CBC news

NSA's shuttered program was 'a sacrificial lamb' in U.S. mass surveillance

NSA ordered to stop bulk phone record collection program last weekend

Aleksandra Sagan

December 6, 2015

The National Security Agency in the United States may have shuttered its controversial bulk phone record collection program, but that doesn't mean people living in that country suddenly have their communications free from government scrutiny.

The NSA can still access much of Americans' communication metadata, security experts say, and some believe the agency may secretly continue its previous mass surveillance of phone records regardless of government orders.

The change is "not going to be a big blow" to the NSA, says David Murakami Wood, the Canadian Research Chair in surveillance studies at Queen's University in Kingston, Ont.

"The fact that they've allowed it to be cancelled probably suggests it's a bit of a sacrificial lamb."

Murky definition of bulk collection

By the stroke of midnight last Sunday, Nov. 29, the USA Freedom Act forced the NSA to halt its mass collection of Americans' phone records, a practice revealed by former NSA contractor turned whistleblower Edward Snowden.

Snowden also revealed that Canada's electronic spy agency **tracks millions of downloads daily** by people around the world, including Canadians.

While it's hard to know much about the Canadian Security Establishment because of the secrecy surrounding the agency, there is "evidence of the same kind of indiscriminate surveillance as the NSA engages in," says David Lyon, the director of Queen's University's surveillance studies centre and author of *Surveillance after Snowden*.

Following American uproar after Snowden exposed the NSA's activities and the expiration of the USA Freedom Act's deadline this past weekend, the security agency must now seek permission from the Foreign Intelligence Surveillance Court (FISC) for targeted surveillance. That could allow it to see phone records of Americans who match any criteria they are searching for, such as individuals who live in a specific area or have visited suspicious internet sites.

Sometimes the difference between bulk and targeted data collection can be fuzzy, says Julian Sanchez, a senior fellow at the Cato Institute, an American think-tank in Washington, D.C.

"The intelligence community uses bulk collection to really only mean, essentially, totally indiscriminate collection," he says. "There are lots of types of collection you and I might intuitively think of as bulk that they would not call bulk."

This means the NSA will still be able to gather data from large segments of the population. For example, the NSA could create a list of 100 suspicious websites and 10,000 jihadist YouTube videos, he says, and ask FISC to grant it access to the detailed records for all the IP addresses that have accessed any of that content.

Most people would consider that bulk collection because it doesn't seem to be rooted in very specific grounds for suspicion, Sanchez says, but the intelligence agency will likely consider that a targeted search.

Similar collection programs may exist

It may even be simpler to get that information than turning to FISC for permission.

The NSA likely has at least one other program, which it was not ordered to stop, or more that "do very similar things or cover the same ground," Murakami Wood says.

The security agency "continually plays this shell game with Congressional overseers," writes Bruce Schneier, author of *Data and Goliath*, on his security blog.

When the NSA claims the agency doesn't do something under a particular program or under a particular authority, he writes, "you can be sure that it's being done under some other program or some other authority."

For example, Murakami Wood says, the NSA could simply ask one of its international partners, like the United Kingdom's Government Communications Headquarters (GCHQ), to conduct a similar program, which doesn't have to abide by American laws.

Potential to ignore orders

It's also possible the NSA will simply ignore government orders and carry on with secret surveillance of telecommunication metadata, says Murakami Wood.

"[The NSA] frequently does things which are technically illegal under U.S. law, and then when it's found out, it promises to ease back on these things."

He recalls the reveal of project MINARET, which ran in the late 1960s and early 1970s, during which the NSA spied on the communications of some U.S. citizens placed on a watchlist.

"It's happened again and again and again," Murakami Wood says.

Lyon says he remains hopeful that won't be the case. But "it's difficult to be definitive when the agency has clearly not only been secretive, but has also directly spread untruth through their director."

In March 2013, Senator Ron Wyden asked national intelligence director James Clapper if the NSA collects any type of data on millions or hundreds of millions of Americans. Clapper denied the agency "wittingly" does this.

Snowden's first revelations were made public in June 2013.

Internet communications still fair game

Even if the NSA abides by the law and ceases this type of surveillance, as Lyon hopes the agency is doing, it has access to even more revealing communications.

The law only limits telecommunications metadata surveillance. It allows the NSA to continue monitoring Americans' internet metadata, says Lyon.

That information is "much more revealing," he says.

The NSA can track the websites people visits, the files they download, the shows they stream and all kinds of other online activity, says Lyon.

"It reveals much more than phone metadata ever could about people's connections, preferences and commitments, including political or religious allegiances."