



Written by [Joe Wolverton, II, J.D.](#) on January 17, 2014

## NSA Collects “Untargeted” Texts, Controls “Unconnected” Computers

Every day, people wake up to find that the walls of the surveillance state seem taller than they were the day before. In truth, the walls have been this imposing for years, but the blueprints leaked by Edward Snowden reveal the dizzying height of the structure being built while we pay attention to other things.



On January 16, the British newspaper [The Guardian published a new page of the blueprint](#), and the information printed on it is disturbing.

According to top-secret documents, the National Security Agency has collected almost 200 million text messages a day from across the globe, using them to extract data including a person’s location, contact networks, and credit card details.

Investigators from *The Guardian* and Britain’s Channel 4 News discovered these details of the NSA’s dragnet surveillance practices during a search of documents provided by Edward Snowden.

Perhaps the most offensive word used in *The Guardian* report is “untargeted.” Untargeted is another way of saying unconstitutional, which is a word probably not heard very often at the NSA.

When the NSA casts its massive surveillance net into the sea of global electronic communication without having first identified a target and without first having established probable cause to believe that target is breaking the law, then the NSA violates the fundamental civil liberties of everyone caught in its snare.

The Fourth Amendment to the Constitution is very clear:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Regardless of their arguments — [and the opinions of secret courts that rubber stamp their petitions](#) — the NSA may not legally collect and collate the text messages of millions of “untargeted” persons without at the same time violating the Fourth Amendment.

This is the very essence of tyranny and claims of “national security” remove neither the sting nor the seriousness of what is happening in our once-free Republic of laws.

So, why would the NSA want this immense trove of personal data? Reading the Snowden cache, *The Guardian* reports:

The NSA has made extensive use of its vast text message database to extract information on people’s travel plans, contact books, financial transactions and more — including of individuals



Written by [Joe Wolverton, II, J.D.](#) on January 17, 2014

---

under no suspicion of illegal activity.

There it is again: “individuals under no suspicion of illegal activity.” Every time readers see that phrase or a similar one, they should understand that the program being described is an assault on their basic rights and a substantial step toward shackling every one of them with invisible electronic restraints.

Not only is the NSA brazen enough to conduct such offensive operations, but they give them equally audacious titles. The text message collection program is called “Prefer” and is set out in a memo titled, “SMS Text Messages: A Goldmine to Exploit.”

A goldmine. The personal communications of millions of innocent men and women is considered nothing more than a motherlode to the federal agents who understand the inestimable worth of their haul.

Millions of potentially embarrassing private messages make it much much easier for a government bent on consolidating absolute control to coerce citizens to cooperate in constructing the walls of their own prison.

So, upon hearing that the NSA has eyes on everything done in the virtual world, many respond that the best way to keep out of sight is to stay off the Internet. That would seem like sound advice, if it weren't for Quantum.

According to [a story published January 14 in the New York Times](#), the NSA has installed software on almost 100,000 computers that gives the agency access to those computers, even when not connected to a wider network.

Typically, the NSA will upload the malicious software through the target computer's Internet connection, but Quantum is a “secret technology” that allows the snoops to “enter and alter data” on computers that aren't connected to a network. The *Times* article explains:

The technology, which the agency has used since at least 2008, relies on a covert channel of radio waves that can be transmitted from tiny circuit boards and USB cards inserted surreptitiously into the computers. In some cases, they are sent to a briefcase-size relay station that intelligence agencies can set up miles away from the target.

So much for the safe harbor of staying off the Internet. For its part, the NSA is very proud of the program. It removes the barrier of network connection that once kept them from watching everybody. Using the the radio frequency secretly installed in the computer, the NSA can upload and download anything it wants to and from the target device.

If readers are interested in whether the hardware they own is known to have been hacked by the NSA, the German magazine *Der Spiegel* has published the [NSA's list of “hardware products that can secretly transmit and receive digital signals from computers.”](#)

Ironically, the technology enabling the offline surveillance is actually less sophisticated than many of the other tools used by the NSA to keep everyone under watch. The *Times* article describes one of the products the NSA deploys to conduct surveillance on computers not connected to a network.

One, called Cottonmouth I, looks like a normal USB plug but has a tiny transceiver buried in it. According to the catalog, it transmits information swept from the computer “through a covert channel” that allows “data infiltration and exfiltration.” Another variant of the technology involves tiny circuit boards that can be inserted in a laptop computer — either in the field or when they are shipped from manufacturers — so that the computer is broadcasting to the N.S.A. even while the computer's user enjoys the false confidence that being walled off from the Internet constitutes real



Written by [Joe Wolverton, II, J.D.](#) on January 17, 2014

---

protection.

Why should we care that the NSA is reading our texts, tapping our computers, and surreptitiously sending and receiving data from computers not connected to the Internet? If we haven't done anything wrong, we have nothing to fear. Right?

Wrong.

All men are endowed by their Creator with the right to be free from unwarranted searches and seizures. When the government takes away these rights, then there is no liberty, regardless of the pretexts of the powerful.

While it's true that most Americans have "done nothing wrong" criminally speaking, it is equally true that most of us have done many embarrassing things that we would prefer not to have put in a file for future use by political enemies — inside or outside the government. What are these possible peccadilloes? Think bad credit, poor scholastic performance, Web surfing habits, sensitive medical diagnoses, etc.

Besides, the fact is that there is no evidence that the government's constant surveillance and deprivation of liberty have made the "homeland" any safer. What, then, is the true purpose of the surveillance?

It isn't security. Demanding freedom in exchange for safety is the economy of tyrants. When the federal government — or any government — robs citizens of their basic civil rights, then that government has become despotic by definition.

The question remains: Will Americans simply sit and watch as the walls get higher and the electronic chains get tighter?

*Joe A. Wolverton, II, J.D. is a correspondent for The New American and travels frequently nationwide speaking on topics of nullification, the NDAA, the Second Amendment, and the surveillance state. He is the co-founder of Liberty Rising, an educational endeavor aimed at promoting and preserving the Constitution. Follow him on Twitter @TNAJoeWolverton and he can be reached at [jwolverton@thenewamerican.com](mailto:jwolverton@thenewamerican.com).*



## 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.