The World's Second Oldest Profession: The Transatlantic Spying Scandal and its Aftermath

Robert Dover

The revelations from the former National Security Agency contractor, Edward Snowden, in July 2013 will have an enduring impact on the modern business of intelligence and the communication strategies of governments and non-state based adversaries alike. Snowden's revelations do not mark a fundamental divergence from the general understanding of intelligence. In making these implied understandings public, however, Snowden has changed the political dynamic around mass surveillance. The revelations amplify a tension within several layers of social contract from interactions between governments to those between governments and citizens. Long-term, diplomatic relations between the US and European governments should remain largely unaffected.

Keywords: National Security Agency, intelligence, surveillance, legitimacy

> What you have said in the dark will be heard in the daylight, and what you have whispered in the ear in the inner rooms will be proclaimed from the roofs.[1]
>
> The Gospel of Luke, 12:3.

Be he a fugitive or a whistle-blower, the former National Security Agency (NSA) analyst Edward Snowden has generated a sizeable quantity of commentary and (one can predict) an enduring impact on the modern business of intelligence and the communication strategies of governments and non-state based adversaries alike. This article makes two broad claims: it argues 1) that Snowden's revelations about intrusive intelligence efforts by governments should not mark a fundamental divergence from our understanding of these activities prior to his disclosure of sensitive materials. However, in making these implied understandings public, Snowden and his media partners have changed the political dynamic around mass surveillance and dramatically scaled up public understanding of this area; and 2) that the

Robert Dover is Senior Lecturer in International Relations and Associate Dean (Enterprise), Loughborough University. Email: r.m.dover@lboro.ac.uk. The author would like to thank Erik Jones and Friederike Rehn for comments on the earliest draft of the paper, and for three anonymous reviewers for their comments and suggestions.

[1]The author is indebted to his colleague, Jon Walker, for bringing this biblical quote to his attention.

The International Spectator, Vol. 49, No. 2, June 2014, 117–133 ISSN 0393-2729 print/ISSN 1751-9721 online

http://dx.doi.org/10.1080/03932729.2014.904989

revelations both highlight and reflect a tension within several layers of social ontract: between allied governments and international organisations, and between citizens and their governments. The diplomatic relations between the US and European governments will remain largely unaffected. The European states loudly complaining about American intelligence are themselves full spectrum intelligence actors, and so also engaged in this range of activities. The complaints are mostly aimed in three directions: tangential negotiations, such as the EU–US trade negotiations (Transatlantic Trade and Investment Partnership, TTIP), scaling back US efforts for competitive advantage, and responding to public sentiment.

The EU institutions are genuinely affronted about intelligence efforts against their communications and the revelations may impact on the international trade negotiations, in which data protection is now likely to feature, and on existing data protection agreements, which the European Commission would like to reopen.[2] In the realm of public perception of and confidence in security and intelligence, the Snowden affair will do enduring harm unless governments can find a way to re-establish public support. To provide coverage of these issues, this article is divided broadly into three sections: the first checks and challenges the continuity and change points around the activities of the NSA (and its allies) and the observable diplomatic aftermath; the second section explores the impact Snowden has had on the social contract, whilst the third and final section summarises where the enduring and transient legacies from this affair lie.

Business as usual in the dark corridors

The key argument of this section is that the behaviour that the Snowden information uncovered should be neither surprising nor unexpected.[3] Furthermore, it can be argued – with a high degree of certainty – that the response of a large number of European states to this information was nothing short of hypocritical, much as the pan-European response to rendition, or the kidnapping of terrorism suspects, was hypocritical some years ago.[4] As with rendition, a large number of European states had been actively complicit in the PRISM program, taking participation far beyond mere acquiescence. But it is politically untenable for European governments to be relaxed about the NSA engaging in aggressive surveillance of political leaders, even if it was privately well known. The Americans were essentially 'outed', but from a European perspective thankfully by an American, much as they had been in the 1971 *Pentagon Papers* scandal, which bears similar characteristics. The repercussions for any non-US country, had their citizen been the source, would

[2]J. Fontanella-Khan, "Brussels Considers Options to Respond to NSA Spying Scandal", *Financial Times*, 26 November 2013.
[3]For archives of synthesised Snowden material, refer to *The Guardian*, http://www.theguardian.com/world/the-nsa-files, and the *Financial Times*, http://www.ft.com/indepth/us-security-state.
[4]Grey, *Ghost Plane*.

have been severe and enduring. Evidence for this as a generalizable assertion comes from the removal of intelligence product (e.g. raw or analysed information) from the UK following the Klaus Fuchs scandal concerning nuclear technologies,[5] the aftermath of the Cambridge Spy Ring, and the activities of Kim Philby, in particular,[6] and the repercussions for French military intelligence of having provided guidance in Belgrade in targeting what transpired to be the Chinese Embassy.[7] It simply does not pay to embarrass the world's pre-eminent intelligence nation.

