INTERNATIONAL BUSINESS TIMES

NSA Metadata Surveillance: The Loophole That Gives The NSA Free Range Over Millions Of Phone Records

By: Pema Levy -August 5, 2013

Responding to mounting criticism of its secret foreign intelligence operations, last week the director of national intelligence released three formerly classified documents in a symbolic gesture toward more transparency. But the revelations in those documents have only added to privacy advocates' worries about the scope of the government's surveillance powers.

One of the documents detailed how the NSA pulls out potentially millions of Americans' phone records and, rather than being limited in how it analyses those records, can search and analyze the information at any time and with apparently little oversight.

Under the phone records program revealed by former intelligence contractor Edward Snowden in June, the NSA acquires the so-called metadata -- the phone numbers on each end, duration and time -- of all domestic calls as well as calls in which one of the numbers is in the United States. These records, collected on an ongoing basis each day, are stored in a massive database that the NSA can query when it believes it has a lead in a terrorism investigation. What the new document suggests is that this is only how the NSA initially collects and accesses the phone data. But the extent of how the NSA uses that data is much greater.

This information came in the companion court order or "primary order" to the Foreign Intelligence Surveillance Court (FISC) document leaked by Snowden. That document ordered Verizon to turn over the phone numbers on each end, duration and time of all its calls as part of the NSA's phone records collection program. The primary order, declassified last week, stipulates the rules under which that data may be used. In those rules, there appears to be a significant loophole allowing NSA analysts unfettered access to hundreds of thousands, if not millions, of Americans' phone records.

Since the first court order was leaked, administration officials have tried to reassure the public that the program protects Americans' privacy, by mentioning the strict rules and limited use of the database that holds all domestic call records. The system can only be accessed by 22 specially trained NSA analysts and only after the agency determines that a particular query satisfies the legal "reasonable articulable suspicion" standard. The result, officials have often repeated, is that the database was only queried 300 times in the last year.

But according to the new document, the NSA's use of the phone records is "not nearly as limited, not nearly as constrained as that 300 number they keep pressing would suggest," said Patrick Toomey, a national security fellow at the American Civil Liberties Union.

In order to extensively analyze all the results of the initial queries, the phone records resulting from some or all of the queries are transferred to a secondary database that can be analyzed in the future without the strict oversight in place over the original database.

This second database, called the "corporate store," could potentially hold the records of millions of Americans' phone calls. Each time an NSA analyst queries the original database, it can analyze data within three "hops" of the original person suspected in the terrorism investigation. This means that for each of the 300 queries run last year, the analyst could have pulled not only the numbers called by the suspect, but also all the call records of people who spoke with the suspect, and then all the numbers associated with those people, and then all the people connected to those people -- a total of three degrees of separation. If each person touched by the query is in contact with 40 people, then a three-hop search on a single suspect could pull in the records of 2.5 million people.

Now, it appears that all of those records are placed in a new database that can be queried at any time, and without restrictions on what the analysts go fishing for -- in other words, without meeting the "reasonable articulable suspicion" (RAS) standard. The details of what appears to be a big loophole on the restrictions on the government's access to Americans' sensitive information are sprinkled throughout the 17-page FISC order.

According to the document, analysts don't perform all the queries. In addition, some queries of the main phone records database are done by an automated process using pre-approved search terms that meet the legal standard. The "hop-limited results" of those automated searches are placed in the "corporate store." Analysts can search within this second store of data, importantly, "without the requirement that those searches use only RAS-approved selection terms." According to one footnote in the documents, analysts can "apply the full range of SIGINT analytic tradecraft to the result of intelligence analysis queries of the collected BR [telephony] metadata." It is unclear from the document whether all or only some query results go into the second pool of data, or how long data is held in this second pool. But the footnote does not differentiate between how the query was run and what kind of analyses can be performed on those results.

"Reassembling all these different three-hop queries into one place, really, to us, says they're just rebuilding essentially the front-end database with no restrictions," Toomey said.

As evidence of the strict oversight of the metadata program, intelligence officials have cited the fact that each query of the database is recorded and potentially can be audited. This is not the case with any analyses performed on query results, according to the newly-released order, meaning that there may not be a record of how and at what frequency NSA analysts are diving into this second pool of data. "This auditable record requirement shall not apply to accesses of the results of RAS-approved queries," a footnote reads.

Privacy advocates believe that the second database, which allows the NSA to analyze data in ways that does not relate to the initial target of the investigation, gives the NSA too much free rein over Americans' personal information. "It's basically there for the taking once the initial query's been run," Toomey said. By combining the three-hop results from multiple queries in a second database, the NSA "gets around the initial restrictions that they want us to believe are being applied."

On the one hand, the agency's ability to run extensive and largely unrestricted analyses of so many Americans phone records contradicts the assurances of the intelligence community about

the limited and carefully reviewed use of the database. On the other hand, the ability to continually analyze query results and compare them to other suspicious numbers seems like a useful counter-terrorism tool, although the ACLU contends that the three-hop system already allows the NSA access to a vast amount of information to find terrorism links.

“The only real reason to get this much data in the first place is to run sophisticated analyses on -- and comparisons between -- target networks over time,” Julian Sanchez, a privacy expert at the libertarian Cato Institute, wrote in an email. “But it also makes all the government's assurances about the strict checks on initial queries seem like a bit of a sham if those are just the starting points they use to populate their working database.”

“If they're going to search every building in the city, it doesn't make all that much difference that they had a warrant for the house where they started,” he added.