GlobalResearch
Center for Research on Globalization

Whistleblower: “The NSA Is Still Collecting the Full Content Of U.S. Domestic E-Mail, Without a Warrant …”

"The NSA Cannot Identify Future Terrorism Because 99.9999% of What It Collects and Analyzes Is Foreseeably Irrelevant”

By Bill Binney and Washington's Blog
Global Research, July 09, 2017
Washington's Blog 7 July 2017

Region: USA
Theme: Intelligence, Law and Justice, Police State & Civil Rights, Terrorism

The man who designed the NSA’s electronic intelligence gathering system (Bill Binney) sent us an affidavit which he signed on the Fourth of July explaining that the NSA is still spying on normal, every day Americans … and not focused on stopping terror attacks (I’ve added links to provide some background):

> The attacks on September 11, 2001 completely changed how the NSA conducted surveillance …. the individual liberties preserved in the U.S. Constitution were no longer a consideration. In October 2001, the NSA began to implement a group of intelligence activities now known as the “President’s Surveillance Program.”
>
> The President’s Surveillance Program involved the collection of the full content of domestic e-mail traffic without any of the privacy protections built into [the program that Binney had designed]. This was done under the authorization of Executive Order 12333. This meant that the nation’s e-mail could be read by NSA staff members without the approval of any court or judge.
>
> ***
>
> The NSA is still collecting the full content of U.S. domestic e-mail, without a warrant. We know this because of the highly-detailed information contained in the documents leaked by former NSA-contractor, Edward Snowden. I have personally reviewed many of these documents.
>
> I can authenticate these documents because they relate to programs that I created and supervised during my years at the NSA.
>
> [U.S. government officials] have also admitted the authenticity of these documents.
>
> ***
>
> The documents provided by Mr. Snowden are the type of data that experts in the intelligence community would typically and reasonably rely upon to form an opinion as to the conduct of the intelligence community.
>
> [The Snowden documents prove that the NSA is still spying on most Americans.]

When Mr. Snowden said that he could read the e-mail of a federal judge if he had that judge's email address, he was not exaggerating.

***

The NSA is creating a program that shows the real-time location of all cell phones, tablets and computers in the world, at any time. To have a state-actor engaging in this sort of behavior, without any court supervision, is troubling.

***

In their public statements, [government officials] claim that collection of information is limited, and is being done pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). FBI Director James Comey recently described Section 702 of FISA as the "crown jewel" of the intelligence community.

Defendants, however, are not being candid with the Court. Collection is actually being done pursuant to Executive Order 12333(2)(3)(c), which — to my knowledge — has never been subject to judicial review. This order allows the intelligence community to collect "incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws." Any lawyer can appreciate the scope of this broad language. [Background.]

***

Susan Rice (Source: U.S. State Dept. / Wikimedia Commons)

According to media reports, President Obama's former National Security Advisor, Susan Rice, requested email and phone records on President Trump and various members of his political campaign during and after the 2016 election.

According to these reports, the National Security Council ("NSC") has computer logs showing when Rice requested and viewed such records. The requests were made from July 2016 through January 2017, and included President Trump and various members of his campaign staff According to an internal NSC report, the accessed information contained "valuable political information on the Trump transition." Rice's requests into Trump-related conversations increased following the presidential election last November. None of the requests were reviewed by any independent court.

***

We also know that certain NSA staffers have used their access to e-mail and phone calls to conduct surveillance on current and former significant others. The NSA has referred to this sort of action as "LOVEINT," a phrase taken from other internal-NSA terms of art, such as "SIGINT" for signals intelligence.

***

Bulk collection makes it impossible for the NSA to actually do its job.

For example, consider the Pinwale program, discussed above, in which the NSA searches the collected data based on certain pre-defined keywords, known as

the “dictionary.” The results from the dictionary search are known as the “daily pull.”

Eighty percent of the NSA’s resources go towards review of the daily pull. The problem is that the daily pull is enormous. It is simply not possible for one analyst to review all questionable communications made by millions of people generating e-mail, text messages, web search queries, and visits to websites. Every person making a joke about a gun, bomb or a terrorist incident theoretically gets reviewed by a live person. This is not possible. When I was at the NSA, each analyst was theoretically required to review 40,000 to 50,000 questionable records each day. The analyst gets overwhelmed, and the actual known targets — from the metadata analysis — get ignored.

This is clear from some of the internal NSA memos released by Edward Snowden and published by the Intercept. In these memos, NSA analysts say:

“NSA is gathering too much data. . . . It’s making it impossible to focus.”

“Analysis Paralysis.”

“Data Is Not Intelligence.”
“Overcome by Overload.”

Bulk collection is making it difficult for the NSA to find the real threats. [Indeed.] The net effect from the current approach is that people die first. The NSA has missed repeated terrorist incidents over the last few years, despite its mass monitoring efforts. The NSA cannot identify future terrorism because 99.9999% of what it collects and analyzes is foreseeably irrelevant. This is swamping the intelligence community, while creating the moral hazards and risks to the republic ….

After a terrorist incident occurs, only then do analysts and law enforcement go into their vast data, and focus on the perpetrators of the crime. This is exactly the reverse of what they should be doing. If the NSA wants to predict intentions and capabilities prior to the crime, then it must focus on known subversive relationships, giving decision-makers time to react and influence events.

There is a second reason why data mining bulk collected data is a waste of time and resources: the professional terrorists know that we are looking at their e-mail and telephonic communications. As a result, they use code words that are not in the dictionary, and will not come up in the daily pull.

***

Thus, collecting mass amounts of data and searching it to find the proverbial needle in a haystack doesn’t work. It is fishing in the empty ocean, where the fish are scientifically and foreseeably not present.

Binney explains what we should do instead:

The truth is that there has always been a safe, alternate path to take. That’s a focused, professional, disciplined selection of data off the fiber lines.

***

I serve as a consultant to many foreign governments on the issues described in this affidavit. As such, I have testified before the German Parliament, the

> British House of Lords, and the EU Libe Committee on Civil Liberties on these issues. I also consult regularly with members of the European Union on intelligence issues.
>
> ***
>
> it is my understanding that the European Union intends to adopt legislation requiring its intelligence community to get out of the business of bulk collection, and implement smart selection.
>
> ***
>
> Smart selection is not enough. Governments, courts and the public need to have an absolute means of verifying what intelligence agencies are doing. This should be done within government by having a cleared technical team responsible to the whole of government and the courts with the authority and clearances to go into any intelligence agency and look directly into databases and tools in use. This would insure that government as a whole could get to the bottom line truth of what the intelligence agencies were really doing
>
> I would also suggest that agencies be required to implement software that audits their analytic processes to insure compliance with law and to automatically detect and report any violations to the courts and others.

Indeed, Binney has patiently explained for many years that we know how to help prevent terrorism ... and corruption is what's preventing us from doing it.

Binney thinks we should get serious about motivating the intelligence agencies to do their job.

The original source of this article is Washington's Blog
Copyright © Bill Binney and Washington's Blog, Washington's Blog, 2017

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Bill Binney and Washington's Blog

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca