Life through a PRISM: Data Mining, Processing Capacity and Intelligence Gathering

https://www.e-ir.info/2013/07/04/life-through-a-prism-data-mining-processing-capacity-and-intelligence-gathering/

KRISTAN STODDART, JUL 4 2013

In early June 2013 *The Washington Post* and the *Guardian* newspapers ran stories simultaneously on each side of the Atlantic exposing a top secret intelligence gathering operation run by the U.S. National Security Agency (NSA) codenamed *PRISM*.[1] With much of the world's electronic communications routed through the U.S. it was also reported that both the Federal Bureau of Investigation (FBI) and Government Communication Head Quarters in Britain (GCHQ) also had access to the intelligence gathered from PRISM.

The existence and details of PRISM were leaked by the now fugitive whistle-blower, Edward Snowden, who worked for Booz Allen Hamilton. They are one of a number of private security contractors providing outsourced services to the U.S. government begun under the Clinton administration and growing markedly following 9/11.[2] It is alleged the data was harvested from "the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets".[3] The corporations named by the newspapers were Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple with the information shared with GCHQ under the codename *Tempora* through long-standing U.S.-UK intelligence agreements which stretch back to the UKUSA Agreement of 1946.[4] The furor over PRISM followed the disclosure that the U.S. telecommunications company, Verizon, had been required to pass the NSA metadata of the calls it handled, both domestic and international, if either the recipient or destination originated in the U.S.[5]

What is metadata? IBM states that every day 2.5 quintillion bytes of data are created. This constantly rising volume of data is such that "90% of the data in the world today has been created in the last two years alone". This "comes from everywhere: sensors used to gather climate information, posts to social media sites, digital pictures and videos, purchase transaction records, and cell phone GPS signals to name a few. This data is **big data**".[6] This metadata will grow deeper and wider as technology and public consumption develops, driven by increasingly low entry points, storage capacity (particularly through 'Cloud' services), increasing processing capacity and growing sophistication of Artificial Intelligence (AI). AI, such as that demonstrated by IBM's Watson, has the capacity to understand and interpret natural language and speech patterns with a wide variety of applications for many areas of human endeavor and a further step towards the Singularity whereby Artificial Intelligence could match and exceed human intelligence. AI has the capacity to 'join the dots' for the Intelligence Community (IC) in tracking targets and plots through this kind of metadata.[7]

As the New York Times reported "separate streams of data are integrated into large databases – matching, for example, time and location data from cellphones with credit card purposes or E-Zpass use – [through which] intelligence analysts are given a mosaic of a person's life" with only four data points needed from the time and location of a phone call needed to correctly identify a caller 95% of the time.[8] Furthermore the NSA is building a data storage farm in Utah to handle the metadata they are collecting – the latest of tens of NSA facilities spread across America and abroad.[9]

PRISM bears similarities to the Total Information Awareness project rejected by Congress in 2003 and is likely linked with work conducted by the U.S. government's Intelligence Advanced Research Projects Activity (IARPA) established in 2006. Part of their remit is to analyze Open Source intelligence (OPINT) which in conjunction with "14

universities in the United States, Europe, and Israel…[has] the goal of using advanced analytics to predict significant societal events".[10]

"In other words, they are tackling Donald Rumsfeld's infamous "unknown unknowns" problem. If you know what you can predict, then you can predict it; if you know what you can't predict, you can make other plans".[11] Crowdsourcing or to give it a less catchy title, Aggregative Contingent Estimation (ACE), draws on many disciplines and this kind of work has been useful in mapping epidemics and pandemics such as H1N1, and has been used for economic forecasting. However, even with the entire range of metadata available, combined with the analytical processing power now available, Chaos Theory shows that unpredictable minor changes in complex systems can lead to the 'Butterfly Effect'.[12] This undermines the prospects for Total Information Awareness.

Through a U.S. legislative process dating back to 2007 and the George W. Bush administration, the NSA has been able to gather intelligence which, according to testimony from General Keith B. Alexander, the Commander of U.S. Cyber Command and Director of the NSA, have meant, "these programs, together with other intelligence, have protected the U.S. and our allies from terrorist threats across the globe…over fifty times since 9/11…in over twenty countries around the world."[13] Alexander added, "I believe we have achieved this security and relative safety in a way that does not compromise the privacy and civil liberties of our citizens…[and] are critical to the Intelligence Community's efforts to connect the dots."[14]

Mike Rogers, the Chairman of the U.S. House Permanent Select Committee on Intelligence, noted during Alexander's appearance before the Committee in the wake of the PRISM disclosure, the activities of PRISM "are legal, court-approved and are subject to an extensive oversight regime" authorised under Section 702 of the Foreign Intelligence Surveillance Act (FISA) which was passed in 1978.[15] Rogers went on,

