawks are finding it harder and harder to surveil average citizens.

Answering a question from Senator Jacky Rosen (D-Nev.) about what Congress can do to help law enforcement and intelligence agencies fight terrorism and domestic extremism, Wray said, "I can't overstate the impact of default encryption and the role it's playing, including on terrorism." He went on to say, "The information that will allow us to separate the wheat from the chaff, in terms of social media, is being able to — with lawful process — get access to those communications, where most of the meaningful discussions of the violence is occurring."

The implication is clear: If not for end-to-end encryption (where communications are encrypted by the sender's device and only decrypted by the recipient's device), our brave and valiant spooks could do their jobs. That, of course, is a bunch of garbage. If those agencies already suspect someone of being a terrorist, they should already be investigating them and using all the tools at their disposal to that end. Those tools include many ways to watch and listen to subjects. But those tools require warrants and real investigative techniques.

But as the Snowden leaks showed, the Surveillance State prefers to vacuum up everyone's everything and sort it all out later. They constantly claim they are looking for a needle in a haystack. They have never explained how adding more hay increases their possibility of success. It appears that they are lying as they have done for years — such as when former Director of National Intelligence James Clapper famously lied under oath and on camera in sworn testimony before a Senate Committee by claiming that the NSA does not "collect any type of data at all on millions or hundreds of millions of Americans." Given their penchant for mendacity, it appears that Snowden's claim that the "needle in a haystack" argument is a smokescreen for their true objective of illegally surveilling all Americans for the purpose of creating profiles on everyone is spot on.

And while Wray and other surveillance hawks pretend that such encryption tools stand in the way of law enforcement and intelligence agencies fighting terrorism, the reality is that terrorists don't use mass-market encryption tools. They create their own.

Just think about it for a second. Encryption is essentially math. That can't be outlawed. Or, perhaps it can, but there would be no way to enforce that ban. The genie is out of the bottle and isn't going back in. Now, imagine you are a terrorist (or better yet, one of the FBI's favorite bogeymen these days, a *domestic extremist* — whatever that means). Would you send criminal communications over a service you didn't create and don't control? Not likely.

It has long been known that terrorists create their own encryption apps. Doing so gives them greater control — since they built and own the application, only they have access to it and they can know there are no back doors. It also allows them to tailor the software to their needs. And since they only need it to scale to dozens instead of millions, any bugs are easily found and solved.

By applying existing encryption standards, terrorists and other criminal groups are able to build their own applications and communicate privately — regardless of any laws prohibiting such applications. Similar to the adage, "If guns are outlawed, only outlaws will have guns" is the point that if secure, encrypted communications are outlawed, only terrorists and other criminals will have encryption. The root word of *criminal* is *crime*. Terrorists and other dangerous criminals — *by their very nature* — don't care if something (such as the attacks of 9/11) are illegal or immoral. They will just do them anyway.

So, Wray's request for Congress to ban all encryption that does not have a back door is ridiculous for two main reasons: First, it would not do what he claims it would seek to do — namely, prevent terrorists and other criminals from communicating privately. What it *would* do is prevent the rest of us — law-abiding citizens — from doing so. Secondly, his demand is technologically impossible. As the *Epoch Times* reported:

> According to Wray and other law enforcers, tech companies should be able to build "backdoors" into their encryption that preserves privacy, while allowing for access when necessary. That, they say, strikes the proper balance between data security and national security.

But what he is imagining does not (and can *never*) exist. It is likened to a lock on a door to which only the owner has the key. Law enforcement wants locks to be created to accept a "law enforcement master key" that unlocks all doors, but only for law enforcement and only when — and they *swear* this would be the case — they have really, really good reasons.

The problem here is that, first, it is impossible to create a backdoor to software that only the "good guys" can use. If it exists, others could use it, as well. And, second, it assumes that government agencies never abuse their power. Given the history of the NSA and other three-letter agencies illegally spying on U.S. citizens and lying to us and to Congress about it, that prospect is laughable.

As the *Epoch Times* reported:

> However, numerous tech experts, civil libertarians, and others say that it's impossible to build a backdoor that can't be exploited by hackers. They also say that by banning encryption, the United States would be following in the footsteps of authoritarian countries such as China, which recently blocked Signal.
>
> "It is important to understand that any kind of back door (or front door) access for the 'good guys' can also be exploited by the 'bad guys,'" the pro-industry Information Technology & Innovation Foundation stated in a July 2020 report, in the midst of the Apple-Barr controversy.
>
> "For example, key escrow systems would introduce new attack vectors that could allow attackers to gain access to encrypted information, such as by compromising the system that maintains copies of the keys."

Backdoors or any other weakening of encryption would spell the end of privacy for millions of Americans and would give the Surveillance State the digital keys to the kingdom.