TU Delft

Delft University of Technology

Rethinking `five eyes security intelligence collection policies and practice post Snowden

Walsh, PF; Miller, SRM

DOI
10.1080/02684527.2014.998436

Publication date
2016

Document Version
Final published version

Published in
Intelligence and National Security

Citation (APA)
Walsh, PF., & Miller, SRM. (2016). Rethinking `five eyes security intelligence collection policies and practice post Snowden. *Intelligence and National Security*, *31*(3), 345-368. https://doi.org/10.1080/02684527.2014.998436

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Green Open Access added to TU Delft Institutional Repository

'You share, we take care!' - Taverne project

https://www.openaccess.nl/en/you-share-we-take-care

Otherwise as indicated in the copyright section: the publisher is the copyright holder of this work and the author uses the Dutch legislation to make this work public.

Intelligence and National Security, 2016
Vol. 31, No. 3, 345–368, http://dx.doi.org/10.1080/02684527.2014.998436

Routledge
Taylor & Francis Group

ARTICLE

Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden

PATRICK F. WALSH* AND SEUMAS MILLER

ABSTRACT The Edward Snowden leaks challenge policy makers and the public's understanding and perspectives on the role of security intelligence in liberal democratic states. This article explores the challenges confronting security intelligence collection by the 'Five Eyes' countries – particularly those most affected by the leaks. We argue that the debate now needs to move beyond simplistic notions of privacy vs. security to a more detailed understanding of the policy and ethical dilemmas confronting policy makers and intelligence agencies. To that end, we provide a schematic framework (*methods, context and target*) to promote a better understanding of the practical, policy and ethical problems for security intelligence collection emerging post Snowden. The framework is a first step in identifying common principles that could be used develop an ethically informed set of policy guidelines to help decision makers better navigate between citizen's two basic rights: security and privacy.

The tension between the legitimate collection of information for national security and the rights to privacy of the individual in liberal democratic states has increased markedly since 9/11.[1] From 9/11 onwards, in Australia and other liberal democratic countries, the threat from terrorism resulted in a number of significant changes to the laws and practices of policing and national security intelligence agencies.[2] Major reforms in the US resulted in the creation of new agencies (e.g. the Office of Director of National Intelligence, Department of Homeland Security) whereas in other liberal democracies such as Australia, Canada and New Zealand less dramatic bureaucratic reform initiatives were implemented to better coordinate the

*Corresponding author. Email: pawalsh@csu.edu.au

[1]Patrick F. Walsh, *Intelligence and Intelligence Analysis* (Abingdon: Routledge 2011); John Kleinig et al., *Security and Privacy* (Canberra: ANU Press 2011); Mark Lowenthal, *Intelligence from Secrets to Policy,* 5th ed. (Thousand Oaks, CA: CQ Press 2012).

[2]Seumas Miller, *Terrorism and Counter-terrorism: Ethics and Liberal Democracy* (Oxford: Blackwell 2009).

© 2015 Taylor & Francis

efforts of their intelligence communities.[3] Five years after 9/11, governments in liberal democracies also implemented a raft of intelligence reform measures in policies, procedures and legislation.[4]

The net result of key reform measures is that governments have given intelligence agencies far greater surveillance and collection capabilities to proactively detect, disrupt and arrest difficult to get at non-state threats like terrorism and transnational criminals than they had pre-9/11.[5] The impact of these national security policy decisions from 9/11 to the present have sparked national debates about whether more proactive surveillance and intelligence collection methods have resulted in an unsustainable and intolerable level of infringements of the privacy rights of domestic citizens and foreigners alike.[6] Shortly after the initial leaks by Snowden, fault lines began to emerge between critics and defenders of proactive surveillance methods such as metadata collection. For example, from the defender perspective, the former head of US counterintelligence under the Bush Administration, Michelle Van Cleave said: 'to my mind, far from being "Stasi-like", as some overheated critics have charged, such automated systems analysing digits (not people) are non-intrusive public safety responsibilities of the US Government, subject to careful internal checks as well as both judicial and congressional oversight to ensure they do not go beyond those clear boundaries'.[7] From the critical perspective, former NSA whistleblower, Thomas Drake tweeted: 'NSA-dystopian Stasi on steroids that just wants to "know everything" about anybody, anytime, anywhere – regardless of any and all constraints'.[8]

