Written by **C. Mitchell Shaw** on April 18, 2018

Surveillance Hawks Plan New Legislative Attacks on Encryption

The battle over privacy and encryption is heating up. Again. Following FBI director Christopher Wray's January calls for legislation that would put an end to any meaningful encryption standard, Senator Dianne Feinstein (D-Calif.) is planning to keep her promise to reintroduce the anti-encryption bill she and Senator Richard Burr (R-N.C.) tried to pass in the wake of the San Bernardino shooting.

The Compliance with Court Orders Act of 2016 co-authored by Feinstein and Burr never really got off the ground. In fact, fresh on the heels of the failed FBI attempt to get Apple to build in a backdoor to the encryption on their products, the bill could not even gain enough traction to make it out of committee for a vote. There was simply not enough support for the legislation.

According to a report by Reuters, not even the Obama White House would support the bill. In late May 2016, Burr and Feinstein announced that the bill was dead. They said they had not given up, though. Reuters reported that Burr said, "There was no timeline for the bill" and "Feinstein said she planned to talk to more tech stakeholders." Burr reportedly said, "Be patient," indicating that the pair had plans to try again. So the bill fizzled and failed, but that has never stopped the surveillance hawks before, and this is no different. As always, the surveillance hawks in Congress — with the support of the surveillance hawks in law enforcement — will simply reboot the bill and try again.

When Wray — new on the job — called for this new round of legislation, he claimed that the FBI was in possession of nearly 8,000 devices that could not be searched due to the encryption of those devices. As ZDNet reported in January:

> Wray said that each device was tied to a specific subject or threat, but did not say how many investigations were affected by the lack of access.
>
> ZDNet filed a Freedom of Information Act request in October to seek answers on the number of investigations impacted, but has not yet received a response beyond an initial acknowledgement.
>
> This is not the first time Wray as FBI director, like his predecessors, has argued that encryption gets in the way of investigations. The so-called "going dark" issue, referring to the inability to gain access to criminals' devices and data, remains a key challenge for the FBI.

What Wray was hinting at — though without as much subtlety as he may think — is the creation of a "backdoor" to encryption. A backdoor is an idea that has been proposed by surveillance hawks — and rejected by privacy advocates — for years. The battle over encryption — known as the Crypto Wars — has been going on since the early 1990s.

Wray claimed that the FBI's interest in unlocking encrypted devices is narrow and limited, saying, "We're not interested in the millions of devices of everyday citizens. We're interested in the devices that are used to plan or execute terrorist or criminal activity."

Of course, the surveillance hawks that have built their careers building and expanding the surveillance state have always claimed to have a specific focus. And they have lied. Given that record — including the denials of the NSA, ODNI, FBI, and other overreaching government agencies — it would be foolish to believe that this time is any different.

As the Apple case demonstrated, the desire to unlock a particular device (or pile of particular devices) is merely a smokescreen to put an end to the one type of technology that stands in the way of the surveillance state. Powerful encryption is a major part of protecting privacy in the digital era. In fact, it is essential. When used properly, it guarantees that no unauthorized person can access your data.

It is that protection in the hands of private citizens — acting as a counterbalance to the surveillance state's ability to spy on those private citizens — that is the real reason for attacks on encryption. As this writer explained in an article that originally appeared in print (in our July 18, 2016 issue) and was later published online:

> To understand what is at stake here, it is important to look at the first round of what have been called the "Crypto Wars." In 1991, a 37-year-old software engineer named Phil Zimmermann wrote an encryption program called Pretty Good Privacy (PGP). PGP allowed anyone with a fairly modern computer and the ability to follow instructions to encrypt their e-mails in such a way that (1) the e-mail could be read only by the intended recipient, and (2) the e-mail could be digitally "signed" in such a way that the recipient could be sure it was sent by the sender and not by an imposter. He made it available for download on the Internet — which was fairly young, but quickly growing. He also published the source code of the program in old-fashioned book form and directly exported that book all over the world.
>
> Zimmermann — and those using his new encryption standard — quickly ran into a problem. The U.S. government classified as a munition any encryption program strong enough to actually work, and banned its export. Since the Internet made it possible for anyone in the world to get their hands on a copy of the program (and also made it *impossible* to prevent them from doing so), Zimmermann soon found himself under criminal investigation by the U.S. Customs Service for alleged violations of the Arms Export Control Act.

