GlobalResearch
Center for Research on Globalization

The Government's Spying Is Not As Bad As The Whistleblower Said … It's WORSE

By Washington's Blog
Global Research, June 16, 2013
Washington's Blog

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

Whistleblower Claims Validated … and Then Some

The government is attacking whistleblower Edward Snowden by claiming that he was lying about the scope of the NSA's spying on Americans.

However, CNET reports today:

> The National Security Agency has acknowledged in a new classified briefing that it does not need court authorization to listen to domestic phone calls.
>
> Rep. Jerrold Nadler, a New York Democrat, disclosed this week that during a secret briefing to members of Congress, he was told that the contents of a phone call could be accessed "simply based on an analyst deciding that."
>
> If the NSA wants "to listen to the phone," an analyst's decision is sufficient, without any other legal authorization required, Nadler said he learned. "I was rather startled," said Nadler, an attorney and congressman who serves on the House Judiciary committee.
>
> Not only does this disclosure shed more light on how the NSA's formidable eavesdropping apparatus works domestically, it also suggests the Justice Department has secretly interpreted federal surveillance law to permit thousands of low-ranking analysts to eavesdrop on phone calls.
>
> Because the same legal standards that apply to phone calls also apply to e-mail messages, text messages, and instant messages, Nadler's disclosure indicates the NSA analysts could also access the contents of Internet communications without going before a court and seeking approval.
>
> The disclosure appears to confirm some of the allegations made by Edward Snowden, a former NSA infrastructure analyst who leaked classified documents to the Guardian. Snowden said in a video interview that, while not all NSA analysts had this ability, he could from Hawaii "wiretap anyone from you or your accountant to a federal judge to even the president."
>
> ***
>
> Earlier reports have indicated that the NSA has the ability to record nearly all domestic and international phone calls — in case an analyst needed to access the recordings in the future. A Wired magazine article last year disclosed that the NSA has established "listening posts" that allow the agency to collect and sift through billions of phone calls through a massive new data center in Utah, "whether they originate within the country or overseas." That includes not just metadata, but also the contents of the communications.

***

A requirement of the 2008 law is that the NSA "may not intentionally target any person known at the time of acquisition to be located in the United States." A possible interpretation of that language, some legal experts said, is that the agency may vacuum up everything it can domestically — on the theory that indiscriminate data acquisition was not intended to "target" a specific American citizen.

***

Sen. Dianne Feinstein (D-Calif.), the head of the Senate Intelligence committee, separately acknowledged this week that the agency's analysts have the ability to access the "content of a call."

Director of National Intelligence Michael McConnell indicated during a House Intelligence hearing in 2007 that the NSA's surveillance process involves "billions" of bulk communications being intercepted, analyzed, and incorporated into a database.

***

Former FBI counterterrorism agent Tim Clemente told CNN last month that, in national security investigations, the bureau can access records of a previously made telephone call. "All of that stuff is being captured as we speak whether we know it or like it or not," he said. Clemente added in an appearance the next day that, thanks to the "intelligence community" — an apparent reference to the NSA — "there's a way to look at digital communications in the past."

Remember that Snowden also revealed that the NSA is tapping into the servers of 9 big internet companies. Two government officials have admitted that as many as *50* American companies are now feeding the NSA with real-time user data. And we've documented that the NSA gives information gained through spying to large corporations.

Bloomberg reports:

Thousands of technology, finance and manufacturing companies are working closely with U.S. national security agencies, providing sensitive information and in return receiving benefits that include access to classified intelligence, four people familiar with the process said. [We documented Tuesday that the government is illegally spying on all Americans ... and then giving the info to giant corporations.]

These programs, whose participants are known as trusted partners, extend far beyond what was revealed by Edward Snowden ….

Makers of hardware and software, banks, Internet security providers, satellite telecommunications companies and many other companies also participate in the government programs. In some cases, the information gathered may be used not just to defend the nation but to help infiltrate computers of its adversaries.

Along with the NSA, the Central Intelligence Agency, the Federal Bureau of Investigation and branches of the U.S. military have agreements with such companies to gather data that might seem innocuous but could be highly useful in the hands of U.S. intelligence or cyber warfare units, according to the people, who have either worked for the government or are in companies that

have these accords.

***

Microsoft and other software or Internet security companies have been aware that this type of early alert allowed the U.S. to exploit vulnerabilities in software sold to foreign governments, according to two U.S. officials. Microsoft doesn't ask and can't be told how the government uses such tip-offs, said the officials, who asked not to be identified because the matter is confidential.

***

Some U.S. telecommunications companies willingly provide intelligence agencies with access to facilities and data offshore that would require a judge's order if it were done in the U.S.…

***

Most of the arrangements are so sensitive that only a handful of people in a company know of them, and they are sometimes brokered directly between chief executive officers and the heads of the U.S.'s major spy agencies, the people familiar with those programs said.

Michael Hayden, who formerly directed the National Security Agency and the CIA, described the attention paid to important company partners: "If I were the director and had a relationship with a company who was doing things that were not just directed by law but were also valuable to the defense of the Republic, I would go out of my way to thank them and give them a sense as to why this is necessary and useful."

***

Intel's McAfee unit, which makes Internet security software, regularly cooperates with the NSA, FBI and the CIA, for example ….

***

In exchange, leaders of companies are showered with attention and information by the agencies to help maintain the relationship, the person said.