The intelligence leaks by Wikileaks in 2011 were a further and significant catalyst to ongoing political and public debates about legitimate national security intelligence collection and an acceptable burden on the rights of privacy, freedoms and civil liberties, on the internet and elsewhere.[9] However, in 2013, the leaks by former NSA contractor Edward Snowden are having a greater impact as they also revealed significant information about how secret communications interception agencies like the National Security Agency (NSA) actually collect the information. Though what is not known with any certainty is how the Snowden leaks will impact on the future of security intelligence collection in liberal democratic states, on the foreign

[3]Walsh, *Intelligence and Intelligence Analysis*, pp.9–32.
[4]Ibid.; Lowenthal, *Intelligence from Secrets to Policy,* pp.327–44.
[5]M. Innes and J. Sheptycki, 'From Detection to Disruption: Intelligence and the Changing Logic of Police Crime Control in the UK', *International Criminal Justice Review* 14 (2004) pp.1–24; Kleinig et al., *Security and Privacy,* pp.89–129.
[6]G. Mascalo and B. Scott, *Lessons from the Summer of Snowden, Open Technology Institute* (Washington, DC: Wilson Center 2013).
[7]M. Van Cleave, 'What it Takes in Defense of the NSA', *World Affairs* November/December (2013) pp.57–64.
[8]'Snowden Saw What I Saw: Surveillance Criminally Subverting the Constitution', *The Guardian*, 12 June 2013.
[9]Walsh, *Intelligence and Intelligence Analysis*, pp.210–8.

policies of these states, and on the privacy, freedoms and civil liberties of their citizens.[10]

What is known though is that the Snowden leaks have increased tensions and debates over what is appropriate national security intelligence collection to a level never seen in modern intelligence practice.[11] This issue is now a public policy priority of many liberal democratic states. President Obama's January (2014) *Presidential Policy Directive Number 28* is an attempt to respond both from a political and policy perspective to the issue in a way that will not degrade the capabilities of intelligence agencies while addressing concerns by citizens and allies about the nature and extent of security intelligence collection by the NSA and others (PPD 28, 2014). Similar political and policy debates have arisen in the political leadership of Australia, Germany and France.[12]

At the same time, many privacy and civil rights advocates view the information gained from Snowden leaks as an affront to a citizen's privacy. Some groups and even political leaders are lobbying for either the closure or limitations of various kinds of security intelligence collection (e.g. the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center). However, they do not offer any realistic options that would also maintain a citizen's other most basic security: national security. A significant limitation on the scope of all kinds of security intelligence collection will result in Australia and other liberal democratic states still facing numerous and significant national security threats. Threats include international terrorism, the proliferation of weapons of mass destruction, cyber espionage, transnational crime and warfare. Importantly, these are threats to human rights, notably, the right to life. Accordingly, the counter-argument put to privacy advocates on the part of those in favour of security intelligence collection is that infringements of privacy are justified by the protection of the lives of citizens. The arguments on both sides are overly simplified.

Historically, the intelligence studies literature has been relatively slow to identify the ethical dimensions of intelligence practice for organizations and its practitioners.[13] That said, there have been some developments in the theorizing of ethics and intelligence since 9/11. Some studies (Gendron, Erskine, Herman, Bar-Joseph) have attempted to build basic taxonomies for understanding key ethical issues both for the collectors and analysts of

[10]For a useful recent set of discussions on some of these points, see Loch Johnson's edited special forum on the implications of the Snowden leaks, Loch Johnson et al., 'An INS Special Forum: Implications of the Snowden Leaks', *Intelligence and National Security* 29/6 (2014) pp.793–810.

[11]Mascalo and Scott, *Lessons from the Summer of Snowden*.

[12]Ibid., p.18.

[13]J. Goldman (ed.), *Ethics of Spying: A Reader for the Intelligence Professional* (Lanham, MD: Scarecrow Press 2006); J. Olson, *Fair Play, The Moral Dilemmas of Spying* (Washington, DC: Potomac Books 2006).

intelligence.[14] Others have framed the ethics of intelligence collection in 'Just War Theory' to a 'Just Intelligence Theory' (Gendron, Quinlan, Bellaby) or tried to develop frameworks for addressing moral dilemmas (Bellaby, Shelton).[15] Still others have analysed specific forms of criminal intelligence gathering in terms of a policing paradigm.[16] However, none of these theoretical perspectives offers a comprehensive, ethically informed analysis and evaluation of the various different types of security intelligence collection (e.g. wiretaps, metadata, social media).Yet the latter is required in order to give direction to policy in this area. Indeed, significant gaps remain also in our knowledge on what kinds of ethical and policy dilemmas arise in different security intelligence contexts (e.g. transnational crime, counter-terrorism, trade, domestic vs. international collection), and how differences can be reconciled with the ongoing need for this kind of intelligence collection for managing national security threats.

