New American

Written by **Mitch** on April 4, 2016

Published in the April 4, 2016 issue of the New American magazine. Vol. 32, No. 07

Correction, Please!

Surveillance in Session

Item: *On November 16, 2015, CNNMoney ran an article online entitled "Terrorists hide plans by 'going dark'" that said:*

Violent extremists meet in the open on Facebook or Twitter. Then they take the conversation private, using technology called encryption to encode their messages.

It's called "going dark." And it's the most alarming concern for police worldwide right now. They worry they can't prevent the next terrorist attack.

In recent weeks, FBI director James Comey has repeatedly told Congress that surveillance is getting harder.

"Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse," Comey said during a speech at a Washington, D.C., think tank last month.

Item: *An article on Foreign Policy's website dated November 16, 2015 asserted that passage of the USA Freedom Act and other "surveillance reforms" have weakened national security by making it harder for law-enforcement agencies — at all levels — to do their jobs. The article quotes CIA Director John Brennan as saying that "policy" and "legal" actions taken in the wake of the Snowden revelations "make our ability collectively, internationally, to find these terrorists much more challenging."*

After leading the reader to the conclusion that the attacks in Paris were the result of a lack of effective surveillance, the article says:

Brennan said the attacks should serve as a "wake-up call" for those misrepresenting what intelligence services do to protect innocent civilians. He cited "a number of unauthorized disclosures, and a lot of handwringing over the government's role in the effort to try to uncover these terrorists."

Correction: The oft-repeated claim that terrorists are "going dark" has become almost a mantra for the surveillance hawks. And it is one of the Big Lies that — they seem to hope — if repeated often enough and with just the right amount of emotional appeal, will stick in the American consciousness and be taken for granted as truth. But when examined in the light of the truth, the issue of "going dark" simply fails the test.

On February 1, 2016, *The Intercept* published an online article about a newly released study entitled *Don't Panic*. The study, published by Harvard's Berkman Center for Internet and Society, says that "unbreakable encryption — which prevents easy, conventional surveillance of digital communications — isn't a big problem for law enforcement," and that America is not likely "headed to a future in which our ability to effectively surveil criminals and bad actors is impossible" because of the encrypted devices and communication apps used by millions of Americans.

The study was the result of what *The Intercept* called "a diverse group of technologists, cryptographers, and former and current government officials — from think tanks, universities, the NSA, FBI, ODNI, and others" who held private meetings over the course of a year to discuss the issues surrounding encryption and surveillance before publishing their findings.

And what did those experts conclude? That end-to-end encryption "doesn't pose an existential threat to

law enforcement investigations." How can that be? The reasons the authors (which included government employees who were unable to sign the report "because of their employment") gave were:

• Many companies do not offer end-to-end encryption as part of the services they make available because it would hinder their ability to harvest the data of their users. The bottom line is that doing so would affect their bottom line.

• End-to-end encryption is not "user friendly." The difficulty of having to sign into a service or app with a password that is sufficiently long and random to protect the encryption key is more trouble than many are willing to go to. As a result, while many are encrypting *some things*, very few are encrypting *everything*.

• Many online backup and syncing services are either not encrypted at all or are done so in such a way that the service provider holds the keys and would easily be able to (and therefore required to) cooperate with a government agency that issued a warrant. For instance, Apple's iCloud — which is turned on by default on most devices, including the iPhone — is encrypted, but — unlike the iPhone itself — the password *is* known to Apple. The company says this is necessary because if a user forgets his or her password, Apple can still access the data and restore the account for the user.

• Even when encryption is used to protect the *contents* of a communication, the *metadata* (data about the communication, including the sender, the recipient, the date and time of the communication, the length of the call or size of the text or e-mail, etc.) *is not* encrypted. And while the USA Freedom Act promised to end the collection of that metadata, you will soon see that it did no such thing.

• As the Internet of Things (Internet-connected devices such as Smart Watches, Smart TVs, Internet-connected refrigerators, washing machines, security systems, etc.) has grown and continues to grow, there is an ever-widening pool of devices providing information about more and more people.