A key element of the Snowden revelations has been to demonstrate the closely interconnected workings of the US via the NSA and friendly intelligence services abroad in controlling the development of mass surveillance techniques. Similarly it has now been shown that these nations (in particular Britain, France, Germany, Spain and Sweden) have liaised to manoeuvre around the spirit of established laws, or the legislators' intentions for the law via intelligence liaison practice.[8] That liaison mechanisms have been allowed to be used in this way has been overtly or tacitly approved at government level, so it is for political parties to respond to the aggregated pressure from their electorates on this issue. Similarly, it had been thought that the so-called 'Five Eyes' group, established in 1946,[9] had imposed upon itself a rule that stated that each other's citizens were off-limits for surveillance activity, whilst a 2005 amendment moved this understanding to a derogation where it is in the national security interests of the primary party. Documents leaked by Snowden to *The Guardian* newspaper in the UK showed that this rule was breached by consent from British intelligence officials in 2007. The memorandum – reprinted in *The Guardian* on 20 November 2013 – stated that:

> Sigint [signals intelligence] policy … and the UK Liaison Office here at NSAW [NSA Washington] worked together to come up with a new policy that expands the use of incidentally collected unminimized[10] UK data in Sigint analysis. …The new policy expands the previous memo issued in 2004 that only allowed the unminimizing of incidentally collected UK phone numbers for use in analysis ... now SID analysts can unminimize all incidentally collected UK contact identifiers, including IP and email addresses, fax and cell phone numbers, for use in analysis.[11]

---

[5]Goodman, "Klaus Fuchs and Anglo-American Intelligence".
[6]Jeffreys-Jones, "End of an Exclusive Intelligence Relationship".
[7]Mandelbaum, "Perfect Failure".
[8]J. Borger, "GCHQ and European Spy Agencies Worked Together on Mass Surveillance", *The Guardian,* 1 November 2013.
[9]The five countries (or Eyes) are Australia, Canada, New Zealand, United Kingdom, United States of America, and the group's mission is to facilitate enhanced levels of intelligence sharing between these nations. This arrangement springs from an agreement struck in 1946, and whilst there are five lead members, other nations, including Germany and Sweden, have found themselves on the periphery of the group. Until the Snowden revelations, it was thought that the group operated a 'no-spy' arrangement against each other.
[10]The term 'minimize' in this context means the removal of records from the NSA archive.
[11]J. Ball, "US and UK Struck Secret Deal to Allow NSA to 'Unmask' Britons' Personal Data", *The Guardian*, 20 November 2013.

So, whilst the NSA can still not explicitly target a British citizen without a warrant, it may do so if it collects the data 'incidentally', which means in the course of an investigation into a warranted suspect or target. As such, many British citizens with, for example, connections with Pakistani nationals at the fringes of fundamentalist forms of Islam, would be caught by the 'three hops' rule, or three degrees of separation, which would capture a significant percentage of a target audience with non-UK based contacts (and who themselves could be subject to an indiscriminate haul). Thus within the somewhat wide provision of the three degrees of separation (where patterns of life or contacts chain analysis is used), a large number of British citizens have had their communications data stored and analysed by the NSA, under US rules, with the agreement of British intelligence officials.[12] This runs somewhat contrary to the statement made by the British Foreign Secretary, William Hague, in Parliament on 10 June 2013:

> It has been suggested GCHQ uses our partnership with the United States to get around UK law, obtaining information that they cannot legally obtain in the UK. I wish to be absolutely clear that this accusation is baseless. Any data obtained by us from the US involving UK nationals is subject to proper UK statutory controls and safeguards.[13]

It is quite difficult to see how this statement tallies with the agreement that Snowden's leak suggests is in place between UK and US intelligence officials, even if only within the spirit of the words spoken.

Political ownership

One aspect of the internal positioning of the agreements between the UK and US agencies that is not clear is whether British intelligence officials kept their political masters informed of the minutiae of this detailing or whether, as the British Foreign Minister said in answer to questions on this very topic, he and the Home Secretary make decisions on this area with the intelligence commissioners and thus it remains outside of wider government.[14] Such a stove-piping of information about issues that have strong public interest and public policy resonance would seem alien in almost any other area of government activity: the agenda to normalise the understanding of intelligence within bureaucratic frames of reference, typified by the work of Peter Gill is placed under serious tension by these more recent activities.[15] It also raises

[12]It should be noted, however, that a 2005 NSA document 'Collection, Processing and Dissemination of Allied Communications', also stated that it should be possible for the US to spy on the citizens of the Five Eyes nations without the permission of those nations, and without them being notified that the activity was occurring.

[13]W. Hague, *Foreign Secretary Statement to the House of Commons – GCHQ*. 10 June 2013, https://www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq.

[14]A. Sparrow, "Guardian Faces Fresh Criticism over Edward Snowden Revelations", *The Guardian*, 10 November 2013.

[15]Gill, *Policing Politics*.

questions over the extent to which intelligence activity is even tangentially accountable to the citizenry, which will be addressed at greater length later in this article.

The flow of information about the operational aspects of intelligence policy and a more general flow of information around intelligence communities is highly and deliberately constrained, not just in the UK but across European capitals. This is partly on the grounds of operational and information security, but mostly to provide the widest scope for intelligence officers and assets to operate unmolested by adversaries. It is therefore accurate to see intelligence as an exceptional area of diplomacy where oversight and political control are looser than one might find in almost every other area of government activity.[16] This works well in terms of efficiency, but poorly when it comes to a divergence in government and public expectations. European publics (and their political masters for that matter) have been shocked and surprised to discover that oversight mechanisms can be observed to have been successful and effective, whilst simultaneously providing a backdrop to ubiquitous dragnet surveillance.[17] Thus it would be wrong to describe parliamentary oversight as having failed, but it is simply that systems of oversight have been given underspecified powers, particularly in those nations with highly developed capabilities. As such, a public discourse has emerged in which both intelligence and the political oversight of intelligence have become separated or disconnected from the publics these agencies serve. For the future efficacy of intelligence activity, it is important that this disconnect be quickly bridged by improving legal powers to question and secure evidence and by publishing reports that can be quickly understood by the public in direct form (e.g. from parliamentary web-sources) or via media filters.