Snowden has compounded significantly the intelligence policy and ethical dilemmas liberal democratic states now face. How do they, as Richards says: 'balance the provision of good security with respecting civil liberties and ensuring the continuing support of the population for security and intelligence policy'.[17] The growing complexity of the security environment, the blurring of domestic and international security, globalization and rapid growth of cyber-technology make the need for better evidence based and ethically informed policy frameworks for security intelligence collection critical.

Accordingly, there is a need to develop ethically informed sets of policy guidelines to guide policy making on improving security intelligence collection in liberal democratic countries whilst managing the risks associated with it. The policy guidelines should not necessarily provide specific 'one size fits all' policy prescriptions, but rather develop generic standards, purposes and parameters that could be applicable to different contexts (e.g. intelligence collection in war, disrupting crime, terrorism, collecting against, friends, allies or neighbours).

---

[14]A. Gendron, 'Just War', *International Journal of Intelligence and Counterintelligence* 18/3 (2005) pp.398–435; T. Erskine, 'As Rays of Light to the Human Soul? Moral Agents and Intelligence Gathering', *Intelligence and National Security* 19/2 (2004) pp.359–81; M. Herman, 'Ethics and Intelligence after September 2001', *Intelligence and National Security* 19 (2004) pp.342–58; U. Bar-Joseph, 'The Professional Ethics of Intelligence Analysis', *International Journal of Intelligence and Counterintelligence* 24/1 (2011) pp.22–43.

[15]Gendron, 'Just War'; M. Quinlan, 'Just Intelligence: Prolegomena to and Ethical Theory', *Intelligence and National Security* 22/1 (2007) pp.1–13; R. Bellaby, 'What's the Harm? The Ethics of Intelligence Collection', *Intelligence and National Security* 27/1 (2012) pp.93–117; A. Shelton, 'Framing the Oxymoron: A New Ethics Paradigm for Intelligence Ethics', *Intelligence and National Security* 26/1 (2011) pp.23–45.

[16]S. Miller and I. Gordon, *Investigative Ethics: Ethics for Police Detectives and Criminal Investigators* (Oxford: Wiley-Blackwell 2014).

[17]J. Richards, 'Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy', *Intelligence and National Security* 27/5 (2012) pp.761–80.

Here we can make a threefold distinction between: (1) *methods* of intelligence gathering, e.g. electronic surveillance; (2) *context* of intelligence-gathering e.g. in wartime, counter-terrorism; (3) *targets* of intelligence-gathering, e.g. the Chinese military or terrorist groups.

In respect of (1), our focus in this paper is only on 'security intelligence collection' as it relates to electronic surveillance (i.e. interception of emails, wiretapping, data bases and social media) and not on human intelligence gathering involving collecting information covertly from physical surveillance or undercover agents. So our discussion of relevant ethically informed policy guideless will be somewhat restricted in scope.

In respect of (2), our aim is to seek to demarcate and justify intelligence-gathering in a variety of contexts. In some such contexts, e.g. organized crime, protocols (indeed, laws) are well-developed. Other contexts are bereft of protocols and subject only to vague and very permissive legislation. Accordingly, we will seek to identify areas where there is a pressing need for ethically informed policy guidelines, given the current lacunae in these areas.

In respect of (3), we discuss a range of different kinds of cases and how a set of ethically informed policy guidelines might be appropriately different, depending on the nature of the target. Such policy guidelines should be sensitive to the nature of the political and cognate relationships between the nation-states in play. Obviously, policy guidelines with respect to intelligence gathering among the liberal democratic 'Five Eyes' intelligence countries (Australia, US, UK, New Zealand, Canada) will necessarily differ from intelligence gathering by these countries from authoritarian nation-states they regard as threats, for example. China. But there are also differences in this regard between the 'Five Eyes' members and other like liberal democratic states. These differences have surfaced recently when it emerged Australia has been 'spying on' on its 'friend' Indonesia and the US on Germany. In part these more nuanced differences are a result of the close historical relationships the 'Five Eyes' countries have built with each other from the start of the Cold War in sharing security intelligence collection material. And while Germany and other EU states have close relations with 'Five Eyes' countries when it comes national security and intelligence policy, they are not members of the 'Five Eyes' group; moreover, there is a diversity in intelligence policy perspectives between member-states of the European Union and 'Five Eyes' countries.

