Written by **C. Mitchell Shaw** on November 3, 2016

Surveillance "Reforms" Allow NSA Greater Access Than Ever to Phone Data

Even as surveillance hawks such as FBI Director James Comey, CIA Director John Brennan, and joint chairs of the Senate Intelligence Committee Senators Richard Burr (R-N.C.) and Dianne Feinstein (D-Calif.) continue to claim that terrorists and other criminals are using technology to "go dark," so America needs an increased ability to perform civilian surveillance, the reality is that the hawks have more access to more data than ever before. And — as recent information confirms — many of the reasons for that increased surveillance ability are the supposed "reforms" that were sold to the American people as a way to curtail that surveillance.

Those in power — especially those who have built their careers in government by expanding the surveillance state — are not above using manipulation to increase their power by increasing that surveillance. The recent surveillance "reforms" — particularly the misnamed USA FREEDOM Act — prove that point perhaps better than anything else could. As this writer said last year:

> On Saturday, November 28, 2015, the NSA telephone surveillance program ended. Except that it didn't. The spying program — made famous when former NSA contractor Ed Snowden leaked a trove of secret documents to reporters — has simply continued under different authority. The "new and improved" surveillance may even be worse than before because the required warrants will be issued by a secret court.
>
> When the USA FREEDOM Act became law in June 2015, it was sold to the American people as a solution to the unwarranted surveillance Snowden had revealed. The law was set to take effect November 28, 2015 and "reform" that warrantless surveillance.
>
> The USA FREEDOM Act, like the USA PATRIOT Act of 2001, is a misnomer. The name is a not-very-subtle manipulation, designed to hide from the American people the real nature of the law. The architects of the USA PATRIOT Act used the word "patriot" to persuade Americans that the "patriotic" way to confront the specter of terrorism was to trade liberty for security. It took the one but never delivered the other. Likewise, in the USA FREEDOM Act, the use of the word "freedom" is designed to convince Americans that their freedom is being returned to them by "reforming" the surveillance state. In fact, no such reform is taking place.

And while the surveillance hawks claim that the "war on terror" (another misnomer) depends on mass surveillance, there is more at stake here than just security. Liberty — and the privacy that must necessarily accompany it — falls in direct proportion to the rise of the surveillance state. In the digital age, there is no line of demarcation between digital privacy and any other privacy, between digital

liberty and any other liberty. After all, if you have no choice about the data that is collected on you and who has access to it — including your phone calls, texts, e-mails, browsing history, calendar, and more — can you really be said to be free?

Mass surveillance, far from a solution, is itself a major part of the problem. Not only does it threaten privacy and liberty, it is counterproductive to the stated goal of finding and stopping terrorists. If one is trying to find a needle in a haystack, adding more hay is not the way to go about it; investigators should *narrow* their searches, not *expand* them.

The rise of the surveillance state in the 15 years since 9/11 has taken its toll on the American spirit. And yet, even while gathering data on more and more of the inhabitants of planet Earth at a greater and greater rate, the surveillance hawks still want more. Last December, Senator Burr wrote an op-ed piece for the *Wall Street Journal* that was laden with errors, half-truths, and outright lies. The article claimed that encryption — used by millions of ordinary people every day — is a tool of terrorism which "allows criminals and terrorists, as the law enforcement community says, to 'go dark' and plot with abandon." In an obvious attempt at giving lip service to the rights of individuals to protect their privacy and liberty, Burr wrote:

> Consumer information should be protected, and the development of stronger and more robust levels of encryption is necessary. 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.

But is Burr correct? Does modern technology allow " criminals and terrorists, as the law enforcement community says, to 'go dark' and plot with abandon"? Not even close. The myth of "going dark" is little more than a bogey-man, used to scare people into sacrificing their rights for the hollow promise of safety. As this writer said in the article quoted above:

> When the final USA FREEDOM Act vote was counted in the Senate on June 2, 2015, *The New American*'s Warren Mass reported that the act, which was sold to the American people as a way to "reform the authorities of the Federal Government" to (among other things) conduct electronic surveillance for "foreign intelligence, counterterrorism, and criminal purposes," was both misleading and unnecessary. If true reform had been the goal, a large part of that goal had already been accomplished. On May 31 the provisions of the USA PATRIOT Act, which had been interpreted to allow much of the surveillance exposed by Snowden, expired:
>
> > Many of those authorities — which the National Security Agency (NSA) has used to justify the collection of phone records — had been found in provisions of the USA PATRIOT Act that expired at midnight Sunday night. Therefore, Congress could have eliminated those surveillance powers merely by doing nothing.
> >
> > Despite promises made by its supporters, the USA Freedom Act doesn't end government snooping. It merely shifts the responsibility for collecting communications metadata from the NSA to companies such as AT&T, Sprint, and Verizon, which already keep customer records for as long as five years. The NSA or the FBI would simply need to obtain permission from the secret FISA Court to access that data — and the court nearly always grants it.

At the time *The New American* published that article and the previous article by Warren Mass (which is

quoted in that article), the mainstream media was singing the praises of the USA FREEDOM Act. Recently, our dire predictions of greater surveillance resulting from the very law which promised to curtail that surveillance have been shown true. And the same mainstream media is now confirming that. ABC News recently reported that the "NSA can access more phone data than ever," and said:

> One of the reforms designed to rein in the surveillance authorities of the National Security Agency has perhaps inadvertently solved a technical problem for the spy outfit and granted it potential access to much more data than before, a former top official told ABC News.

The article cites Chris Inglis, who served as the NSA's deputy director until January 2014. Inglis told ABC News that before the USA FREEDOM Act, the NSA had incomplete access to phone records because the agency had to pull the data from several different networks, reformat much of it and compile it "according to existing privacy policies." Since the USA FREEDOM Act shifts much of that responsibility to the carriers — who are required under the law to maintain that data and make it available to the NSA — Inglis told ABC News that all the technical and compliance issues are now "somebody else's problem." The report also says:

> The USA Freedom Act ended the NSA's bulk collection of metadata but charged the telecommunications companies with keeping the data on hand. The NSA and other U.S. government agencies now must request information about specific phone numbers or other identifying elements from the telecommunications companies after going through the Foreign Intelligence Surveillance Act (FISA) court and arguing that there is a "reasonable, articulable suspicion" that the number is associated with international terrorism.
>
> As a result, the NSA no longer has to worry about keeping up its own database and, according to Inglis, the percentage of available records has shot up from 30 percent to virtually 100. Rather than one internal, incomplete database, the NSA can now query any of several complete ones.
>
> The new system "guarantees that the NSA can have access to all of it," Inglis said.

Just let that marinate for a while: "The NSA can have access to all of it."

So the American people were sold a bill of goods. One thing was promised and another delivered. If the mainstream media had reported on this as *The New American* did, perhaps America could have been spared this increased surveillance. As it is, the mainstream media is catching on too little, too late.

As the surveillance hawks on the one side and privacy advocates on the other side continue to wage the battle for digital privacy, it is likely that some type of "compromise" will be offered to "solve the problem" of encryption.

Don't fall for it.