New American

Written by C. Mitchell Shaw on February 14, 2020

What Does Recent CIA Revelation Mean About Encryption?

As a joint report from the *Washington Post* and German broadcaster ZDF reveals, the CIA secretly owned the major manufacturer of encryption devices used by most governments of the world from the 1950s until well into the 2000s. That Swiss company — Crypto AG — built back doors into all of its encryption so that the CIA and NSA could easily decrypt the communications at will. Since the U.S. Intelligence Community has spent the past several years renewing its war on encryption in the hands of private citizens, what does this mean for private communications of those who use encryption?

In a previous article, this writer addressed the implications of this report on failed U.S. foreign policy. Put simply: How could the United States have made so many foreign policy missteps with a direct line to the "secret" communications of 120 nations? But another hugely important question (the subject of this arirle) is: "What does the recent CIA revelation mean about encryption used by ordinary citizens?"

As the *Post* reported:

> For more than half a century, governments all over the world trusted a single company to keep the communications of their spies, soldiers and diplomats secret.
>
> The company, Crypto AG, got its first break with a contract to build code-making machines for U.S. troops during World War II. Flush with cash, it became a dominant maker of encryption devices for decades, navigating waves of technology from mechanical gears to electronic circuits and, finally, silicon chips and software.
>
> The Swiss firm made millions of dollars selling equipment to more than 120 countries well into the 21st century. Its clients included Iran, military juntas in Latin America, nuclear rivals India and Pakistan, and even the Vatican.
>
> But what none of its customers ever knew was that Crypto AG was secretly owned by the CIA in a highly classified partnership with West German intelligence. These spy agencies rigged the company's devices so they could easily break the codes that countries used to send encrypted messages.

Furthermore, the conspiracy to hack the nations of the world by selling them bogus encryption involved employees of Crypto AG who were kept completely in the dark for nearly 50 years. As the *Post* reported:

> After the CIA and BND acquisition, one of the most vexing problems for the secret partners was ensuring that Crypto's workforce remained compliant and unsuspecting.
>
> Even while hidden from view, the agencies went to significant lengths to maintain Hagelin's [the "owner" of Crypto AG] benevolent approach to ownership. Employees were well paid and had

> abundant perks including access to a small sailboat on Lake Zug near company headquarters.
>
> And yet, those who worked most closely with the encryption designs seemed constantly to be getting closer to uncovering the operation's core secret. The engineers and designers responsible for developing prototype models often questioned the algorithms being foisted on them by a mysterious external entity.
>
> Crypto executives often led employees to believe that the designs were being provided as part of the consulting arrangement with Siemens. But even if that were so, why were encryption flaws so easy to spot, and why were Crypto's engineers so routinely blocked from fixing them?

So much for the idea that a conspiracy of this scale would be impossible.

So from the 1950s until at least 2018, the CIA and NSA had unhindered access to the encrypted communications of 120 nations, a list made up of both enemies and allies. Of course, that did not prevent the surveillance hawks from claiming that modern encryption allowed criminals and foes to "go dark" and plan their nefarious deeds in secret.

This writer has dealt with — and answered — those claims in previous articles. The principle boils down to these basic facts:

(1) If — as the surveillance hawks claim — they are "looking for a needle in a hay stack," adding more hay is not the solution. They should focus their searches and not cast a surveillance net that encompasses the world and everyone in it.

(2) It is more than mere hypocrisy when the same people who use encrypted communications to hide their actions from the people refuse the people the right to encrypt their own communications. It smacks of the same elitist thinking that decries an armed populace while surrounded by armed guards, police, and military.

(3) The argument that encryption in the hands of private citizens empowers the criminal underworld and terrorists to act under the cloak of secrecy is based on the false idea that the Mafia and ISIS are downloading and using commercially available apps such as Signal and What'sApp. In reality, they are not. Since encryption is simply a math equation used to scramble data, they simply create their own. They do not need it to scale to millions of users. They only need it for dozens.

Keep in mind that while having access to the communications of 120 nations across the globe, the surveillance hawks here at home were crying about a lack of access to your data.

But can you trust Signal, What'sApp, and other companies and apps that claim to protect your data and communications? Yes — and no. It depends on the code and whether or not it is accessible. As this writer explained in his first article for The New American back in 2014:

> All encryption is not equal, as we now know that many encryption software companies have been pressured by the NSA to provide backdoors. Because of this and the closed-source nature of many of these programs, you should only use open-source encryption.

In simple terms, open-source software is licensed in such a way that its source code must be available for anyone to view, audit, modify, and redistribute. Because the open-source community is so large and diverse, the likelihood of anything nefarious being hidden in the code is at or near zero. Another benefit of open-source software is that where vulnerabilities exist, they are more quickly discovered and patched as a community of thousands of people works to solve problems. That is why viruses, which are such a problem for Windows and, to a lesser degree, Mac, are unheard of for Linux.

By way of analogy, imagine you are shopping for a frozen dinner. You find one that looks good, but the label only lists the "ingredients" as: "A proprietary blend of nutrients and flavors." Would you want to eat that if there were another choice that broke everything down and even provided you with a recipe so that you could make it yourself at home?

Open-Source software cannot hide anything. It is not a matter of trust, but of the ability to verify. Encryption offered by companies such as Microsoft may be good for keeping out the average nosy roommate or criminal, but given what this report from the *Post* reveals, it will likely not even slow a government agency down.

The upshot to this bad news about the CIA having owned the world's most respected encryption company is this: Even during that time, the surveillance hawks in the Intelligence Community and in Congress were fighting to force encryption companies to insert back doors to allow them the access they sought. That means that Open-Source encryption works and they likely can't break it. Period.

C. Mitchell Shaw is a freelance journalist and public speaker who addresses a range of topics related to liberty and the U.S. Constitution. A strong privacy advocate, he was a privacy nerd before it was cool. You can check out his "Enemy of the Surveillance State" podcast at enemyofsurveillance.podbean.com