Methods of Intelligence Gathering: Policy Overview

Wiretaps

In this article we discuss three methods of intelligence gathering: wiretaps, metadata and social media. Wiretaps are interceptions of communications between one or more individuals, who are either residing in a country whose intelligence agency is doing the intercepting and/or are located overseas. Compared to other methods of intelligence gathering discussed here (metadata and social media), wiretaps have been used historically by

national security and law enforcement intelligence for decades. The two world wars and technological advancements first in radio and telegraph utilized in military intelligence were later adopted by the internal security or national policing institutions in 'Five Eyes' countries. Wiretapping continued post war, but the passing of the US Federal Communications Act in 1934 became an early example of the current debates about the role of communications interception following the Snowden leaks. These debates include the policy, legislative challenges involved in the permissibility of wiretaps, executive vs. legislative oversight and discussions about under what threat conditions are wiretaps appropriate. We will return to a detailed discussion of these debates in subsequent sections. Here we simply note that in most liberal democratic states legislation has been developed in relation to wiretaps in domestic criminal investigations which more or less mirrors underlying ethical principles and which may help give *some* direction to wiretaps in respect of other investigations of interest to us here, e.g. of suspected terrorists domiciled in foreign liberal democratic states. The latter ethical principles include the following ones.[18]

First, because such accessing and/or intercepting are by definition an infringement of the right to privacy, the presumption must be against their use. This presumption can be overridden by other very weighty moral considerations – especially the need to protect other fundamental moral rights, such as the right to life – or by exceptional circumstances, such as might obtain in wartime.

Second, the benefits of such accessing and/or intercepting must offset the likely costs, including the costs in terms of the erosion in public trust.

Third, the accessing and/or interception in question must be in relation to serious crimes.

Fourth, there must be at least a reasonable suspicion or reasonable belief or probable cause that the person whose privacy is to be infringed has committed, or intends to commit, a serious crime and that the resulting information is likely to substantially further the investigation under way in relation to that crime. The more intrusive and sustained the infringement of the right to privacy, the more serious the crime in question needs to be (principle of proportionality) and the higher the standard of evidence that ought to be required that the person whose right to privacy is to be infringed is implicated in this crime.

Fifth, there must be no feasible alternative method of gathering the information that does not involve an infringement of privacy.

Sixth, the law enforcement officials must be subject to stringent accountability requirements, including the issuing of warrants in circumstances in which the justification provided is independently adjudicated.

Seventh, those whose privacy has been infringed must be informed that it has been infringed at the earliest time consistent with not compromising the investigation, or connected investigations.

[18]Seumas Miller and John Blackler, *Ethical Issues in Policing* (Aldershot: Ashgate 2005) Chapter 5.

Metadata

Metadata means 'data disassociated from the identities of its subjects or that can infer from gathered data any anomalous activity'.[19] It has generally referred to the bulk collection of telephone data (call numbers, time of call but not content of call) for domestic and international calls. The development of data mining and analytics techniques and technologies has resulted in the more efficient and speedier interception of telephone and other types of communications and linking or associating various methods of electronic communication for the purpose of intelligence surveillance.[20] Intelligence agencies increased their focus on data mining and analytics technologies to 'discover knowledge' from disparate data sources at the same time non state threat actors like terrorists were using multiple and more secure ways to communicate than telephones.[21]

After 9/11, the US Foreign Intelligence Surveillance Court (FISC) authorized the collection of bulk telephony metadata allowing the NSA access to all call records.[22] This was considered by government and the agency as the only effective way to continuously keep track of all activities, communications and plans of foreign terrorists who disguise and obscure their communications and identities.[23]Metadata security intelligence collection solutions such as those revealed in the Snowden leaks were also adopted because non-state actors (terrorists and transnational criminal syndicates) are using technological developments (in data processing, open source information and commercially available encryption) to communicate, plan attacks or conduct their own surveillance on national security and law enforcement authorities. Hence, intelligence agencies like the NSA had to exploit similar communications technology to track the 'digital footprints' in multiple data feeds (metadata), allowing them to respond more pro-actively to threat actor activities.