Diplomatic antecedents and impacts

The focus of attention upon the two leading countries of the 'Five Eyes' Group, the UK and the US, has also allowed capable states, such as France, Germany and Spain to complain that these activities have been done to them, overlooking the fact that they were involved in this range of activities, and indeed shaping the political and legal landscape to further their reach. So, for example, in late 2013, France, Germany and Spain all summoned their respective US ambassadors to discuss surveillance within their borders, whilst in November 2013 the UK ambassador to Germany was invited to discuss alleged eavesdropping from the UK embassy in Berlin, an operation which – on the face of it – did not look particularly sophisticated.[18] It is possible to observe a strong resonance between the European countries' reactions to PRISM and associated programmes and their

[16]Bochel *et al*., "New Mechanisms of Independent Accountability".
[17]V. Medick and A. Meiritz, "NSA Scandal: Parliamentary Spying Inquiry Poses Challenges", *Der Speigel Online,* 29 October 2013.
[18]"Et Tu, UK? Anger Grows over British Spying in Berlin", *Der Spiegel Online*, 5 November 2013.

reaction to the breaking stories around the US policy of so-called 'rendition' (or extra-judicial kidnapping) after 2003.

European states keenly reacted to rendition with horror that a shadow system of prisons and extra-judicial activity could be in place and active. But it then became clear, in a way that never received a similar level of public exposure, that these same European states – and 11 were cited by the European Parliament – were at least knowledgeably complicit in rendition, and that some had been actively involved.[19] Such complicity ranged from providing overflight rights to the 1245 rendition flights identified by the European Parliament, a smaller number of refuelling rights to the small jets transporting captives from one facility to another,[20] through to providing information that led to the original 'rendering' or information which allegedly contributed to the questioning-under-duress of those captives.[21] The European Court of Human Rights in Strasbourg is waiting to hear cases on what they have described as "the lawlessness that characterised the CIA [rendition] programme" that emanate from Germany, Poland, Lithuania and Romania.[22]

The diplomatic impact of the NSA's activities seems starkest in Germany, France and Spain. The allegations that German Chancellor Angela Merkel's personal phone had been intercepted caused genuine anger in Germany.[23] US President Barack Obama had somewhat unwisely stated in July 2013 that "Here's one last thing. I'm the end user of this kind of intelligence. And if I want to know what Chancellor Merkel is thinking, I will call Chancellor Merkel", which seemed to imply – by the time the news broke in October – that either he was not telling the truth, or that he was unaware that this surveillance was going on.[24] Chancellor Merkel let it be known that she viewed this activity as "a grave breach of trust", and opinion polls indicated both that German public confidence in the US as an

[19]Fava, *Report on Alleged Use of European Countries.*

[20]It found: Cyprus: 57 stopovers; Germany: 336 stopovers; Greece: 64 stopovers; Ireland: 147 stopovers; Italy: 46 stopovers, Poland: 11 stopovers; Portugal: 91 stopovers; Romania: 21 stopovers; Spain: 68 stopovers; United Kingdom: 170 stopovers.

[21]N. Muižnieks, *Time for Accountability in CIA Torture Cases*, Council of Europe's Commissioner for Human Rights, 11 September 2013, http://humanrightscomment.org/2013/09/11/time-for-accountability-in-cia-torture-cases/ So, for example, in the case of the Libyan national Sami al-Saadi, the UK government paid an out-of-court settlement to him of £2.5million, whilst not admitting liability in answer to his civil action claiming that MI6 (SIS) had been instrumental in his rendition.

[22]D. Casciani, "UK Pays £2.2m to Settle Libyan Rendition Claim", *BBC News*, 13 Dec. 2012.

[23]C. Lane, "NSA's Spying Humiliates Germany, Again", *Washington Post*, 5 November 2013, http://www.washingtonpost.com/opinions/charles-lane-nsas-spying-humiliates-germany-again/2013/11/04/f13eba14-456d-11e3-b6f8-3782ff6cb769_story.html.

[24]B. Obama, *Remarks by President Obama and President Kikwete of Tanzania at Joint Press Conference*, The White House, 1 July 2013, http://www.whitehouse.gov/the-press-office/2013/07/01/remarks-president-obama-and-president-kikwete-tanzania-joint-press-confe.

ally had dropped (down some 14 percent in three months) and that 92 percent of Germans were in favour of a 'no-spy' treaty as a result.[25]

It was not just from the German government, however, that the Americans received diplomatic complaints. The European Union institutions complained bitterly about their offices and communications being intercepted, whilst the French President François Hollande phoned President Obama to complain about the revelations that 70.3 million incidents of telephone communication had been collected in France against French citizens between 10 December 2012 and 8 January 2013, suggesting a huge amount of activity. Indeed, the American ambassador was called in to account for this level of surveillance.[26] Of particular concern to the French authorities was that the surveillance net had been cast far wider than those suspected of terrorist offences or seeking to injure American interests: collection also targeted French political and business communities – a strong resonance with the pattern of behaviour around ECHELON.[27]

