Written by **C. Mitchell Shaw** on December 30, 2015

N.C. Senator Calls for "Backdoors" in Encryption

In the digital age, people do nearly everything on their computers and mobile devices. They talk, text, e-mail, and use video chat. They manage their businesses, transact their banking, shop, and pay their bills. They manage their social media accounts and search for needed — and sometimes frivolous — information. By using the various types of encryption available, they can do all these things with privacy and security.

Encryption — a method of scrambling communications and data so that only the sender and the intended recipient can see them — is as important to privacy and security as sealed envelopes and locked doors. And it's even more effective. Public-key encryption, such as the popular GPG, has been proven unbreakable, making communications and data inaccessible to both criminals and law-enforcement agencies. Since the recent terrorist attacks in Texas, France, and California, there have been increased calls for restrictions on the private use of encryption by the very people who need it most: private citizens who have been the victims of spying by crimials, corporations, and overreaching government agencies.

Private citizens did not start the Crypto Wars, but since technology is — thankfully — an equal-opportunity tool, they are better equipped to fight back. The increased use of better and better encryption by individuals is the result of broad-net surveillance on the part of governments and corporations. 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.

Last week, Senator Richard Burr (shown, R-N.C.), chairman of the Select Committee on Intelligence, wrote an error-laden piece for the *Wall Street Journal* in which he claimed that "Encrypted devices block law enforcement from collecting evidence. Period." As if the only item in the law-enforcement tool box is ubiquitous surveillance, and without it no evidence can be collected.

In his article, Burr shows both his preference of surveillance over privacy and his ignorance of how encryption works. He admits that encryption is necessary, but appears to think it should apply only to "consumer information." Even *then*, he sees it as a danger that must be regulated because, he claims, it enables "murderers, pedophiles, drug dealers and, increasingly, terrorists." He states:

> 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.

Burr's observation that "the protection that encryption provides law-abiding citizens is also available to criminals and terrorists" is deliberately misleading. Yes, "criminals and terrorists" use encrypted devices and technologies to plan and carry out their fell deeds. They also use cars, buses, planes, the U.S. mail, houses, apartments, doors with locks, and a million other things that everyone else uses. None of that keeps law enforcement from conducting investigations. Neither does encryption.

The problem is that law enforcement at almost every level has become addicted to the easiest path. Many in law enforcement prefer to conduct investigations using surveillance techniques instead of using more time-consuming methods. They don't seem concerned that their surveillance does more to injure the privacy and liberty of the law-abiding citizens than it does to build solid cases against criminals and terrorists. The evidence for that is that in many cases, prosecutors have dropped charges or agreed to forgo having evidence admitted if it meant revealing the (likely illegal) use of blanket surveillance.

As for Burr's assertion that encryption allows criminals and terrorists to "plot with abandon," this writer wishes that Burr were as well-schooled on the use of encryption as he is on the use of pulp-fiction phrases designed to scare people into giving up their rights.

The truth is that criminals make mistakes just like everyone else, and skilled investigators are trained to find and use those mistakes in order to solve cases. Encryption is a tool. It is not a silver bullet. Furthermore, this is just one more example of a surveillance hawk making the same tired old argument that criminals and terrorists are getting away with their crimes because law enforcement's hands are tied by encryption. And just like all the other times, Senator Burr fails to credibly cite even *one case* to substantiate his fraudulent claim.

Instead, he quotes from a report released last month by Manhattan District Attorney Cyrus Vance Jr., a well-known critic of encrypted devices. One part of the report he quotes says:

> Congress should enact a statute that requires any designer of an operating system for a smartphone or tablet manufactured, leased, or sold in the U.S. to ensure that data on its devices is accessible pursuant to a search warrant. Such a law would be well within Congress's Commerce Clause powers, and does not require costly or difficult technological innovations.

In a clear case of the blinded-by-power leading the blinded-by-power, Burr accepts Vance's idea that some type of technology could be developed that could "ensure" that encrypted devices can be accessed by law enforcement. There is a name for that type of technology: backdoors. And the technology community is in nearly unanimous agreement that it is impossible to make it work without making encryption worthless. As this writer pointed out in a previous article for *The New American*:

> The problem with "back doors" is that that is just not the way cryptography works. The most powerful form of cryptography is "public key encryption," such as the popular GPG encryption used by millions, including Snowden. The way it works is that each user has a public key (which they share with others) and a private key (which they keep secret). The communication is encrypted using the sender's private key and the recipient's public key. The recipient then decrypts the message using his private key. Since the only keys that can unlock the communication are private, the communication is private. Providing "another key" that only government can use is a farce. Any such key would inevitably be exploited by hackers and foreign governments. Experts in

> cryptography agree: There is simply no way for it to be "kept safe."