Despite the 'promise' of metadata to enhance intelligence collection and surveillance since 9/11 there have been several policy, practice and legislative challenges associated with its use in the 'Five Eyes' countries. One challenge has been sharing the results of 'sensitive' metadata feeds across all member agencies of the intelligence communities and with agencies normally viewed as 'outer' members of intelligence communities such as law enforcement agencies. For example, in the US the Intelligence Reform and Terrorism Protection Act (2004), amongst other seminal reforms introduced an

[19]Jennifer E. Sims and Burton Gerber, *Vaults Mirrors and Masks: Rediscovering US Counterintelligence* (Washington, DC: Georgetown University Press 2009) p.7.

[20]For a discussion of the development of national security data mining capabilities in the United States after 9/11 see Jeffrey W. Seifert, 'Data Mining and Homeland Security', CRS Report RL31798, Congressional Research Service, April 2008.

[21]Christopher Joye and Paul Smith, 'Most Powerful Spy Says Snowden Leaks Will Cost Lives', *The Australian Financial Review*, 8 May 2014, pp.1, 11.

[22]The FISC was established to provide judicial oversight of intelligence agencies (the NSA and FBI) seeking interception of communications of suspects.

[23]Richard Clarke, Michael Morel, Geoffrey Stone, Cass Sunstein and Peter Swire, 'Liberty and Security in a Changing World', Report and Recommendations of the President's Review Group on Intelligence and Communications Technology, 12 December 2013, pp.95–6.

information sharing environment (ISE) to better manage sharing issues identified in the 9/11 Commission Report.[24] The ISE initiative resulted in a number of new policy and technological initiatives that supported the growth in metadata methodologies for agencies like the NSA, but also in other federal, state and local agencies. For example in 2008, the DHS and DOJ jointly sponsored a nationwide Suspicious Activity Reports (SARs) for counter-terrorism that ambitiously was meant to stretch from federal to state and local agencies to collect against indicators of suspicious behaviour or activities.[25] The SAR initiative was originally met by concerns from privacy and human rights groups, who suggested that 'suspect actions' such as someone using binoculars or cameras or even espousing extremist views may not be precursors to terrorism, but may be entirely innocent and legal.[26]

In addition to information about telephone metadata program, Snowden's revelations also included material about NSA's PRISM program, which allows the agency to access a large amount of digital information – emails, Facebook posts and instant messages. The difference between telephone metadata and PRISM is the later also collects the contents of those communications. The revelation has sparked several policy related debates: is the metadata system legal, constitutional and, from a methodological perspective, does it work? We will address each of these briefly in turn.

Director of National Intelligence (DNI) Jim Clapper and the then NSA Director, General Alexander, defended the legality of the metadata approach by stating that it is lawful under both the Foreign Intelligence Surveillance Act (FISA) of 1978, and after 9/11 Section 215 of the Patriot Act. FISA provides procedures for the approval of various investigative methods: electronic surveillance, physical searches, recording all outgoing telephone numbers called and comply to produce documents.[27] Congressional views on the

[24]The ISE initiative sought to connect the 17 members of the US intelligence community with the broader law enforcement agencies to improve information sharing. See Walsh, *Intelligence and Intelligence Analysis*, p.249.

[25]Mark A. Randol, 'Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress', CRS Report 7-5700, Congressional Research Service, November 2009.

[26]The SARs initiative was not completely implemented by many agencies at state and local agencies at the time. Some agencies such as NYPD were not enthusiastic about the system and at the time relied more on a humint rather than a technical data collection approach to surveillance. Ibid., p.177.

