GlobalResearch
Center for Research on Globalization

Top National Security Experts: Spying Program Doesn't Make Us Safer, and Spying Leaks Don't Harm America

By Washington's Blog
Global Research, June 13, 2013
Washington's Blog

Region: USA
Theme: Intelligence, Police State & Civil Rights

NSA Leaks Help – Rather than Hurt – the United States

America's top national security experts say that the NSA's mass surveillance program *doesn't* make us safer ... and that whistleblowers revealing the nature and extent of the program *don't* harm America.

The top counter-terrorism czar under Presidents Clinton and Bush – Richard Clarke – notes:

> The just-revealed surveillance stretches the law to its breaking point and opens the door to future potential abuses
>
> ***
>
> I am troubled by the precedent of stretching a law on domestic surveillance almost to the breaking point. On issues so fundamental to our civil liberties, elected leaders should not be so needlessly secretive.
>
> The argument that this sweeping search must be kept secret from the terrorists is laughable. Terrorists already assume this sort of thing is being done. Only law-abiding American citizens were blissfully ignorant of what their government was doing.
>
> ***
>
> If the government wanted a particular set of records, it could tell the Foreign Intelligence Surveillance Court why — and then be granted permission to access those records directly from specially maintained company servers. The telephone companies would not have to know what data were being accessed. There are no technical disadvantages to doing it that way, although it might be more expensive.
>
> Would we, as a nation, be willing to pay a little more for a program designed this way, to avoid a situation in which the government keeps on its own computers a record of every time anyone picks up a telephone? That is a question that should have been openly asked and answered in Congress.

The author of the Patriot Act and chairman on the House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations – Congressman Jim Sensenbrenner – says:

- Lawmakers' and the executive branch's excuses about recent revelations of NSA activity are "a bunch of bunk"

- The government has gone far beyond what the Patriot Act intended, and that section 215 of the act "was originally drafted to prevent data mining" on the scale that's occurred

- Whistleblower Edward Snowden is not a traitor, and Sensenbrenner would not have known the extent of abuse by the NSA and the FISA court without Snowden's disclosures

- The Patriot Act needs to be amended to protect Americans' privacy

The former head of the NSA's global digital data gathering program, William Binney:

- Confirms Snowden's allegations about the mass surveillance program

- Says that revealing the details of the spying program will not harm national security … and that government officials are only mad because it exposes their overreaching

- Says that massive surveillance doesn't work to make us safer

- Says that he set up the NSA's system so that all of the information would automatically be *encrypted*, so that the government had to obtain a search warrant based upon probably cause before a particular suspect's communications could be decrypted. But the NSA now collects all data in an *unencrypted* form, so that no probable cause is needed to view any citizen's information. He says that it is actually cheaper and easier to store the data in an encrypted format: so the government's current system is being done for political – *not practical* – purposes. Binney's statements have been confirmed by other NSA whistleblowers

- Says that the government is using information gained through mass surveillance in order to go after anyone they take a dislike to

- Says that the NSA's spying programs have brought us incredibly close to "a turnkey totalitarian state"

Former FBI counterterrorism agent Tim Clemente confirmed Snowden's allegations, and told CNN:

- "Welcome to America. All of that stuff is being captured as we speak whether we know it or like it or not"

- "No digital communication is secure"

Senator Jon Tester – a member of the Committee on Homeland Security and Governmental

Affairs, and the Approrpriations Committee's Subcommittee on Homeland Security – says Snowden didn't harm national security, and that his leaks were helpful:

> The information that they wrote about was just the fact that NSA was doing broad sweeps of foreign and domestic phone records, metadata. [T]he fact of the matter is is I don't see how that compromises the security of this country whatsoever.
>
> And quite frankly, it helps people like me become aware of a situation that I wasn't aware of before because I don't sit on that Intelligence Committee.

And Thomas Drake – a former senior NSA executive and a decorated Air Force and Navy veteran – writes:

> What Edward Snowden has done is an amazingly brave and courageous act of civil disobedience.
>
> Like me, he became discomforted by [the NSA's] direct violation of the fourth amendment of the US constitution.
>
> The NSAprograms that Snowden has revealed are nothing new: they date back to the days and weeks after 9/11. I had direct exposure to similar programs, such as Stellar Wind, in 2001. In the first week of October, I had an extraordinary conversation with NSA's lead attorney. When I pressed hard about the unconstitutionality of Stellar Wind, he said:
>
> > "The White House has approved the program; it's all legal. NSA is the executive agent."
>
> It was made clear to me that the original intent of government was to gain access to all the information it could without regard for constitutional safeguards. "You don't understand," I was told. "We just need the data."
>
> In the first week of October 2001, President Bush had signed an extraordinary order authorizing blanket dragnet electronic surveillance: Stellar Wind was a highly secret program that, without warrant or any approval from the Fisa court, gave the NSA access to all phone records from the major telephone companies, including US-to-US calls. It correlates precisely with the Verizon order revealed by Snowden; and based on what we know, you have to assume that there are standing orders for the other major telephone companies.
>
> ***
>
> The supposed oversight, combined with enabling legislation – the Fisa court, the congressional committees – is all a kabuki dance, predicated on the national security claim that we need to find a threat. The reality is, they just want it all, period.
>
> So I was there at the very nascent stages, when the government – wilfully and in deepest secrecy – subverted the constitution. All you need to know about so-called oversight is that the NSA was already in violation of the Patriot Act by the time it was signed into law.
>
> ***

To the US government today, however, we are all foreigners.

