Written by **Joe Wolverton, II, J.D.** on July 11, 2012

NSA Chief Says Spy Agency Does Not Read Private Email

On Monday, the head of the National Security Agency (NSA) urged Congress to act swiftly to establish workable guidelines and jurisdictional boundaries in the war against destructive computer attacks that might be made against the online infrastructure of the United States.

General Keith Alexander of the U.S. Army delivered an address at the American Enterprise Institute arguing that the need for such congressional action is urgent, and that something has to be done before the nation is hit with a disabling cyberattack. He insisted that the likelihood of such an assault was increasing. "The conflict is growing, the probability for crisis is mounting," Alexander said. "While we have the time, we should think about and enact those things that we need to ensure our security in this area. Do it now, before a crisis," he continued.

The steps outlined in Alexander's proposal were already approved by the House of Representatives in a bill passed in April. The legislation would have given a green light to the swapping of critical data between the government and corporate concerns.

Thankfully, there are those who have decried such schemes as leading to violations of the constitutional right of Americans to be free from unwarranted and unreasonable searches and seizures. Critics argue that, although it isn't promoted by those pushing for this type of legislation, the effect of passage would be granting the National Security Agency the power to monitor, collect, and catalog all the Internet communications of citizens who have not been accused or suspected of committing a crime.

The fear is well-founded in light of the story *The New American* covered recently highlighting the domestic spy service's intent to keep mum about just how much and what kind of personal electronic data it has already collected and collated. Not only does the NSA refuse to provide such information, it says that it cannot be forced to.

In July of 2011, and again in May 2012, Senators Mark Udall (D-Colo.) and Ron Wyden (D-Ore.) wrote a letter to James R. Clapper, Jr., the director of national intelligence, asking him a series of questions regarding the activities of the NSA and other intelligence agencies regarding domestic surveillance.

In one of the questions, Senators Udall and Wyden asked Clapper if "any apparently law-abiding Americans had their communications collected by the government pursuant to the FISA [Foreign Intelligence Surveillance Act] Amendments Act" and if so, how many Americans were affected by this surveillance.

Regarding the Wyden-Udall inquiry, in a letter dated June 15, 2012, I. Charles McCullough III informed

the senators that calculating the number of Americans who've had their electronic communications "collected or reviewed" by the NSA was "beyond the capacity of his office" and dedicating sufficient additional resources would likely impede the NSA's mission.

In other words, the NSA is too busy illegally recording our private e-mails, texts, Facebook posts, and phone calls to figure out how many of us are already caught in their net. And, furthermore, there is nothing Congress can do about it.

Naturally, Senators Udall and Wyden didn't take kindly to Inspector General McCullough's brush off. In a response to the response, the senators told McCullough that they just wanted a "ballpark estimate" of the number of American citizens who have been monitored under the authority of the FISA. In an additional statement released by Senator Wyden, he expressed concern that the figure is likely very high:

> I am concerned, of course, that if no one has even estimated how many Americans have had their communications collected under the FISA Amendments Act, then it is possible that this number could be quite large. Since all of the communications collected by the government under section 702 are collected without individual warrants, I believe that there should be clear rules prohibiting the government from searching through these communications in an effort to find the phone calls or emails of a particular American, unless the government has obtained a warrant or emergency authorization permitting surveillance of that American.

Given the intelligence community's disdain for not only the Constitution but for congressional oversight, it is unlikely that the information requested by Senators Udall and Wyden will ever be forthcoming.

In his speech at the American Enterprise Institute, General Alexander said that there was nothing mutually exclusive about personal privacy and national security. "The reality is we can do protection of civil liberties and privacy and cybersecurity as a nation," he said.

Without a hint of irony, Alexander argued that individual liberty can only really be kept safe if the government is given the power to scan and surveil the entirety of Internet traffic so as to prevent it from being compromised by cyberattacks. Fear not, though, the general promises are that such surveillance will not include your e-mail. "It doesn't require the government to read their mail or your mail to do that. It requires them, the Internet service provider or that company, to tell us that that type of event is going on at this time. And it has to be at network speed if you're going to stop it," Alexander said.

Alexander took time to reassure Americans that the new mammoth NSA facility being constructed in Utah would not house computers that would read and store the personal e-mails exchanged by citizens. He went on to call allegations to the contrary "baloney."

The take-away from Alexander's remarks regarding the actual interception of private communication is that the government won't do the dirty work; it will outsource the contravention of the Constitution to the Internet service providers and cellphone companies.

As usual, those advocating the proliferation of the snooping arsenal available to the agencies of the surveillance state claim that something must be done immediately or our alleged vulnerability will be exploited by cyber-criminals. If we wait too long, the general warns, then the government will overreach and the American people wouldn't want that. "When something bad happens, we're going to jump way over here where we don't want to be," he said. "So while we have the time, the patience and the understanding, let's get this right. Let's do it now."

An essential question that has yet to be answered by Alexander or those of his predisposition to disregard the Fourth Amendment is how they justify the decrying of the as-yet-imaginary attacks on our own Internet infrastructure, while we concurrently carry out actual assaults on the computer networks of other nations.

Recently, stories have been leaked detailing the U.S. government's creation and implementation of two such cyberattacks.

"Flame" was the name of a computer virus reportedly developed and launched by the United States in order to glean critical data from computers in several Middle Eastern countries.

According to a story published in the *Washington Post*, the United States and Israel launched a joint venture to develop the Flame virus. Once launched into cyberspace, the code reportedly collected online intelligence data that was then used to create a similar bit of malware that would cripple Iran's nuclear capabilities. Officials cited in the *Post* article revealed that the effort was a collaboration of the National Security Agency (NSA), the CIA, and the Israeli military.

One product of that Israeli-American secret enterprise was the Stuxnet virus. Stuxnet was the virus allegedly deployed by the United States to decelerate Iran's progress toward the development of a nuclear weapon.

Apparently, Flame and Stuxnet were just the beginning of a more sophisticated and sustained American cyberassault against the Iranian nuclear infrastructure. As one source quoted by the *Washington Post* reports: "This is about preparing the battlefield for another type of covert action," said one former high-ranking U.S. intelligence official, who added that Flame and Stuxnet were elements of a broader assault that continues today. "Cyber-collection against the Iranian program is way further down the road than this."

In light of these revelations, it becomes important to ask what will the United States do if a nation decides unilaterally that its own national security is threatened by America's possession of so many nuclear weapons and decides to dismantle the computer systems that control those missiles? On what moral ground will the United States stand in defense of such attacks?

And how will such defenses be buttressed by granting the federal government the power to peruse, prevent, and punish the personal online activity of citizens of the United States who have done nothing to warrant such statist intrusions?

Photo of NSA headquarters at Fort Meade, Maryland