dataprotectionlaw&policy

THE MONTHLY JOURNAL FOR DATA PROTECTION PROFESSIONALS
AUGUST 2013 VOLUME 10 ISSUE 08
WWW.E-COMLAW.COM

Analysis of the USA PRISM and other NSA surveillance programs

Following leaks from notorious whistleblower Edward Snowden, more has been revealed about the National Security Agency (NSA)'s clandestine data gathering and surveillance methods in its fight against terrorism. The new information has led to welcome debate to assess and reform the scope of NSA authority and oversight. Despite an unprecedented public defense of its practices by the NSA, as well as President Obama and the Department of Justice (DoJ), the revelations have raised a host of questions about the NSA's activities. In Part One of this feature, Alex Lakatos, Partner at Mayer Brown LLP1, explores the legal underpinnings of the NSA programs and discusses the proposals for reform of the NSA's legal authority now pending before Congress.

The NSA programs

PRISM

PRISM is a tool that allows the NSA to collect and process certain data from USA internet companies, while allowing for ongoing data monitoring and data-pattern analysis.

Nine american internet companies provide the content that PRISM searches and analyzes: Microsoft, Yahoo!, Google, Facebook, PalTalk, YouTube, Skype, and AOL.

Participation is mandatory and legally sanctioned by the Government. The NSA refers to the companies that feed information to PRISM as 'Special Source Operations', and views the tech companies as trusted partners, albeit with a minimal voice in the direction of the operation. About 98% of the data for PRISM comes from just three of them: Google, Yahoo! and Microsoft. By contrast, Twitter has so far refused to provide data for PRISM. It is not readily apparent how long Twitter will be able to hold out if the Government decides to prioritise the acquisition of Twitter's data.

The data that these companies provide includes nearly every form of communication on the internet, including 'metadata'.

While PRISM participants strive to downplay what they are sharing, the NSA and the Obama administration try to emphasize the importance of the data. According to the NSA, for example, each month it generates 2,000 reports based upon PRISM data, with over 77,000 such reports generated to date. The Obama administration further claims that PRISM has helped thwart a number of would-be terrorist attacks. In a recent statement, Director of National Intelligence (DNI), James R. Clapper, said, "information collected under this program is among the most important and valuable foreign intelligence information we collect, and is used to protect our nation from a wide variety of threats".

Upstream

One of Snowden's leaks unveiled an NSA program called 'Upstream', which provides for the '[c]ollection of communications on fiber cables and infrastructure as the data flows past'. In August 2013, the NSA made an unprecedented release of a memo describing and justifying certain aspect of its data collection efforts. The memo indicates that the NSA 'touched' 1.6% of the world's internet traffic and actually read 0.025% of that traffic. It is unknown what the NSA meant by the term 'touched' or how much of the data is collected via Upstream.

As Upstream is not acknowledged by the Obama administration, key questions remain: Does cable tapping occur? If so, to what extent is it limited to communications of persons outside the USA? Moreover, what does the NSA do with the data when it 'touches'?

Phone Records Program

Sometimes mistakenly confused or conflated with PRISM, the phone records program enables the NSA to compel major phone operators to provide metadata for every telephone communication made by their customers. Importantly, the content of the calls or personal information about the caller are not required. It may, however, be possible to infer the general content of the call based on the metadata.

The Obama administration explains that the phone records program 'allows counterterrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, particularly people located inside the United States'. As with PRISM, the Administration has asserted that this program has helped to foil terrorist plots.

Legal authority

PRISM

The stated legal authority for PRISM is Section 702 of the Foreign Intelligence Surveillance Act (FISA), which provides that the Attorney General (AG) and the DNI may jointly authorize for a period of a year the targeting of certain persons for surveillance to acquire foreign intelligence information. The targets must be non-USA citizens who are 'reasonably believed to be located outside the United States'. Blanket authorizations are permissible, meaning broad categories of people can be targeted.