[27]Section 215 allows agencies like the FBI and NSA to compel the production of telecommunication records, public accommodation facilities, storage facilities and vehicle rental facilities. Under Section 215 the FBI could apply to the Foreign Surveillance Court (FISC) to compel an individual to produce records if the FBI present FISC with evidence that the individual lived abroad or the record sought are 'relevant to an authorised foreign intelligence, international terrorism, or counter-espionage investigation'. The FISA Amendments Act of 2008 added additional provisions for the intelligence targeting of US persons believed to be located abroad. Edward Liu, Andrew Nolan and Richard Thompson, 'Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments', CRS Report 7-5700, Congressional Research Service, April 2014.

legality of metadata methodologies, however, have been conflicted with some senators and congressmen declaring they were either not aware of it/ and or it was unconstitutional.[28] Subsequently, the President's 2013 Review Group on intelligence and communications technology did not explicitly argue that the bulk telephone metadata collection was unconstitutional. However, they did say that: 'in our view, the current storage by the government of bulk metadata creates potential risks to public trust, personal privacy and civil liberty'.[29] Many privacy advocates and journalists (such as Glenn Greenwald) of course support Snowden's view that metadata collection is illegal, unconstitutional and affronts against privacy.[30]

Leaving the legality and constitutionality perspectives aside, another key political and policy issue arising from the Snowden leaks are debates about whether the metadata methodology has been effective in disrupting and reducing terrorism attacks. Immediately after the revelations, President Obama, General Alexander, Senator Dianne Feinstein, Representative, and Congressman Mike Rogers were quick to report that the metadata program had stopped 50 terrorist attacks. This assertion was later contested and rephrased to mean 53 terrorist events (not attacks). A further review said none were legitimate attacks and that there really was only one case that prevented a terrorist event on US soil. Given the secrecy around the metadata programs, it is difficult to provide an accurate assessment of their effectiveness. A related concern that the Snowden leaks on metadata raise though is the influence of technological determinism – or the view by some that more technology will always make 'better intelligence collection'. Technology has led to greater understanding of complex security environments, but data mining and analytics platforms used in metadata applications are still not sufficiently sophisticated to find quickly, efficiently and reliably the 'footprints of a terrorist' in the data *ahead* of an attack. Hence, metadata efforts need to be blended with other forms of collection, which are often more expensive and painstaking such as humint. Policy makers need to be aware that metadata can never be the golden goose and it's doubtful that sensible intelligence officers ever thought it was.

Finally, private sector issues have also arisen from the PRISM (metadata) revelations. There is now a lack of trust and cooperation between some major telecommunication and technology companies and security intelligence collection agencies. This could potentially have several knock on effects. For example, countries who leaders and citizens were revealed by Snowden as 'NSA targets' such as Germany and Brazil have started discussing changes to re-routing of communications via the internet. US corporations such as Google, Facebook, Microsoft and Yahoo have become increasingly worried about losing market share (based on the revelations that the NSA exploited

[28]See, for example, Senators Ron Wyden, Mark Udall and Martin Heinrich, 'End the NSA Dragnet, Now', *New York Times*, 25 November 2013.
[29]Clarke et al., 'Liberty and Security in a Changing World', p.17.
[30]Glenn Greenwald, *No Place to Hide. Edward Snowden, the NSA and the Surveillance State* (London: Hamish Hamilton 2014) pp.2–3.

their system) are now sealing cracks in their systems, and further encrypting data for their customers.[31] This lack of cooperation, and hardening of security measures for internet and social media customers, could potentially impact on security intelligence collection efforts against national security threats.

The collection of bulk metadata is morally problematic in that, as we saw above, there is a presumption against the gathering of personal information on citizens by government officials, including law enforcement and other security personnel. As we also saw, this presumption can be overridden in relation to specific kinds of information required for specific legitimate purposes, such as the investigation of someone reasonably suspected of engaging in serious criminal activity. But information gathered for one purpose should not be made available for another purpose, unless a specific case can be made out for doing so.

This latter problem is evident in the metadata collection arising in the Verizon[32] and PRISM controversies. Verizon involved the collection by the NSA of the metadata from the calls made within the US, and between the US and any foreign country, of millions of customers of Verizon and other telecommunication providers whereas PRISM involved the agreements between NSA and various US-based internet companies (Google, Facebook, Skype etc.) to enable NSA to monitor the on-line communications of non-US citizens based overseas. While privacy laws tend to focus on the content of phone calls, emails and the like, the Verizon episode draws our attention to so-called metadata, e.g. the unique phone number/email address of caller/recipient, the time of calls and their duration, and the location of caller/recipient. Such metadata while collected to facilitate the communication purposes of callers/recipients and their telecommunication providers – and is consented to for this purpose – also enables the non-consensual construction of a detailed description of a person's activities, associates, movements and so on, especially when combined with financial and other data. The availability to security agencies of such descriptions is surely an infringement of privacy and, therefore, needs justification; notably by reference to the moral and legal principle of reasonable suspicion (or probable cause in the US).