• Even if a person encrypted all of their communications, they would still be open to the surveillance being conducted on the people around them who are not encrypting all of their communications. Listening to "person A's" conversation with "person B" would be a simple matter of using the microphone in the phone of "person C" who is standing close by.

As The New American has reported previously, with as many tools as the surveillance hawks have at their disposal — including satellite photography, street cameras, undercover agents who infiltrate terrorist cells and criminal organizations, spy planes and drones, and a plethora of other tools — the idea of terrorists and other criminals "going dark" is ridiculous.

The other Big Lie projected onto the American consciousness is that the surveillance "reforms" that have been enacted are tying the hands of those who would protect America. In truth, there have been no real reforms. The USA Freedom Act, which is touted as the biggest and best of the "reforms" so far, does not reform anything; it simply reorganizes it. The same surveillance that took place before is taking place now. It just happens under a different authority. As The New American reported online when the USA Freedom Act began to take effect:

On Saturday, November 28, 2015, the NSA telephone surveillance program ended. Except that it didn't. The spying program … 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.

Written by **Mitch** on April 4, 2016

Published in the April 4, 2016 issue of the New American magazine. Vol. 32, No. 07

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.

When the final USA Freedom Act vote was counted in the Senate on June 2, 2015, we reported that 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.

So rather than limiting government powers — which had already been done by the sun setting on parts of the USA PATRIOT Act — what the USA Freedom Act really does is make the mobile telecom companies arms of the federal government in keeping the surveillance state running along smoothly.

Perhaps one of the best examples of the surveillance hawks promising reform while shifting programs around is found in documents that were released as a result of a Freedom of Information Act (FOIA) lawsuit in November 2015 — just before the so-called USA Freedom Act was to become active. As the *New York Times* reported:

While that particular secret program stopped, newly disclosed documents show that the N.S.A. had found a way to create a functional equivalent. The shift has permitted the agency to continue analyzing social links revealed by Americans' email patterns, but without collecting the data in bulk from American telecommunications companies — and with less oversight by the Foreign Intelligence Surveillance Court.

So the NSA was caught playing a shell game with the American people. It admitted the existence of the first program only when it was pointless to deny it because of the Snowden documents, and then basically said, "But don't worry. We're not even using that program now." Deliberately withheld was the fact that the program was replaced by something worse, with even less oversight.

As we reported then:

The documents the *New York Times* received as a result of the FOIA lawsuit included a report which was highly redacted. The portions not redacted show that the NSA found "two other legal ways to get" the data it wanted about Americans' e-mails.

As the *Times* reported, "One was the collection of bulk data that had been gathered in other countries, where the N.S.A.'s activities are largely not subject to regulation by the Foreign Intelligence Surveillance Act and oversight by the intelligence court."

In other words, the NSA simply obtained the data it wanted from intelligence agencies in the other Five Eyes nations. It has already been widely reported that GCHQ — the UK's equivalent to the NSA — has used the NSA to collect data on U.K. citizens which it would have been barred by law from collecting itself. It appears that one hand washes the other.

The *Times* report goes on to explain, "The other replacement source for the data was collection under the FISA Amendments Act of 2008, which permits warrantless surveillance on domestic soil that targets specific noncitizens abroad, including their new or stored emails to or from Americans."

And now, a recent report by The *Guardian* shows that the FBI "has quietly revised its privacy rules for searching data involving Americans' international communications that was collected by the National Security Agency." Internet data the government demands from such entities as Yahoo!, Google, and Microsoft is fair game for random searches:

FBI officials can search through the data, using Americans' identifying information, for what PCLOB [Privacy and Civil Liberties Oversight Board] called "routine" queries unrelated to national security….

As of 2014, the FBI was not even required to make note of when it searched the metadata, which includes the "to" or "from" lines of an email. Nor does it record how many of its data searches involve Americans' identifying details.

So, while Comey, Brennan, and the other surveillance hawks claim that terrorists are "going dark" and that "reforms" of the surveillance laws tie their hands, the reality is that they have at least as many surveillance tools and opportunities as ever before — if not more. It appears that — as always — those who have built and are maintaining the surveillance state still think too much is never enough.

Written by **Mitch** on April 4, 2016
Published in the April 4, 2016 issue of the New American magazine. Vol. 32, No. 07