The AG and the DNI can direct a company providing electronic communications services to immediately provide the Government with 'all information, facilities, or assistance necessary to obtain the target's electronic communication', and moreover, to do so 'in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services [being provided] to the target'. The company can seek to appeal or narrow the directive by petitioning the Foreign Intelligence Surveillance Court (FISC) – the court that presides over the Patriot Act surveillance requests in secret proceedings. Many companies do not seek the FISC's input, however.

So long as the target is a foreign national outside of the USA, the Government is likely operating within the letter of Section 702 of FISA. However, that still leaves a lot of room for the data of persons in the USA to get swept up into the PRISM program, an encroachment that the Government dismisses as 'incidental' to its investigations of foreigners. Data from USA citizens can be snared in the PRISM net in several ways. First, although under Section 702, the persons targeted should be outside of the USA, their communications with non-targeted persons in the USA can still be included in the surveillance.

Second, the Government's checks on whether a target is outside of the USA are not particularly rigorous. As long as the NSA certifies that it is 51% confident that its target is a foreign national located outside the country, it may obtain information pursuant to Section 702. It is not entirely clear how the NSA reaches that conclusion. We do know that, as one check, the Federal Bureau of Investigation (FBI) searches its own database to see if the person under investigation is a USA citizen.

Finally, even if the NSA is correct that its target is a foreign national located outside of the USA, that is cold comfort for foreign allies who increasingly resent what some call the USA's digital colonization of foreign sovereigns.

Upstream

Because of the secrecy surrounding Upstream, the basis of the NSA's authority is unknown. One clue leaked by Snowden refers to Section 702 of FISA, the same authority that backs PRISM. That makes sense, given that Upstream – like PRISM – purports to target non-USA communications, and Section 702 of FISA is aimed at such communications. Another possibility is reflected in the memo that the NSA released in August 2013, which cites Executive Order 12333 as the 'foundational authority by which the NSA collects…foreign signal intelligence information.'

Phone Records Program

The NSA obtained telephone data pursuant to Section 215 of the Patriot Act, which allows the NSA (through the FBI) to obtain business records by applying to the FISC for an order for production of data. The FISC may grant the order based on the FBI's certification that the data is to be used for an 'investigation to protect against international terrorism or clandestine intelligence activities'. Originally, Section 215 of the Patriot Act was used to make targeted requests, but starting on 24 May 2006, the FISC began to issue Section 215 orders requiring telecommunications providers to share their entire database of information with the NSA. The order directed to Verizon, for example, requires it to provide an 'electronic copy' of 'all call detail or 'telephony metadata' created by Verizon for communications:

(i) between the USA and abroad; or

(ii) wholly within the USA, including local telephone calls.

This affords the NSA over 100 million Verizon phone records a day. The FISC revisits this type of Section 215 order every three months. The FISC renewed the Verizon order on 19 July 2013, notwithstanding controversy surrounding the NSA phone records program, as well as the ongoing Congressional and public debate over potential reforms.

While the FISC has interpreted Section 215 to allow the NSA to cast a very broad net, it may well have gone beyond anything the Patriot Act's drafters envisioned. Rep. Jim Sensenbrenner (one of the authors of the Patriot Act) expressed the view that the collection of phone records was not "consistent with the requirements of the Patriot Act". More specifically, he stated: "Congress intended to allow the intelligence communities to access targeted information for specific investigations. How can every call that every American makes or receives be relevant to a specific investigation?"

Constitutionality

The Fourth Amendment of the Constitution prohibits unreasonable searches and seizures, and requires any warrant to be judicially sanctioned and supported by probable cause. It is considered as a low standard, and in practice, may allow law enforcement to obtain a warrant for a search as long as it can justifiy that it is more than a 'hunch' or 'gut feeling'. Further, the search and seizure that the court permits should be limited in scope, according to specific information supplied to the issuing court.