One of the frustrating parts about being a member of this Committee is sitting at the intersection of classified intelligence programs and transparent democracy as representatives of the American people. The public trusts the government to protect the country from another 9/11 type attack, but that trust can start to wane when they are faced with inaccuracies, half truths and outright lies about the way intelligence programs are being run.[16]

For Edward Snowden that trust has broken down meaning, "The government has granted itself power it is not entitled to. There is no public oversight. The result is people like myself have the latitude to go further than they are allowed to".[17] Both Alexander and Rogers are acutely aware of the balance between the protection of civil liberties and democratic values, whilst guarding national security. They based their arguments on how PRISM and the wider efforts of the IC have prevented another 9/11 whilst maintaining political and legislative checks through *in camera* provisions from FISA, judicially approved actions and political oversight from the House Permanent Select Committee on Intelligence.

These checks and balances have not prevented foreign governments, many of whom are allied to the U.S., from asking some pertinent questions related to PRISM. For example, German Justice Minister, Sabine Leutheusser-Schnarrenberger, publicly articulated her government's concerns with PRISM. She stated in *Der Spiegel,*

The suspicion of excessive surveillance of communication is so alarming that it cannot be ignored. For that reason, openness and clarification by the US administration itself should be paramount at this point…The global Internet has become indispensable for a competitive economy, the sharing of information and the strengthening of human rights in authoritarian countries. But our trust in these technologies threatens to be lost in the face of comprehensive surveillance activities.[18]

Indeed the right to hold governments to account, governments who are there to protect the citizens of the state, remains very much alive. A number of the principles of the social contract between a state and its citizens are enshrined in the U.S. Declaration of Independence and Constitution, but as Leutheusser-Schnarrenberger (in invoking the latter) also noted,

America has been a different country since the horrible terrorist attacks of Sept. 11, 2001, The relationship between

freedom and security has shifted, to the detriment of freedom, especially as a result of the Patriot Act… We should remember that the strength of the liberal constitutional state lies in the trust of its citizens.[19]

Opposition Social Democrat floor leader, Thomas Oppermann, went further in pointing to the alleged use of PRISM by Britain's GCHQ, when he argued "The accusations make it sound as if George Orwell's surveillance society has become reality in Great Britain".[20] In a country steeped in the memory of state surveillance of its citizens first by the Nazi's and then in East Germany by the Stasi, PRISM has powerful resonance.

The British government has been quick and steadfast in defending the U.S.-UK intelligence sharing arrangement, part of the wider 'Special Relationship', whilst refusing to go into any details regarding PRISM. Following discussions with John Kerry, the U.S. Secretary of State, William Hague, the British Foreign Secretary, stated, "that's something the citizens of both our countries should have confidence in, in particular that that relationship is based on a framework of law in both countries, a law that is vigorously upheld."[21] This has not stopped other governments registering their disquiet.

The remaining partner governments in the UKUSA Agreement (Canada, Australia and New Zealand) have been more muted in condemning PRISM, with a spokesperson for the Communications Security Establishment Canada (CSEC), who monitor and evaluate foreign signals intelligence (SIGINT) and protect Canadian information, communications and technology (ICT), declared that CSEC does not access PRISM.[22] Instead CSEC uses an indigenous, and controversial, intelligence program to gather identical metadata (phone numbers, length and time of calls, email addresses and internet routing information – but not content).[23]

A similarly controversial program was being proposed in Australia but was shelved by the government ahead of the recent election which saw John Rudd succeed Julia Gillard.[24] Although the Gillard government refused to divulge whether Australian intelligence agencies were receiving information gathered via PRISM[25]. Their embarrassment was clear though, as "The US may be able to brush aside some of the diplomatic fallout from the Snowden leak, but that may not be the case for Australia. China, Malaysia, other countries may respond to us in ways that they would not to Washington". It was also judged to "have a much greater and more lasting impact than the Manning leaks" which brought Julian Assange and Wikileaks into the limelight.[26]

Conclusion

As Rhodri Jeffreys-Jones indicated in his recent article in e-IR; against the background of inflated terrorists threats what is needed is "an intelligence arrangement we can trust".[27] We now live in an era of unparalleled peace with a single hegemonic power, the United States, and a series of rising powers, headed by China, leading to a rebalancing of the international system. The prospect of major inter-state war is remote in the extreme at the present time and in structural decline for both established and rising powers.[28] Part of the explanation for this unprecedented stability in the international system is the growing and deepening interdependency between nation-states and the forces of globalization powered and enabled by global and instantaneous communication systems – the most profound of which is the Internet.