So, the key question that emerges from this is the degree to which real disruption to diplomatic flows has occurred. It is difficult to measure this in a scientific way, particularly so close to the events unfolding. It is possible to judge that there is a degree of positioning and hypocrisy to the condemnations: both France and Germany in particular have fully functioning espionage activities, and the French are considered to be the most active of the Western nations in espionage in the US itself. So, strong condemnations are partly for the purposes of counter-espionage: an attempt to disrupt US activity. Similarly, the condemnation may serve another purpose: in the case of France, President Hollande has implied a threat against the comprehensive trade agreement being negotiated between the EU and the US (the TTIP), so part of this positioning can be seen as an attempt to reduce the negotiating power of the US. Surveillance done against the European institutions will almost inevitably feature in how they approach these negotiations too, and the European Commission has stated that it wishes to reopen negotiations on data-sharing with the US and to insert 'anti-snooping measures' into the TTIP. European parliamentarians have also called for a suspension of financial data sharing with the US in retaliation.[28] So across Europe, the reactions to the Snowden revelations are in line with general dispositions towards the US, save for Germany which responded with greater anger than could have been predicted in July 2013.

---

[25]"Germans' Trust in US Plummets in Wake of Spying Scandal", *Deutsche Welle*, 8 November 2013, http://www.dw.de/germans-trust-in-us-plummets-in-wake-of-spying-scandal/a-17213441.

[26]J. Follorou and G. Greenwald, "France in the NSA's Crosshair: Phone Networks under Surveillance", *Le Monde*, 21 Oct. 2013.

[27]More details on ECHELON are given in a later section of this article.

[28]J. Fontanella-Khan, "Brussels Considers Options to Respond to NSA Spying Scandal", *Financial Times*, 26 November 2013.

Comforting the enemy?

A strong part of the official discourse surrounding the Snowden leaks was, firstly, that they gave 'comfort to the enemy', and it was on this basis that the some in the US wanted Snowden extradited back to the US, and secondly, that the revelations around US tactics and capabilities would give current and future belligerents a competitive advantage.[29] Of all the things said about these leaks, these are the least persuasive. Those involved in serious activities against Western interests would already be acutely aware of the insecurity of electronic communications and data trails. This is why jihadists at various stages during the 2000s switched to small, cellular structures, away from telecommunications, to voice-over-internet-protocol communications, to 'burner phones', and satellite phones, from electronic money transfers and bank-holdings to cash-passed-on in person and, in the case of bin Laden, to accommodations with high walls, and cloth drapes for outside shade to evade overhead surveillance – no longer out in the wilderness but conspicuously in the suburbs, just away from the prying overhead eye. So, those engaged in these activities in a serious way would already have been avoiding (as far as they could) the techniques being deployed by the US and allies. Those self-radicalising or partaking in less well planned activities might have gained some kind of additional wisdom, but the actual risk or threat posed by these actors is difficult to assess and is likely to be small.

The invocation of 'giving comfort to the enemy' is geared more towards its public relations impact: the positioning of Snowden as a whistle-blower (while to some he is a heroic sacrificial figure) was addressed – in part – by seeking to appeal to patriotic sentiment: 'comfort to the enemy' constructs Snowden as *them,* helping *them*, against the interests of *us*. That the *them* might be better equipped to strike *us* is a strengthened version of the same rhetorical device. That a significant proportion of the public across North America and Europe viewed the NSA's activities as being targeted at them has reduced the usual traction such a message would have received.

The other example of where such rhetoric was used was in the 1971 *Pentagon Papers* scandal, where Daniel Ellsberg photocopied the secret internal review papers of the Vietnam conflict and delivered them to the *New York Times* and the *Washington Post* because he felt the US government had lied to the public about the purpose and conduct of the war. Ellsberg and Snowden were similar in their tactic of using multiple news agencies to disseminate their leaks, thus reducing the prospect of suppression, as was attempted in the case of the Pentagon Papers.[30] They were also similar in passing on primary evidence to these news organisations:

[29]B. Keller, "Manning and Snowden", *The New York Times*, 30 July 2013, http://keller.blogs.nytimes.com/2013/07/30/manning-and-snowden/?_r=0.
[30]New York Times Co. v. United States, 403 U.S. 713 (1971).

Ellsberg with Xeroxed copies, Snowden with digital copies, but to the same effect.[31] Finally, with both the Ellsberg and Snowden leaks, only a tiny proportion of this material made it into the public realm, and thus both are of a different character to the Wikileaks *Cablegate* episode, but both have arguably had a far more significant impact.

'If you've got nothing to hide…': the transformation in the social contract

The main argument of this section is that these revelations of the activities of the large and capable intelligence organisations in the developed world, and particularly the NSA and Government Communications Headquarters (GCHQ), have had the impact of perturbing the diplomatic system in the short-term, but for the ordinary public they have the capacity to drive a larger wedge between the governmental elites and the populous.