Section 702 of FISA, the authority for PRISM, has been criticized as inconsistent with the Fourth Amendment because it does not require a court-approved warrant to obtain data, nor does it require a showing of probable cause. Section 215 of the Patriot Act – the basis for the phone records program – requires a court order to obtain phone records, but it does not require that such orders be granted on a case-by-case basis, nor that the order be based upon a showing of probable cause.

A chief legal argument justifying the constitutionality of these programs is the Supreme Court's position that the Fourth Amendment does not apply to intelligence gathering aimed at foreign sovereigns, rather than at USA citizens who the Constitution is meant to protect. As Margaret Kaminsky,

Executive Director of the Information Society Project at Yale Law School, stated: "foreign intelligence is the exception that has swallowed the Fourth Amendment whole".

Whether various Constitutional challenges to the PRISM and phone records programs prevail has yet to be seen. In the past, similar challenges have often faltered on technical grounds. In any event, the concerns they raise are well-founded and legitimate.

Proposals for reform

A number of bills have been introduced in Congress to roll back the NSA's authority and activities. For example, Rep. Justin Amash (R-MI) proposed legislation that would have defunded the NSA's phone records program, effectively sounding its death knell; however, it would not have affected Section 215 of the Patriot Act. Thus, even if the bill had been enacted, the NSA could still have used Section 215 for other types of investigations. In any event, the Amash amendment was recently defeated in the House of Representatives by a narrow bipartisan 205-217 majority. In the past, similar measures have been defeated by a much wider margin and have split more clearly along party lines, indicating a growing momentum for reform.

The current leading reform proposal in Congress is the FISA Accountability and Privacy Protection Act of 2013, introduced by Sen. Patrick Leahy (D-VT) and co-sponsored by nine senators. The proposal would make a number of narrowly tailored changes to the existing legal framework for NSA activity. It would narrow the scope of Section 215 of the Patriot Act by requiring the Government to produce a statement of facts showing that the information sought is relevant to an authorized investigation and that there is a link to a foreign group or power. The proposal would also allow for greater judicial review of Patriot Act gag orders, and impose an earlier sunset clause, allowing for reexamination of Section 702 of FISA in June 2015 rather than 2017. Leahy's proposal would require the inspector general of the intelligence community to conduct a comprehensive review of the FISA Amendments Act, and its impact on the privacy rights of all Americans. It would further require an unclassified report for the public that would review the impact of the Government's secret surveillance powers on the privacy of Americans. Despite growing momentum for reform, Leahy's ambitious proposal still faces an uphill battle.

Another interesting proposal has been put forward by Rep. Adam B. Schiff (D-CA), a senior member of the House Intelligence Committee. Schiff is pushing for FISC judges to be appointed by the President and confirmed by the Senate. Schiff also supports a plan, advocated by some former FISC judges, to have privacy-focused lawyers before the FISC. Currently, FISC judges hear only from the DoJ.

The most ambitious suggestion, unlikely to gain any traction, is the Surveillance State Repeal Act, introduced by Rep. Rush Holt (D-NJ). That bill proposes to repeal the Patriot Act and the FISA Amendments Act, and would also include, among other things, whistleblower protections for employees of intelligence agencies. Likely seeking to blunt the force of any Congressional action, President Obama announced four reform proposals of his own in August 2013. He proposes:

- working with Congress to amend Section 215 of the Patriot Act to incorporate greater oversight, transparency and constraints on use;
- reforming the FISC to incorporate an adversarial element;
- having the NSA appoint a privacy and civil liberties officer and create a website disclosing more of its activities; and
- creating an independent advisory group of 'outside experts' to review the Government's surveillance activities and publish a public report.

The exact form of the amendment the Administration foresees to Section 215 is unknown. The proposal for reform of the FISC also raises questions, including whether the proposed advocacy for the public's privacy rights would be effective, given the FISC judges' historically pro-surveillance decisions.

Alex Lakatos
Partner
Mayer Brown LLP
alakatos@mayerbrown.com

Footnotes
1. The author would like to thank his partner Jeffery Taft and his associate Matthew Bisanz for their assistance with this article.

This article has been edited for content.