The Facts About the Metadata 'Menace'

by K. Jack Riley
January 26, 2014

photo by Reuters/Larry Downing
Member of the protest group, Code Pink, protests against U.S. President Barack Obama and the NSA before his arrival at the Department of Justice, Jan. 17, 2014

President Obama has announced several significant changes to U.S. counter-terrorism intelligence-collection programs, including an overhaul of the way the National Security Agency stores and accesses telephone metadata. But what has sometimes been overlooked in the firestorm created by Edward Snowden's leaks about the program is a clear definition of what metadata is, and what it is not.

On the eve of the president's announcement, I took part in a daylong session of briefings, discussion and debate at the NSA. The session, arranged by Carnegie Mellon University professor Kiron Skinner and Emily Goldman of the Pentagon's Cyber Command, involved a small group of computer scientists and other researchers and the top leadership of the NSA. The meetings were spectacular for their clarity and candor.

Much of what Snowden leaked has proved controversial, but probably nothing more so than the metadata program authorized by the Patriot Act. This program permits the collection and — under limited circumstances — analysis of metadata on American phone numbers and thus American citizens for counter-terrorism purposes.

Metadata from a phone call include information such as the direction (who called whom), length, date and time. The program does not record the location or the name associated with a call. No one is listening to the call and no content is recorded. And the metadata are segregated and stored separately from all the other signals data the NSA collects.

Here's a typical way the metadata are used: An intelligence community client, say the FBI, will send the NSA an official request for investigation of a certain phone number that it believes might be associated with suspected terrorists. In order to examine the metadata associated with a phone number, the NSA has to "make RAS" — that is, to show "reasonably articulable suspicion."

For a phone number that meets the RAS standard, the NSA can examine metadata two hops, or two call generations, away from the original number. Think of a phone bill that displays calls made and received. It can look at metadata for every phone number on the original bill, plus the phone numbers on the bills for the numbers that show up on the bill of the original number. That's two hops. Among the reforms unveiled by Obama was the reduction in the number of permitted hops from three to two.

What prevents the NSA from relentlessly hopping from one "interesting" number to the next? There are a number of checks: Subsequent generations of metadata and phone numbers cannot be investigated without making RAS on them, which means new review and new approvals; only 22 NSA managers are authorized to approve examination of metadata; the Justice Department audits the program every 90 days; and the program has to undergo reauthorization with the Foreign Intelligence Surveillance Court every quarter. That means at least 15 different federal judges have looked at — and approved — the program since its inception.

What is not happening with the metadata? There's no freewheeling data-mining, no Facebook-style graphing of social networks and no unrestricted exploratory data analysis.

The president has proposed a number of reforms, including requiring judicial approval before the NSA can access metadata. He also proposed a transition that would shift storage of the metadata from NSA to a third party, possibly the telephone companies.

Judicial review of metadata use is already occurring, albeit after the fact in quarterly court reviews. Integrating judicial review into each explicit accessing of the metadata is a prudent and reasonable step, though it has the potential to slow investigations.

At first glance, shifting data-retention responsibilities to a third party might appear to keep Americans' metadata one additional step removed from prying NSA eyes. But there are potential risks associated with this move. Private retention could be technically complex and could slow investigations. Even with the NSA providing storage standards and guidance, the data may be less secure simply because they are spread across more organizations and locations.

The reforms sought by the administration may or may not ease the privacy concerns many Americans have about the metadata collection program. Understanding what metadata is, and isn't, might.

Jack Riley is vice president of the nonpartisan, nonprofit Rand Corp. and director of the RAND National Security Research Division.

This commentary appeared in *Los Angeles Times* on January 26, 2014.