In his interview evidence to *The Guardian,* Edward Snowden said the following (and this provides the principle driver for his actions in leaking the material):

> Even if you're not doing anything wrong you're being watched and recorded… The storage capability of these systems increases every year consistently by orders of magnitude to where it's getting to the point – you don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody, even by a wrong call. And then they can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with. And attack you on that basis to sort of derive suspicion from an innocent life paint anyone in the context of a wrongdoer.[32]

This is the logic of the panoptican and, within popular political discourse, it is the logic of totalitarian states that the democratic world are said to oppose. It is within this central irony of democratic states adopting the tools and methods of autocracy to protect freedom that the core political problem appears, and within two main modes of transmission: 1) a simple political divergence that is based on a failure of expectations e.g. we thought that the core values of these services were x, and they appear to be y, and 2) a psychological process that is akin to criminalisation, which means the observable process by which individuals become desensitised to certain types of criminal activity. The most obvious 'benign' examples are paying for services in cash to avoid taxation, or downloading music from peer-to-peer websites, or speeding on the highway. The ubiquity of these activities gradually places the individual outside of the frame of certain laws – which have uneven patterns of

[31]Ellsberg, *Secrets.*

[32]E. Snowden, *Full Interview With NSA Whistleblower Edward Snowden*, 9 June 2013, YouTube, http://www.youtube.com/watch?v=bdPbvKeRgpk.

enforcement – and eventually blurs the line between those who are law-abiding and those who hold a 'pragmatic' view of the sanctity of the law.[33]

A similar phenomenon can be seen to be emerging with reference to intelligence agencies. Part of the observation is analogous, and is captured by communities using alternative internet services, such as 'Tor', an online anonymity service established in 2002, that was partly funded by US government monies in its initial phase, which allows users to evade the normal surveillance over their internet activities.[34] Typical users are those in sensitive professions (journalists, military personnel and business people), as well as those which an NSA official recently called "very naughty", by which he meant criminals.[35] The debate in the UK around Tor and services using the Tor architecture has focussed in on the 'naughty' elements of it, as an allegedly permissive environment for child pornographers, drug smugglers and others intent on criminal activity.[36] The political discourse around Tor, that if there is not unfettered access to it for security officials then 'bad things will happen', misses out on the reality that criminals are good at adopting multiple, fluid identities with or without Tor, and that the Tor services are used by legitimate users seeking internet anonymity, up to and including dissidents in developing countries whom Americans and their European allies support. The official response to Tor is informative though: it is an ungovernable cyber-space generating a large amount of anxiety in security and political circles (and, we learn, particularly the NSA), resulting in a strong dominant discourse around deviance.[37] If one were to poll those who have read media coverage of the Tor service, one would assume that it was essentially criminal in character. This is a clear attempt to shape politics and to curtail certain kinds of lawful activities and speech-acts. But it should also be noted that those using Tor and related services have rapidly increased since July 2013, suggesting there is a strong demand for these kind of services currently.

The one percent doctrine and electoral disillusionment

The attempts to unveil the identities of Tor users and to survey their activities also points to a continuation of the famous 1 percent doctrine (also known as the Cheney Doctrine), whereby government action was deemed justified if there was just a 1 percent chance of a threat being realised: the emphasis was on the response

[33]Corbett and Grayson, "Speed Limit Enforcement".
[34]Soghoian, "Enforced Community Standards".
[35]S. Dredge, "What is Tor? A beginner's guide to the privacy tool", *The Guardian*, 5 November 2013, http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser.
[36]J. Smith, *Hansard*, 31 October 2013, http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm#13103154000305.
[37]B. Schnier, "Attacking TOR: How the NSA attacks online users' anonymity", *The Guardian*, 4 October 2013, http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

rather than the threat.[38] The impact on the public of the 1 percent doctrine, or variations of it, is that rather than being protected by government agencies, the public are the object of their attentions and that shift in emphasis is crucial in understanding a recasting of the social contract between state and citizenry. In a British context, this is simply expressed in using an imperial and post-imperial frame of reference: *we* are happy that security measures are taken against *them*, in order to protect *us*. But if we run the same basic sentence and premise under what we now know, post-Snowden, it becomes 'security measures are taken against *us and them*, in order to protect *us* from *them*. The astute reader will see that the definitional clarity of the first sentence (even if socially constructed) is lost in the second sentence where the identity of *us* and *them* is entirely merged. There is thus the potential for an uneasily, or unintentionally aligned coalition of *us and them* to emerge, which sees security and intelligence efforts in an adversarial guise. Such a coalition, if allowed to persist, would put the fundamental social contract of the public offering up their unfettered freedom of action for a security guarantee from the state under question.

An adversarial relationship between intelligence agencies and the citizenry are not emerging in a vacuum, however, and it is more worryingly replicated in the drift away from mainstream political processes and towards the politics of protest and radicalism. Classically, this was typified by a soft correlation between the reduction in popular participation in political parties and election turnout, and an increase in participation in interest groups.[39] More recently, and particularly since the economic crisis of 2007-08, this has dovetailed with the emergence of consistent opinion poll data suggesting a disillusionment with the political establishment as a class or activity, put alongside corporate financiers as part of a coupled elite.[40] Put more simply, there is a growing trend to think that these elites have 'nothing to do with us', and 'do not work in our interests'. There are many possible responses governments could take to this, including out-reach efforts and efforts in transparency. The most productive route for governments will be mild reform, including more overt and publicised oversight mechanisms and a long period of time without adverse publicity.