***

Following an attack on his company by Chinese hackers in 2010, Sergey Brin, Google's co-founder, was provided with highly sensitive government intelligence linking the attack to a specific unit of the People's Liberation Army, China's military, according to one of the people, who is familiar with the government's investigation. Brin was given a temporary classified clearance to sit in on the briefing, the person said.

According to information provided by Snowden, Google, owner of the world's most popular search engine, had at that point been a Prism participant for more than a year.

***

The information provided by Snowden also exposed a secret NSA program known as Blarney. As the program was described in the Washington Post (WPO), the agency gathers metadata on computers and devices that are used to send e-mails or browse the Internet through principal data routes, known as a backbone.

> That metadata includes which version of the operating system, browser and Java software are being used on millions of devices around the world, information that U.S. spy agencies could use to infiltrate those computers or phones and spy on their users.
>
> "It's highly offensive information," said Glenn Chisholm, the former chief information officer for Telstra Corp (TLS)., one of Australia's largest telecommunications companies, contrasting it to defensive information used to protect computers rather than infiltrate them.
>
> According to Snowden's information, Blarney's purpose is "to gain access and exploit foreign intelligence," the Post said.
>
> ***
>
> Lawmakers who oversee U.S. intelligence agencies may not understand the significance of some of the metadata being collected, said Jacob Olcott, a former cybersecurity assistant for Senator John D. Rockefeller IV of West Virginia, the Democratic chairman of the Senate Commerce Committee.
>
> "That's what makes this issue of oversight so challenging," said Olcott, now a principal at Good Harbor Security Risk Management in Washington. "You have a situation where the technology and technical policy is far outpacing the background and expertise of most elected members of Congress or their staffs."
>
> While companies are offered powerful inducements to cooperate with U.S. intelligence, many executives are motivated by patriotism or a sense they are defending national security, the people familiar with the trusted partner programs said.

Indeed, former top NSA executives Thomas Drake and William Binney, Congresswoman Loretta Sanchez – a member of the Committee on Homeland Security and the Armed Services Committee's Subcommittee on Emerging Threats and Capabilities – and others say that Snowden's revelations are only "the tip of the iceberg".

AP reports:

> Interviews with more than a dozen current and former government and technology officials and outside experts show that, while Prism has attracted the recent attention, the program actually is a relatively small part of a much more expansive and intrusive eavesdropping effort.
>
> Americans who disapprove of the government reading their emails have more to worry about from a different and larger NSA effort that snatches data as it passes through the fiber optic cables that make up the Internet's backbone. That program … copies Internet traffic as it enters and leaves the United States, then routes it to the NSA for analysis.
>
> ***

Deep in the oceans, hundreds of cables carry much of the world's phone and Internet traffic. Since at least the early 1970s, the NSA has been tapping foreign cables. It doesn't need permission. That's its job.

But Internet data doesn't care about borders. Send an email from Pakistan to Afghanistan and it might pass through a mail server in the United States, the same computer that handles messages to and from Americans. The NSA is prohibited from spying on Americans or anyone inside the United States. That's the FBI's job and it requires a warrant.

Despite that prohibition, shortly after the Sept. 11 terrorist attacks, President George W. Bush secretly authorized the NSA to plug into the fiber optic cables that enter and leave the United States, knowing it would give the government unprecedented, warrantless access to Americans' private conversations.

Tapping into those cables allows the NSA access to monitor emails, telephone calls, video chats, websites, bank transactions and more. It takes powerful computers to decrypt, store and analyze all this information, but the information is all there, zipping by at the speed of light.

"You have to assume EVERYTHING is being collected," said Bruce Schneier, who has been studying and writing about cryptography and computer security for two decades.

***

The New York Times disclosed the existence of this effort in 2005. In 2006, former AT&T technician Mark Klein revealed that the company had allowed the NSA to install a computer at its San Francisco switching center, a spot where fiber optic cables enter the U.S.

***

Americans' personal emails can live in government computers, but analysts can't access, read or listen to them unless the emails become relevant to a national security investigation.

The government doesn't automatically delete the data, officials said, because an email or phone conversation that seems innocuous today might be significant a year from now.

***

Two decades from now, the government could have a trove of American emails and phone records it can tap to investigative whatever Congress declares a threat to national security.

***

In slide made public by the newspapers, NSA analysts were encouraged to use data coming from both Prism and from the fiber-optic cables.

Prism, as its name suggests, helps narrow and focus the stream. If eavesdroppers spot a suspicious email among the torrent of data pouring into the United States, analysts can use information from Internet companies to pinpoint the user.

With Prism, the government gets a user's entire email inbox. Every email, including contacts with American citizens, becomes government property.

Once the NSA has an inbox, it can search its huge archives for information about everyone with whom the target communicated. All those people can be investigated, too.

That's one example of how emails belonging to Americans can become swept up in the hunt.

In that way, Prism helps justify specific, potentially personal searches. But it's the broader operation on the Internet fiber optics cables that actually captures the data, experts agree.

"I'm much more frightened and concerned about real-time monitoring on the Internet backbone," said Wolf Ruzicka, CEO of EastBanc Technologies, a Washington software company. "I cannot think of anything, outside of a face-to-face conversation, that they could not have access to."

***

Schneier, the author and security expert, said it doesn't really matter how Prism works, technically. Just assume the government collects everything, he said.

He said it doesn't matter what the government and the companies say, either …. "No one is telling the truth."