In the book *PGP & GPG: Email for the Practical Paranoid*, Michael W. Lucas explains that Zimmerman — by directly exporting the source code in book form — managed to turn what the U.S. government had treated as a *software* issue into a *free speech* issue.

As the case moved through the courts, Uncle Sam realized that the courts were likely to consider the dissemination of the written code behind the software as protected speech. Rather than risk a verdict — and a precedent — that might make the export of encryption software legally acceptable in almost any case, the federal government dropped the case and relaxed the standards for exporting software used for encryption. In 1996, President Clinton issued Executive Order 13026, essentially removing encryption from the munitions list.

But the Crypto Wars were far from over. While encryption has been the standard in business for more than 20 years (you use it without even seeing it when you transfer money or log in to certain websites), it has not been largely adopted by the average citizen for much of anything, including e-mail. Until recently.

The upswing in the use of powerful encryption to protect data-at-rest (data stored on a device such as a computer, mobile device, external hard drive, or USB stick) and data-in-motion (data being sent from

one device to another over mobile towers, the Internet, or another network) is the direct result of people reacting to what Edward Snowden revealed to the world in May 2013: U.S. government agencies routinely spy on everyone, including American citizens.

So, while Wray (and Comey before him) as well as other surveillance hawks cry and whine that encryption in the hands of private citizens is — in Wray's words — "an urgent public safety issue," the reality is that they hate it because it pulls the plug on huge portions of the surveillance machine.

As this writer said in that previous article:

> For all the ostensible reasons that the intelligence and law-enforcement communities give for wanting to limit the ability of ordinary citizens to encrypt their data and communications, the real reason is that those in power love power and want a monopoly on it. Government officials — who use encrypted systems for both data storage and communications — 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 while surveillance hawks love to repeat the mantra that encryption is "the tool of choice" for terrorists and other criminals, they pretend not to know that it is also the tool of choice for average citizens who want to protect their data from those who would spy on them — whether those who would spy on them work for a nosy corporation, a criminal organization, or an overreaching government agency.

Another favorite argument of the surveillance hawks is that encryption keeps law enforcement out of devices even when there is a warrant. This argument ignores the fact that warrants aren't what they used to be. This is illustrated by the case of a federal judge issuing a warrant for an intrusive search of a family's home based on no more probable cause than the facts that the husband and daughter shopped at a gardening store and the wife drank herbal tea.

Average citizens who use encryption to protect their data did not start the Crypto Wars; The surveillance state did. The use of powerful encryption is merely a reaction to the crimes of the state.

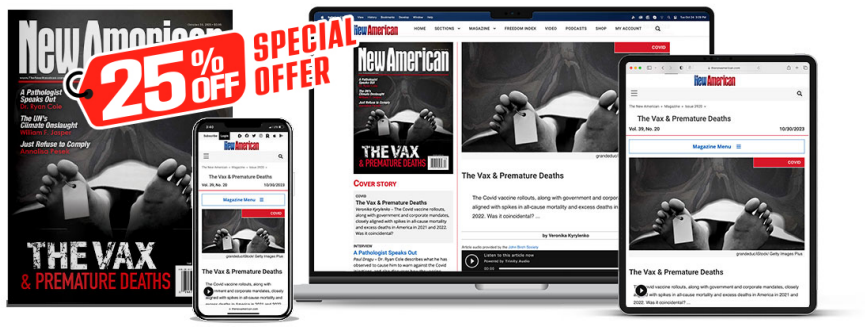
And — par for the course — the surveillance state is posturing once again to take away the one tool that truly levels the playing field. While no date has been set for the re-introduction of the Feinstein/Burr anti-encryption bill, freedom-loving Americans need to brace themselves for the next round of this ongoing battle. The next few weeks and months will likely show an increase in test-cases, claims, and statements by surveillance hawks about the evils of encryption as they attempt to psychologically seduce the people to accept yet another encroachment on their God-given rights.

Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture,
and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.