An unchallenged past? Echoes of ECHELON

The revelations around the ECHELON programme, first brought to light by investigative journalist Duncan Campbell in 1988, via a former employee at the UK's main listening station Menwith Hill, brings further weight to the argument that the real transformation from the Snowden leak is the switch from targeted

[38]Suskind, *The One Percent Doctrine*.
[39]Richardson, "The Market for Political Activism".
[40]Flinders and Kelso, "Mind the Gap".

intrusive surveillance to ubiquitous or dragnet surveillance that moves *us* into being part of *them*.[41] ECHELON was an electronic and signals interception programme, with global reach, run by the Five Eyes members, the data from which was analysed, stored in, and disseminated from the NSA.[42] When triggered by particular words, names or other search terms, the ECHELON system intercepted communications from the two main communications satellites (Intelsat and Inmarsat), through which public, business and government telephone calls and fax messages were communicated. As William Studeman, former NSA Director, noted in 1992 about the amount of useful intelligence gathered in this way:

> One intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence.[43]

In a direct echo to the Snowden papers and PRISM, the defence of ECHELON was that it did not intercept a particular target's communications, but that it focussed on target phrases and patterns and that individuals were thus identified as a by-product of those sifts. The defence of PRISM is that it collects meta-data, from which targets may be selected for closer attention, or that is then sifted once a target has been identified. ECHELON did not attract the public attention that Snowden and PRISM has. This may be due – in part – to the reliance at the time on print, radio and non-24 hour rolling news outputs for dissemination of such messages. An analogue era compared to the ubiquity of social media and internet delivered news content today, but a more likely explanation is that ECHELON did not target the ordinary citizen on a wide scale.

The most active organisation in Europe on the question and dangers of ECHELON was the European Parliament, whose members were particularly concerned about the potential advantages America was gaining via interceptions of the positioning, commercial manoeuvres and negotiations of European business interests. Two of the stronger research papers on ECHELON commissioned by the European Parliament were written by Duncan Campbell, who had originally broken the story, and Dick Holdsworth, who was the first to point out the economic espionage possibilities from NSA stations in Europe.[44] However, the marginal position of the European Parliament at the time, prior to the Lisbon reforms, was a hindrance to the widening of opposition to invasive surveillance techniques and practices, and may have contributed to giving American security officials a sense that

[41]Campbell, "They've got it Taped".
[42]Webb, "ECHELON and the NSA".
[43]W. Studeman, Address to the Symposium on "National Security and National Competitiveness: Open Source Solutions", McLean, Virginia, 1992.
[44]Campbell, *Interception Capabilities 2000*, and Holdsworth, *Development of Surveillance Technology*.

there was little in the way of significant opposition to them expanding these activities. It should also be remembered that the Europeanisation of security and defence (by no means fully developed now) was almost totally absent in 1999 and 2000, and so was that of a competency that was vested in member governments, some of whom were involved in the delivery of ECHELON, whilst others were passive landlords to collecting stations: there was little appetite at a state level to generate adverse commentary about this programme.

Summary remarks: A lot of rhetoric and positioning, but some real damage too

From an area of government activity that was largely anonymous prior to 2001, "the hidden wiring" of governments, as Peter Hennessy famously called intelligence, has been a constant presence in all forms of news media and popular culture since.[45] The aftermath of the 2013 Snowden revelations has amplified intelligence as a prominent government function even further. Writing in the immediate aftermath of Snowden, it would be easy to be seduced by the acres of lurid media reportage and analysis on the topic: intelligence studies, and its parent disciplines have a duty and a role to 'distil the frenzy'[46] to assess where the best truths lie. The following is a summary assessment of the impact on politics of the Snowden revelations.

The magnitude of the American collection programme – in terms of the volume of data it is capturing and the ubiquity of the trawl – is confirmation of something suspected by intelligence scholars and intelligence campaigners alike. The final chapter of Richard Aldrich's excellent book on the UK collection agency, GCHQ, is a good example of where this thinking was prior to Snowden.[47] However, whilst it can be said that this situation was anticipated, predicted or analysed to be the case, there was little in the way of public understanding. This understanding amongst publics has now permeated the entire Atlantic area (the EU, North and Latin America, Euro-Med, West and Southern Africa) and the Pacific, with some serious moments of clear public dissent about it. For the governments of those countries – and in different mixes – they will need to formulate responses that adequately address the concerns of their citizens.

There has been a great deal made by European governments about the NSA programmes, and notable targets, in particular where they have targeted European citizens. That this activity was happening would not have been a surprise to European governments, especially as a good number of them were complicit in the American

[45]Hennessy, *The Hidden Wiring*; and Dover and Goodman, *Spinning Intelligence.*
[46]Echoing the title of another Peter Hennessy book, *Distilling the Frenzy: Writing the History of One's Own Time*.
[47]Aldrich, *GCHQ.*

programme or peripheral European variants. And so the positioning here is in part political necessity, it simply is not possible for a government to say that it is relaxed about a third party engaging in widespread surveillance of its citizens. For those governments not directly involved in the programmes, it is an appropriate moment for them to voice their concerns or opposition to the activities taking place. And for those governments involved, it is an opportunity for them to try and show points of difference and to highlight American activity with the aim of shielding their own well developed programmes from the glare of attention. The complaints from the EU institutions about intrusive surveillance into their operations seem genuinely felt, however, and there are likely to be changes in operating procedure to try and bolster cyber-security.

