After PRISM: on Power, Trust and Accountability

Friday 21 June 2013, by HAYES Ben (Date first published: 21 June 2013).

Multinational corporations who dominate large parts of the internet have provided USA's National Security Agency with massive amounts of their users' intimately personal data. This is simply unacceptable in any democracy worthy of the name, argues Ben Hayes.

Edward Snowden's heroic whistle-blowing and the revelation [1] that the USA's National Security Agency (NSA) and its partners have been harvesting the 'metadata' generated by the users of US-based telephone and internet service providers in the absence of probable cause, meaningful due process or public oversight is a damning indictment of the culture and practice of mass surveillance. Privacy is not, however, the most important issue raised by PRISM. As Seamus Milne has reasoned, this dubious accolade goes to the power and the conduct of our most secretive organs of state.

The USA-UK led international intelligence alliance has a long history of untrammelled surveillance and a proclivity for subverting democratically elected governments and countering protest and organised labour movements. Under the 'war on terror', protecting national security has included orchestrated kidnap ('rendition'), torture (by proxy), internment (in Gitmo and in other 'blacksites') and assassinations (by drone). Despite the hope, the transition from Bush to Obama has been seamless. The USA is now the kind of country that people seek asylum from [2].

"The transition from Bush to Obama has been seamless. The USA is now the kind of country that people seek asylum from."

Back in Europe, with the exception of a few honourable parliamentarians, the illegal acts committed by agencies on both sides of the Atlantic have barely raised a murmur in the EU institutions. This is hardly surprising: Council of Europe investigators accused 14 European states of collusion in the US government's rendition and torture programme [3], and seven of 'actual human rights violations'. With 11 member states in the frame, the EU was never going to take the USA to task, let alone reach for the domestic sanctions for 'serious and persistent human breaches' promised by article 7 of the Treaty on European Union [4]. It is hard to be optimistic that this latest abject demonstration of wrongdoing will elicit the response it deserves.

Like the USA, many European states permit their security services to operate in a shadow world: beyond the reach of the law, cloaked in secrecy and in contempt for the sovereignty of other nations. Given these pre-conditions, we shouldn't be at all surprised that these agencies break the law (and the PRISM revelations came as little or no surprise to seasoned observers) [5], only that we find out.

Following such disclosures, the reflex of government is to defend the indefensible, pre-empting and effectively closing the door to much needed debates how to bring the agencies under proper judicial and democratic control. This impunity is the lifeblood of criminal state enterprises like PRISM and the reason that agencies like the NSA and its UK partner GCHQ (and their misnomered 'political masters') are prepared to disregard people's fundamental rights at the drop of a terrorist's hat. And

the longer the secret intelligence services have gotten away with it, the more the 'intelligence-led' approach [6] contaminates the work of the ordinary police who, like the spooks, inevitably end up bugging, snooping and surveilling just because they can [7].

Collusion and compulsion

The staggering overreach of the NSA has been laid plain for all to see. But questions remain about the precise role that the companies whose data was the lifeblood of PRISM (in order of appearance: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL and Apple) played in facilitating the mass surveillance of their customers. Their similarly worded denials of any wrongdoing or knowledge of PRISM [8] rest on the premise that they did not provide the NSA with 'direct access' to their servers and that they only ever disclose data about their users in compliance with US law.

Both of these claims are certainly true in the technical sense. As Chris Soghoian [9] of the ACLU has pointed out [10], the NSA needs neither a 'backdoor' or 'direct access' to collect all of the data from all of the servers because there are other ways and means to do this. Others have come to the absurd conclusion that the *Guardian*'s Glenn Greenwald (who broke the story) was guilty of an 'epic botch' in his reporting [11].

Regardless, the central tenet of the PRISM story remains: the multinational corporations who dominate large parts of the internet have apparently provided the NSA with massive amounts of their users' intimately personal data [12] and this is simply unacceptable in any democracy worthy of the name. As to the companies' claims that they fully comply with US law, the Verizon leak shows that it was secretly compelled to provide the NSA with all of the metadata relating to all of the phone calls within, from and to the United States [13], rendering the relevant laws and their supposed due process a joke. And let's not forget the most compelling testimony of all: that of Edward Snowden [14].

The mantra was old Silicon Valley: we will protect you from your governments (even if they won't protect you from us).

Ironically, a growing coalition of internet behemoths had appeared to be pushing back, albeit modestly, on 'lawful access' regimes. Google was among the first to start issuing transparency reports [15] showing which governments were asking for the most data and how often such data was released (though it never mentioned the NSA requests). The aim was to convince users that they were sticking up for their rights by holding governments to account and properly scrutinizing their every request. The mantra was old Silicon Valley: we will protect you from your governments (even if they won't protect you from us). They even engaged with privacy experts to help produce a commendable set of principles for legitimate access to metadata by police and security agencies when combating serious crime [16].

PRISM has left the Emperor with no clothes. In their defence the companies are legally compelled to respect the veil of official secrecy covering activities of the intelligence services. They maintain that they have 'consistently pushed back on overly broad government requests for users' data' and requested the US government to allow them to disclose the number and scope of NSA requests 'to the help the community understand and debate these important issues' [17]. Not exactly inspiring, but something has to give.

Ben Hayes

P.S.

* From TNI, 21 June 2013:
http://www.tni.org/article/after-prism-power-trust-and-accountability

* Ben Hayes is a TNI fellow who has worked for the civil liberties organisation Statewatch since 1996, specialising in international and national security and policing policies. Ben also works as an independent researcher and consultant for organisations including the European Centre for Constitutional and Human Rights, Cordaid, the Heinrich Boll Foundation, the European Parliament and European Commission.

Ben's research has two main focuses: (i) the impact of counter-terrorism, surveillance and border control policies on democracy, human rights, civil society and international development, (ii) the influence and activities of the defence and security industries.

Ben has a PhD from Magee College (Derry/Londonderry) awarded by the University of Ulster in 2008. He is currently working on a book on climate change and international security for TNI.

Footnotes

[1] See on ESSF (article 28879), 'Prism': A massive internet spying scheme by U.S. government is revealed.

[2] http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/09/has-the-us-become-the-kind-of-nation-from-which-you-have-to-seek-asylum/

[3] http://assembly.coe.int/Main.asp?Link=/CommitteeDocs/2006/20060606_Ejdoc162006PartII-FINAL.htm

[4] http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/l33500_en.htm

[5] http://www.psmag.com/politics/a-security-scholar-talks-the-nsa-scandal-59964/

[6] http://innovative-analytics.com/docs/IntelligenceLedPolicing.pdf

[7] http://www.guardian.co.uk/world/defence-and-security-blog/2013/jun/17/spying-spooks-intelligence-addiction?CMP=twt_gu

[8] http://www.guardian.co.uk/world/2013/jun/07/google-facebook-prism-surveillance-program

[9] http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf

[10] http://news.yahoo.com/improved-facebook-google-statements-prism-still-holes-222735735.html

[11] http://www.thenation.com/blog/174783/glenn-greenwalds-epic-botch#axzz2Wjh2Q6ay

[12] http://www.washingtonsblog.com/2013/06/metadata-can-tell-the-government-more-about-you-than-the-content-of-your-phonecalls.html

[13] http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order

[14] See on ESSF (article 28898), USA/NSA – Edward Snowden: The man who revealed Prism.

[15] http://www.google.com/transparencyreport/userdatarequests/

[16] http://necessaryandproportionate.net/

[17] http://business.time.com/2013/06/11/google-were-no-nsa-stooge-and-well-prove-it-if-the-feds-let-us/