PONDER THE IMPROBABLE

S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 115/2013 dated 24 June 2013

Intelligence-Gathering in the Digital Age: Building Trust in PRISM?

By Damien D. Cheong

Synopsis

A recent poll suggests that the US Government's controversial PRISM programme has some support among Americans. This raises the question of how governments can build trust among its citizenry for modern intelligence-gathering methods that are highly invasive by nature.

Commentary

PRISM IS a covert US Government intelligence-gathering programme designed to carry out surveillance of foreign suspects by analysing their private conversations and/or electronic exchanges made online. Allegedly, access to such data is made either directly through the main servers of the major companies or through a formal channel requesting the required data from such companies. The companies involved are all based in the US, and include Google, Facebook, Microsoft and Yahoo among others. The PRISM programme has reportedly been in operation since 2007.

When news reports revealed two weeks ago that the above-mentioned companies as well as several countries were involved in the PRISM programme, critics were quick to lament the "killing [of] trust in web freedom. They claimed that such intelligence-gathering methods threatened individuals' online privacy as well as raised serious questions about transparency and accountability.

Invasive nature of modern intelligence-gathering

The US government has admitted to the existence of PRISM, but has reassured the public that: (a) PRISM is used only when there is a "valid foreign intelligence purpose; (b) US citizens and individuals based in the US are not "intentionally targeted; (c) companies "supply information to the Government when they are lawfully required to do so; and (d) intelligence-gathering via PRISM is scrutinised by the Executive, Legislative and Judicial branches. As could be expected, critics and naysayers remain unconvinced.

This raises three key questions: (a) should we expect contemporary intelligence-gathering techniques especially those conducted online to be more intrusive?; (b) can a balance ever be struck between privacy and national security concerns?; and (c) how can governments convince their citizens that such activities will not be misused?

Intelligence-gathering post 9-11 has grown increasingly more complex due mainly to the changing nature of contemporary national security threats as well as the corresponding shift in focus from state to non-state actors.

This has resulted not only in an increase in the number of consumers of intelligence but also to the variety and types of intelligence products that are in demand.

As non-state actors are growing more sophisticated, intelligence agencies must likewise improve their tradecraft or better yet, stay ahead of their targets to be effective. A common medium of communication often used by non-state actors is the Internet and social media, and as such, intelligence-gathering has correspondingly shifted into this domain. The need for timely intelligence requires a quick and efficient method to sieve through voluminous Internet traffic and identify relevant data so that analysts can analyse and transform this into information. Hence, new techniques of gathering intelligence online, such as the PRISM programme, have been, and continue to be, developed.

Around the world, intelligence agencies are planning and/or are in the process of improving their online surveillance capabilities. For instance, *Der Spiegel* reports that the German Foreign Intelligence Service (BND) will spend 100 million euro over the next five years to expand its online surveillance programme.

It would be safe to assume that online intelligence-gathering techniques will continue to expand, and be highly intrusive.

Balancing national security concerns

The on-going debate on striking the right balance between privacy and security concerns is unlikely to result in any real breakthrough in the foreseeable future. During times of peace, the debate often skews towards increased protection of individual privacy, whereas in times of conflict/tension, increasing security at the cost of privacy is regarded more favourably. In any case, the reality, as US President Obama has pointed out, is that "it's important to recognise that you can't have 100 per cent security and also then have 100 per cent privacy and zero inconvenience.

Given that online intelligence-gathering techniques are highly intrusive and will continue to raise concerns about privacy issues, it is imperative for the US government and indeed governments around the world to build and enhance their citizens' trust in the system. This will help negate (although not eliminate) the aversion, cynicism and suspicion often associated with intelligence-gathering and intelligence agencies.

In addition to having the necessary checks and balances in place within the system, such as the ability of a citizen to seek legal recourse in the event that his/her privacy has been unnecessarily breached, and the extensive scrutiny by the three branches of government (legislature, executive and judicial), it might be useful to apply the UK think-tank DEMOS' six ethical principles of intelligence-gathering to guide such activities. These principles are:

1: There must be sufficient, sustainable cause;

2: There must be integrity of motive;

3: The methods used must be proportionate and necessary;

4: There must be right authority, validated by external oversight;

5: Recourse to secret intelligence must be a last resort if more open sources can be used; and

6: There must be a reasonable prospect of success.

Seventh principle?

In relation to the PRISM incident, a CNN/ORC poll conducted in the US last week showed that while 61% of American respondents disapproved of how the Obama administration was carrying out surveillance of its citizens in general, 66% did support the government's actions to gather and analyse online data obtained from IT companies provided it was done to "locate suspected terrorists.

The spectre of 9-11 is a contributory factor to this outcome, but more importantly, the statistics seem to suggest that Americans will tolerate breaches of privacy for national security, and that they have sufficient trust in the system – an outcome that governments should aspire to achieve.

The ethical principles mentioned above serve primarily as a guide, and operational realities must also be taken into account. For instance, many intelligence-gathering activities must remain secret as their revelation could jeopardise the individuals, organisations or states involved. Also, open source data may be incomplete and/or inaccurate and therefore must be complemented with closed source data to provide a clearer perspective.

Perhaps in the interests of further transparency and accountability, a seventh principle should be added to the above-mentioned: the need to withhold information must be validated through independent review. Ultimately, intelligence serves to reduce uncertainty in decision-making, and is not meant to be used to victimise particular individuals or groups.

Damien D. Cheong is a Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.