The bugging of German Chancellor Merkel's phone caused genuine anger and revulsion in Germany. The official American line that President Obama was unaware of this activity against one of his most important European allies gave the impression that either the NSA had gone rogue or the President had not been informed of this highly sensitive activity: one option is as unpalatable as the other. The exceptionalism of the activities against Merkel only lies in the fact that she was such a close ally and diplomatic partner of Obama's, the interception of political leaders' communications is routine. For example, British intelligence officers were revealed to have bugged the UN Secretary General's office in 2002-03 in the run-up to the Iraq war, showing that the need for information sometimes usurps diplomatic conventions and practice.[48] Obama's response to the crisis has crystallised in the early part of 2014, with a defence of the work of the NSA, and a pledge to enact any reform of the NSA and its work considered necessary, including deciding on what activities require warrants through Congress.[49]

Building upon President Obama's embarrassment regarding Chancellor Merkel, the Snowden episode has brought into stark relief the reality that the technical capacity and capabilities of developed world intelligence agencies have outpaced the legal frameworks within which they operate and the political oversight mechanisms that are meant to ensure appropriate tasking and political accountability. If it is true that the NSA focused on Merkel's phone without the highest level authorisation, then the process by which approval is sought is deficient. Similarly in the UK, the parliamentary oversight committee was seen to be ineffective and indeed supine in forewarning the three intelligence directors of certain questions in advance.[50] The Foreign and Home Secretaries decided, at the same time, not to further disseminate their decisions regarding the surveillance of UK nationals by

[48]"UK Spied on UN's Kofi Annan", *BBC News*, 26 February 2004, http://news.bbc.co.uk/1/hi/uk_politics/3488548.stm.
[49]G. Dyer, "Obama Proposals to Reform NSA Set Stage for Fierce Debate", *Financial Times*, 19 January 2014.
[50]I. Oakshott and R. Kerbaj, "Grilling of Spy Chiefs 'a Total Pantomine'", *The Sunday Times*, 17 November 2013.

foreign agencies to their Cabinet colleagues.[51] A disconnect between the intelligence agencies and politicians can be seen to have widened as capacity and capabilities have grown: intelligence agencies enjoy a level of autonomy that is unprecedented. But a critically important disconnect also exists between intelligence agencies and the political classes, on the one side, and the ordinary public, on the other. Such a disconnect goes to the very heart of legitimacy in parliamentary democracies.

One important aspect of the official shaping of the consequences of the Snowden revelations concerned the advantage that had been given to adversaries, who were now able to reconfigure their communications strategies to avoid the attentions of the NSA and associated allies.[52] Given the multifaceted relationship between the allied security forces (be they military or intelligence) and various Iraqi, Afghan and jihadist adversaries, where each side has adapted to the others' developments, approaches and tactics, it seems unlikely in the extreme that all bar the least sophisticated of belligerent actors would have viewed electronic communications as being a safe means by which to communicate prior to the Snowden announcements. To suggest that Snowden has radically altered the operating basis for terrorist groups would seem to be disingenuous.

An enduring impact of this Snowden imbroglio might well become the design and architecture of the internet itself: a move which would be opportunistic rather than one of necessity. US design and control over the fundamental architecture of the internet (naming and address location) has been a live issue for the last five years at least. Knowledge that the NSA and allies have been tapping into the core infrastructure to intercept traffic in transit has produced considerable quantities of analysis around whether an alternative architectural design is desirable: such a move, instigated by Chinese or Russian authorities would significantly raise the transaction costs for US in collecting this material. Whilst naming and addressing is one element of the infrastructure of the internet, physical cabling is the other, and in response to allegations that the NSA has inserted physical intercepts into the submarine cables, a number of states have suggested that they will invest in their own cabling to protect their communications. The most credible of these come from Brazil and Germany.

In February 2014, in the light of a reported decision to abandon attempts at a 'no-spy' deal with the US, Chancellor Merkel suggested that she would seek support for a European communications network, so that electronic traffic no longer needs to transit through American servers (Deutsche Telekom has proposed its own similar system, too).

---

[51]A. Sparrow, "Guardian Faces Fresh Criticism over Edward Snowden Revelations", *The Guardian*, 10 November, 2013.

[52]J. Slack, "'Guardian has Handed a Gift to Terrorists', Warns MI5 Chief: Left-wing Paper's Leaks Caused 'Greatest Damage to Western Security in History' say Whitehall Insiders", *The Daily Mail*, 8 October 2013.

This piece of populism will only be opposed by the most Atlanticist of nations in Europe.[53] In security terms, it now makes clear sense for European governments to be more proactive in securing communications data, but it is more of a question of how this is achieved, with some – including Edward Snowden in subsequent interviews – arguing that it can only be done by international agreement.[54] Some of this international brokerage has already been done within the UN, which pre-Snowden had been focussing on the alleged Chinese government theft of developed world intellectual property, and which the United States is keen to see remains the focus post-Snowden, too. The resolutions within the UN General Assembly made at the end of 2013 were passed without the need for a vote and sought to reaffirm principles of individual privacy and international agreement, so there may be avenues here that can be exploited by governments.[55]

In its response to the revelations about the extent of NSA surveillance on Brazilian communications, the Brazilian government has proposed in draft form a requirement for all Brazilian data to be held in Brazil, and for Brazil to acquire advanced quantum cryptography and its own submarine data cabling.[56] Critics have described these moves as the Balkanization of the internet, and predict that, unless the Brazilian government subsidises data-warehousing within its borders, these measures will add a significant market barrier to technology companies and e-commerce in Brazil.