I became an expert on East Germany, which was then the ultimate surveillance state. Their secret police were monstrously efficient: they had a huge paper-based system that held information on virtually everyone in the country – a population of about 16-17 million. The Stasi's motto was "to know everything".

***

So none of this is new to me. The difference between what the Bush administration was doing in 2001, right after 9/11, and what the Obama administration is doing today is that the system is now under the cover and color of law. Yet, what Snowden has revealed is still the tip of the iceberg. [Congresswoman Loretta Sanchez – a member of the Committee on Homeland Security and the Armed Services Committee's Subcommittee on Emerging Threats and Capabilities confirms this]

General Michael Hayden, who was head of the NSA when I worked there, and then director of the CIA, said, "We need to own the net." [Background] And that is what they're implementing here. They have this extraordinary system: in effect, a 24/7 panopticon on a vast scale that it is gazing at you with an all-seeing eye.

***

My concern [while working for the NSA] was that we were more than an accessory; this was a crime and we were subverting the constitution.

I differed as a whistleblower to Snowden only in this respect: in accordance with the Intelligence Community Whistleblower Protection Act, I took my concerns up within the chain of command, to the very highest levels at the NSA, and then to Congress and the Department of Defense. I understand why Snowden has taken his course of action, because he's been following this for years: he's seen what's happened to other whistleblowers like me.

By following protocol, you get flagged – just for raising issues. You're identified as someone they don't like, someone not to be trusted. [Indeed, Obama has prosecuted more whistleblowers than all other presidents combined. And the government threw in jail the one telecom executive to refuse government orders to hand over mass surveillance records on its customers.] I was exposed early on because I was a material witness for two 9/11 congressional investigations. In closed testimony, I told them everything I knew ….

But as I found out later, none of the material evidence I disclosed went into the official record. It became a state secret even to give information of this kind to the 9/11 investigation.

I reached a point in early 2006 when I decided I would contact a reporter. I had the same level of security clearance as Snowden. If you look at the indictment from 2010, you can see that I was accused of causing "exceptionally grave damage to US national security". Despite allegations that I had tippy-top-secret documents, In fact, I had no classified information in my possession, and I disclosed none to the Baltimore Sun journalist during 2006 and 2007. But I got hammered: in November 2007, I was raided by a dozen armed FBI agents, when I was served with a search warrant. The nightmare had only just begun, including extensive physical and electronic surveillance.

In April 2008, in a secret meeting with the FBI, the chief prosecutor from the Department of Justice assigned to lead the prosecution said, "How would you like to spend the rest of your life in jail, Mr Drake?" – unless I co-operated with

> their multi-year, multimillion-dollar criminal leak investigation, launched in 2005 after the explosive New York Times article revealing for the first time the warrantless wiretapping operation. Two years later, they finally charged me with a ten felony count indictment, including five counts under the Espionage Act. I faced upwards of 35 years in prison.
>
> In July 2011, after the government's case had collapsed under the weight of truth, I plead to a minor misdemeanor for "exceeding authorized use of a computer" under the Computer Fraud and Abuse Act – in exchange for the DOJ dropping all ten felony counts. I received as a sentence one year's probation and 240 hours of community service: I interviewed almost 50 veterans for the Library of Congress veterans history project. This was a rare, almost unprecedented, case of a government prosecution of a whistleblower ending in total defeat and failure.
>
> So, the stakes for whistleblowers are incredibly high. The government has got its knives out: there's a massive manhunt for Snowden. They will use all their resources to hunt him down and every detail of his life will be turned inside out. They'll do everything they can to "bring him to justice" – already there are calls for the "traitor" to be "put away for life".
>
> ***
>
> Since the government unchained itself from the constitution after 9/11, it has been eating our democracy alive from the inside out. There's no room in a democracy for this kind of secrecy: it's anathema to our form of a constitutional republic, which was born out of the struggle to free ourselves from the abuse of such powers, which led to the American revolution.
>
> That is what's at stake here: to an NSA with these unwarranted powers, we're all potentially guilty; we're all potential suspects until we prove otherwise. That is what happens when the government has all the data.
>
> ***
>
> We are seeing an unprecedented campaign against whistleblowers and truth-tellers: it's now criminal to expose the crimes of the state.

Drake also tweets:

> [People] must get clear & present danger of authoritarian totalitarianism via the Leviathan [National Security] state & surveillance

And:

> Snowden chose 2 free darkside NatSec info as magnificent act of selfless civil disobedience 2 protect our liberty.

Comment on Global Research Articles on our Facebook page

Articles by: Washington's Blog