The same principle applies to full-disk encryption. When a device — whether it be a smartphone, a computer, or any other device — is encrypted, the owner has the only key to decrypt it. If another key exists, the encrypted device might as well not be encrypted. Keys work for anyone using them. Since there is no way to make sure only "good guys" could get that key, it should never be created.

As Apple CEO Tim Cook told NPR last month, "National security always matters, obviously. But the reality is that if you have an open door in your software for the good guys, the bad guys get in there, too. Any backdoor means a backdoor for bad guys as well as good guys. So, a backdoor is a non-starter," adding, "It means we're all not safe." In explaining why Apple made the decision to build full-disk encryption into the iOS 8 and up, Cook said, "Some of our most personal data is on the phone: our financial data, our health information, our conversations with our friends and family and co-workers. And so instead of us taking that data into Apple, we've kept [that] data on the phone and it's encrypted by you. You control it."

Apple is not alone on this, either. *The Guardian* reported last month that more than 60 technology companies — including Apple, Google, Twitter, Samsung, and other major players — "have joined together to reject calls for weakening encryption saying it would be 'exploited by the bad guys.'" Dean Garfield, CEO of the Information Technology Industry Council, asserted, "Weakening security with the aim of advancing security simply does not make sense," adding, "Weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys, which would almost certainly cause serious physical and financial harm across our society and our economy."

Along with computer technology experts saying there is no way to do what the surveillance hawks want, there are also experts in intelligence saying the same thing. Back in July, the *Washington Post* published an op-ed piece co-written by three men highly qualified to address this subject. Mike McDonnell (former director of NSA), Michael Chertoff (former secretary of DHS), and William Lynn (former deputy secretary of defense) wrote:

> We recognize the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption. We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.

So, "ubiquitous encryption," which has been the bane of surveillance hawks such as Senator Burr, is "the greater public good" according to these three experts on the subject. Why do they see it so differently from Burr? One reason they give is that, in essence, the genie is already out of the bottle; there is no world without encrypted data and communications anymore. And there is no way to regulate that encryption. If, as Burr would have it, Congress tries to "update the law" and require companies that create encryption technologies to install backdoors, criminals and terrorists would do what they largely already do: use their own home-brewed encryption. As McDonnell, Chertoff, and Lynn put it:

> The smart bad guys will find ways and technologies to avoid access, and we can be sure that the "dark Web" marketplace will offer myriad such capabilities. This could lead to a perverse outcome in which law-abiding organizations and individuals lack protected communications but malicious

actors have them.

So, with experts in both technology and intelligence saying Burr is dead wrong on this issue, he will have to be content with the company of his vice-chairwoman, Senator Dianne Feinstein, who told MSNBC after the Paris attacks, "Silicon Valley has to take a look at their products. Because if you create a product that allows evil monsters to communicate in this way, to behead children, to strike innocents, whether it's at a game in a stadium, in a small restaurant in Paris, take down an airliner — that's a big problem."

What Burr, Feinstein, Vance, and the other surveillance hawks fail to recognize is that the companies of Silicon Valley *have* taken "a look at their products" and have answered the public demand for greater and easier encryption. That's why they build it into their products. Ubiquitous encryption is the free market's answer to ubiquitous surveillance.

As more Americans finally reach their tipping points with the heavy-handed, ubiquitous surveillance of an overreaching government, they are turning to encryption to protect themselves and their data. And that is a good thing.

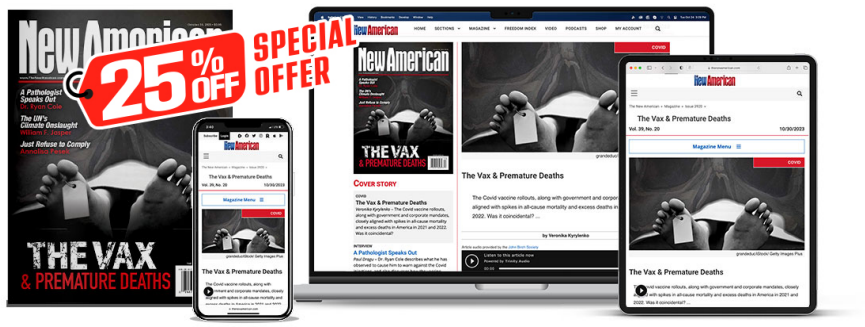
Photo: AP Images

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.



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.

Subscribe