Additionally, a substantial yet underplayed aspect of this whole issue is the considerable market share in network devices designed and manufactured in China, with several of the 'Five Eyes' nations banning the installation of Chinese made devices for fear of deliberately designed flaws to allow vulnerabilities to be exploited by Chinese intelligence operatives.[57] Similarly, the existing internet architecture is said to be vulnerable to wholesale Chinese interception: the NSA scandal may just be the only one we have learned about.[58]

Former US Secretary of War Henry Stimson once famously said, "Gentlemen do not read each other's mail". The Cold War taught us to focus on confronting threats that emanated from within and without. Post-9/11, these Cold War techniques, coupled with the threat from jihadism have crystallised to remove the governmental taboos around individual privacy. As a consequence, this has become no era for gentlemen.

---

[53]"Berlin must not Erect a Data Wall", *Financial Times*, 17 February 2014.
[54]C. Bryant, "EU Efforts to Shield Data from US are Doomed, says Snowden", *Financial Times*, 27 January 2014.
[55]UN, *Developments in the Field of Information.*
[56]J. Leahy, "Brazil Sparks Furore over Internet Privacy Bill", *Financial Times*, 11 November 2013.
[57]J. Ireland, "Tony Abbott Rules out Change to Huawei Ban", *The Sydney Morning Herald*, 1 November 2013.
[58]J. Halliday, "China Denies 'Hijacking' Internet Traffic: US Report Claims Chinese Telecoms Company had Access to 15% of Global Traffic, Including Military Emails, for 18 Minutes", *The Guardian*, 18 November 2010.

References

Aldrich, R. *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: HarperPress, 2011.

Bochel, H., A. Defty, and J. Kirkpatrick. "'New Mechanisms of Independent Accountability': Select Committees and Parliamentary Scrutiny of the Intelligence Services". *Parliamentary Affairs* (13 November 2013): 1–32.

Campbell, D."They've got it Taped - Somebody's Listening." *The New Statesman*, 12 August 1988. http://www.gn.apc.org/duncan/echelon-dc.htm.

Campbell, D. *Interception Capabilities 2000*. PE 168.184/Part4/4 1999. European Parliament, Brussels.

Corbett, C., and G. Grayson. "Speed Limit Enforcement as Perceived by Offenders: Implications for Roads Policing". *Policing*, 4, no. 4 (2010): 364–372.

Dover, R., and M. Goodman. *Spinning Intelligence*. London: Hurst, 2009.

Ellsberg, D. *Secrets: A Memoir of Vietnam and the Pentagon Papers*. New York: Viking Press, 2002.

Fava, G. *Report on the Alleged Use of European Countries by the CIA for the Transportation and Illegal Detention of Prisoners*. 2006/2200(INI). European Parliament, Brussels, 2006.

Flinders, M., and A. Kelso. "Mind the Gap: Political Analysis, Public Expectations and the Parliamentary Decline Thesis". *British Journal of Politics and International Relations* 13, no. 2 (2011): 249–68.

Gill, P. *Policing Politics: Security Intelligence and the Liberal Democratic State*. London: Frank Cass: 1994.

Goodman, M. "Grandfather of the Hydrogen Bomb? Klaus Fuchs and Anglo-American Intelligence". *Historical Studies in the Physical and Biological Sciences* 34, no. 1 (2003): 1–22.

Grey, S. *Ghost Plane*. London: Hurst, 2006.

Hennessy, P. *Distilling the Frenzy: Writing the History of One's Own Time*. London, Biteback Publishing, 2012.

Hennessy, P. *The Hidden Wiring: Unearthing Britain's Constiitution*. London: Pheonix, 1996.

Holdsworth, D. *Development of Surveillance Technology and Risk of Abuse of Economic Information*. PE 168.184/Vol 5/5 1999. European Parliament, Brussels.

Jeffreys-Jones, R. "The End of an Exclusive Special Intelligence Relationship: British-American Intelligence Co-operation Before, During and After the 1960s". *Intelligence and National Security*, 27, no. 5 (2012): 707–21.

Mandelbaum, M. "Perfect Failure – NATO's War against Yugoslavia". *Foreign Affairs*, 78, no. 5 (1999): 2–8.

Richardson, J. "The Market for Political Activism: Interest Groups as a Challenge to Political Parties". *West European Politics*, 18, no. 1 (1995): 116–39.

Soghoian, C. "Enforced Community Standards for Research on Users of the Tor Anonymity Network". In *Financial Cryptography and Data Security*, edited by G. Danezis, S. Dietrich and K. Sako: 146–53. New York: Springer, 2012.

Suskind, R. *The One Percent Doctrine*. New York: Simon and Schuster, 2006.

UN. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/68/243. New York, United Nations General Assembly. 27 December 2013. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/243.

Webb, D. "ECHELON and the NSA." In *Encyclopedia of Cyber Warfare and Cyber Terrorism*, edited by J. Janczewski and A. Colarik: 452-68. Hershey, PA: ICI, 2008.