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.

CNN Justice

Judge: NSA domestic phone data-mining unconstitutional

By **Bill Mears** and **Evan Perez**, CNN
updated 8:52 PM EST, Mon December 16, 2013

STORY HIGHLIGHTS

- Snowden says he knew the surveillance would not withstand legal review
- The limited ruling opens the door to possible further legal challenges
- The NSA data-mining can continue, pending a likely appeal
- Classified leaks by Edward Snowden revealed the extent of the data-mining

Washington (CNN) -- A federal judge said Monday that he believes the government's once-secret collection of domestic phone records is unconstitutional, setting up likely appeals and further challenges to the data mining revealed by classified leaker Edward Snowden.
U.S. District Judge Richard Leon said the National Security Agency's bulk collection of metadata -- phone records of the time and numbers called without any disclosure of content -- apparently violates privacy rights.

His preliminary ruling favored five plaintiffs challenging the practice, but Leon limited the decision only to their cases.

NSA phone surveillance unconstitutional?

"I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every citizen for purposes of querying and analyzing it without prior judicial approval," said Leon, an appointee of President George W. Bush. "Surely, such a program infringes on 'that degree of privacy' that the Founders enshrined in the Fourth Amendment."

Leon's ruling said the "plaintiffs in this case have also shown a strong likelihood of success on the merits of a Fourth Amendment claim," adding "as such, they too have adequately demonstrated irreparable injury."

He rejected the government's argument that a 1979 Maryland case provided precedent for the constitutionality of collecting phone metadata, noting that public use of telephones had increased dramatically in the past three decades.

Leon also noted that the government "does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the government in achieving any objective that was time-sensitive in nature."

However, he put off enforcing his order barring the government from collecting the information, pending an appeal by the government.
A Justice Department spokesman said Monday that "we believe the program is constitutional as previous judges have found," but said the ruling is being studied.

Democratic Sen. Mark Udall of Colorado, a critic of the NSA data mining, said Leon's ruling showed that "the bulk collection of Americans' phone records conflicts with Americans' privacy rights under the U.S. Constitution and has failed to make us safer."

He called on Congress to pass legislation he proposed to "ensure the NSA focuses on terrorists and spies - and not innocent Americans."
Explosive revelations earlier this year by Snowden, a former NSA contractor, triggered new debate about national security and privacy interests in the aftermath of the September 2001 terrorist attacks.

Snowden's revelations led to more public disclosure about the secretive legal process that sets in motion the government surveillance.
In a statement distributed by journalist Glenn Greenwald, who first reported the leaks, Snowden said he acted on the belief that the mass surveillance program would not withstand a constitutional challenge, and that Americans deserved a judicial review.

"Today, a secret program authorized by a secret court was, when exposed to the light of day, found to violate Americans' rights. It is the first of many," according to Snowden, who is living in Russia under a grant of asylum to avoid prosecution over the leaks in the United States.
Greenwald said the judge's ruling vindicates what Snowden did.

"I think it's not only the right, but the duty of an American citizen in Edward Snowden's situation to come forward, at great risk to himself, and inform his fellow citizens about what it is their government is doing in the dark that is illegal," the journalist told CNN's "Anderson Cooper 360" Monday night.

The NSA has admitted it received secret court approval to collect vast amounts of metadata from telecom giant Verizon and leading Internet companies, including Microsoft, Apple, Google, Yahoo and Facebook.

The case before Leon involved approval for surveillance in April by a judge at the Foreign Intelligence Surveillance Court (FISC), a secret body that handles individual requests for electronic surveillance for "foreign intelligence purposes."

Verizon Business Network Services turned over the metadata to the government.

Leon's ruling comes as the Obama administration completes a review of NSA surveillance in the aftermath of the Snowden leaks.
CNN's Jake Tapper reported Monday that tech company executives would meet with President Barack Obama at the White House on Tuesday to discuss the issue.

Obama plans to sit down with Tim Cook of Apple and Eric Schmidt of Google, as well as executives from Twitter, Microsoft, Facebook, Salesforce, Netflix , Etsy, Dropbox, Yahoo!, Zynga, Sherpa Global, Comcast, LinkedIn and AT&T, a White House official said.
Some of those companies issued a joint letter last week calling on the government to change its surveillance policies in the wake of the Snowden revelations.

Last month, the Supreme Court refused to take up the issue when it denied a separate petition, which was filed by the Electronic Information Privacy Center. Prior lawsuits against the broader NSA program also have been unsuccessful.

Days after the Snowden disclosure in June, some Verizon customers filed legal challenges in the D.C. federal court.
The left-leaning American Civil LIberties Union also filed a separate, pending suit in New York federal court.

Under the Foreign Intelligence Surveillance Act of the 1970s, the secret courts were set up to grant certain types of government requests-- wiretapping, data analysis, and other monitoring of possible terrorists and spies operating in the United States.
The Patriot Act that Congress passed after the 9/11 attacks broadened the government's ability to conduct anti-terrorism surveillance in the United States and abroad, eventually including the metadata collection.

In order to collect the information, the government has to demonstrate that it's "relevant" to an international terrorism investigation.
However, the 1978 FISA law lays out exactly what the special court must decide: "A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person."

In defending the program, NSA Director Gen. Keith Alexander told the Senate Judiciary Committee last week that "15 separate judges of the FISA Court have held on 35 occasions that Section 215 (of the Patriot Act) authorizes the collection of telephony metadata in bulk in support of counterterrorism investigations."

Initially, telecommunications companies such as Verizon, were the targets of legal action against Patriot Act provisions. Congress later gave retroactive immunity to those private businesses.

The revelations of the NSA program and the inner workings of the FISC court came after Snowden leaked documents to the Guardian newspaper. Snowden fled to Hong Kong and then Russia to escape U.S. prosecution.

The case is Klayman v. Obama (13-cv-881).

CNN's Tom Cohen contributed to this report.