Thus there are two major sets of questions which PRISM poses for the U.S., its intelligence partners in the UKUSA ('Five Eyes') agreement and indeed for all liberal democracies. Firstly, at what point does the right to privacy, civil liberties and freedom outweigh the protection of national security and whether, in the nebulous and largely clandestine world these legally mandated intelligence agencies operate in, does democratic oversight go far enough in holding these practices to account? Secondly, a world where everything we say and do online is recorded and analyzed to protect 'us' from 'them' is an Orwellian dystopia that few are likely to advocate whether in public or private. This then leads us all – national governments and their intelligence agencies, and citizens who uphold democratic values, to ponder where the balance should be struck?

—

Kristan Stoddart *is a lecturer in Cyber Security at the Department of International Politics at Aberystwyth*

University, which houses the Cyber Connectivity Research Centre with a new Master's programme 'International Politics of the Internet'.

[1] http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data and http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, accessed 23 June 2013.

[2] See for example Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2009), P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Ithaca: Cornell University Press, 2007) and James Bamford, *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America* (London: Doubleday, 2008).

[3] http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, accessed 23 June 2013. Part of the controversy regarding PRISM is that the NSA also has the capacity to monitor U.S. domestic traffic. See for example James Bamford's article in Wired http://www.wired.com/threatlevel/?p=39308, accessed 2 July 2013.

[4] http://www.nsa.gov/public_info/declass/ukusa.shtml, accessed 1 July 2013.

[5] http://www.bbc.co.uk/news/world-us-canada-22793851, accessed 1 July 2013.

[6] http://www-01.ibm.com/software/data/bigdata/, accessed 1 July 2013.

[7] http://singularityhub.com/2012/10/14/ibms-watson-jeopardy-champ-expands-commercial-applications-aims-to-go-mobile/, accessed 1 July 2013. See also Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York: Penguin, 2006) for a wider appreciation of the subject.

[8] http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html?pagewanted=all&_r=0, accessed 1 July 2013. See also Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel, 'Unique in the Crowd: The privacy bounds of human mobility',*Scientific Reports* 3, Article number 1376.

[9] http://www.sltrib.com/sltrib/politics/56461026-90/nsa-data-utah-center.html.csp?page=2, accessed 1 July 2013.

[10] http://www.businessweek.com/articles/2013-02-05/what-the-intelligence-community-is-doing-with-big-data, accessed 1 July 2013.

[11] http://www.businessweek.com/articles/2013-02-05/what-the-intelligence-community-is-doing-with-big-data, accessed 1 July 2013.

[12] The difficulties for accurately forecasting local, national and global weather being a good example. Edward N. Lorenz, *The Essence of Chaos* (Seattle WA: Washington University Press, 1995).

[13] http://www.whatthefolly.com/2013/06/19/transcript-testimony-of-nsa-director-gen-keith-alexander-before-the-house-intelligence-committee-on-june-18-2013/, accessed 24 June 2013.

[14] Ibid.

[15] http://intelligence.house.gov/hearing/how-disclosed-nsa-programs-protect-americans-and-why-disclosure-aids-our-adversaries, accessed 24 June 2013.

[16] Ibid.

[17] http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, accessed 27 June 2013.

[18] http://www.spiegel.de/international/world/minister-leutheusser-schnarrenberger-criticizes-us-over-prism-scandal-a-905001.html, accessed 27 June 2013.

[19] Ibid.

[20] http://uk.reuters.com/article/2013/06/22/usa-security-britain-germany-idUKL5N0EY09Y20130622, accessed 27 June 2013.

[21] http://www.bbc.co.uk/news/uk-politics-22883340, accessed 27 June 2013.

[22] http://uk.reuters.com/article/2013/06/11/usa-security-canada-idUKL2N0EM1SZ20130611, accessed 27 June 2013.

[23] http://www.huffingtonpost.ca/2013/06/14/what-do-we-know-about-can_n_3440432.html, accessed, 27 June 2013.

[24] http://www.smh.com.au/technology/technology-news/government-shelves-controversial-data-retention-scheme-20130624-2oskq.html, accessed 27 June 2013.

[25] http://www.smh.com.au/opinion/political-news/government-refuses-to-say-if-it-receives-prism-data-20130612-2o3ot.html, accessed 27 June 2013.

[26] http://www.smh.com.au/opinion/political-news/snowden-leaks-may-embarrass-canberra-20130625-2ov4l.html, accessed 27 June 2013. New Zealand Prime Minister, John Key, publicly denied New Zealand national law had been circumvented by access to PRISM". http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10889696, accessed 27 June 2013.

[27] http://www.e-ir.info/2013/06/30/a-critique-of-the-surveillance-flap/, accessed 2 July 2013.

[28] Richard Ned Lebow, *Why Nations Fight: Past and Future Motives for War* (Cambridge: Cambridge University Press, 2010).

About the author:

Kristan Stoddart is a lecturer in Cyber Security at the Department of International Politics at Aberystwyth University, which houses the Cyber Connectivity Research Centre with a new Master's programme 'International Politics of the Internet'.