Social Media

Social media is defined as 'both the technology and the use of a varied category of internet services inspired by the participatory web or web 2.0, which enables users to create and share digital content, whether textual, audio or video'.[33] The intelligence community is increasingly embracing

[31]Recent reports suggest that Google is even laying its own underwater fibre optic cables to reduce interception capabilities by the NSA. David Sangar and Nicole Perlroth, 'Internet Giant Erect Barriers to Spy Agencies', *New York Times*, 6 June 2014.

[32]Edward Lucas, 'A Press Corps Full of Snowdenistas', *Wall Street Journal*, 29January 2014 <*http://online.wsj.com/news/articles/SB10001424052702303519404579350663554949356*> (accessed 24June 2014).

[33]Jamie Bartlett and Carl Miller, 'The State of the Art: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism', *Demos* (2013) p.4.

social media as both collection and analytical tools to support different decision making requirements. Ormand, Barlett and Miller provide a good overview of how social media has and could be used in national intelligence frameworks.[34] For example, social media could be used for crowd sourcing information to get a better flow of information in emergency/crisis situations such as in natural disasters or riots. Social media is also useful in generating better understandings of indicators for violence and radicalization as well as providing what they refer to as 'near time situational awareness' where we can collect and cluster social media outputs to get a sense of unfolding events such as the current Ebola outbreak in West Africa.[35] A good example, of providing situational awareness would be being able to monitor effectively Facebook and Twitter as they captured events leading up to the 2011 Egyptian revolution. Event detection technology can profile words over time suggesting that like events might be occurring.[36] The Snowden revelations have shown the recent increase in gathering intelligence from social media sites such as Facebook and Google for counter-terrorism. There is insufficient evidence, however, on the frequency and types of social media terrorists groups are exploiting. Recent research suggests more groups are moving from traditional web based communications to social media for propaganda, recruitment and operational planning. For example, we know some Al Qaeda leaders have used Instagram to share images and quotes glorifying imprisoned fighters and to disseminate images of dead martyrs.[37] More recently, the Islamic State of Iraq and Syria (ISIS/IS) are using social media to recruit fighters and promote violence in ways that some reports have labelled a 'twitter jihad'.[38]

As with metadata there are a number of policy, practice and legislative issues arising from the exploitation of social media by intelligence agencies. One issue has been the extent to which they can compete for relevance with the private sector and think tanks, which have been more adept at managing social media analysis on issues such as the political upheaval in North Africa and the Middle East in 2011–2. Our intelligence agencies have not done well so far at handling the flood of information which comes from social media like Facebook or Twitter and need to demonstrate that they can use social media more quickly and reliably than their private sector competitors.

The accessing, collection and analysis of data emanating from social media gives rise to the privacy concerns already discussed in respect of wiretaps and metadata collection. However, arguably these privacy concerns in relation to social media are much reduced given that the users of *social* media in many cases ought not reasonably expect the same high levels of privacy accorded, for example, to those whose emails are being intercepted or whose phone

[34]Sir David Ormand, Jamie Bartlett and Carl Miller, 'Introducing Social Media Intelligence (SOCMINT)', *National Security and Intelligence Journal* 27/6 (2012) pp.804–6.
[35]Ibid.
[36]Ibid., p.27.
[37]Bartlett and Miller, 'The State of the Art', p.10.
[38]Deborah Richards, 'The Twitterjihad: ISIS Insurgents in Iraq, Syria Using Social Media to Recruit Fighters and Promote Violence', *ABC News*, 21 June 2014.

data is being collected. On the other hand, depending on which forms of social media are in question, the users of social media have not necessarily explicitly or implicitly consented to, or might not otherwise reasonably expect, such interception and collection by persons outside the social group in question and for security purposes. Accordingly, their behaviour might be far more guarded if they knew that their communications were being accessed, collected and analysed in this manner. Moreover, in some such cases it may well be that their privacy is being unjustifiably infringed. Naturally, we are speaking of users with respect to whom there is not an antecedent reasonable suspicion of unlawful and immoral activity of a serious nature.

Contexts of Intelligence Gathering: Policy Overview

Military and Counter-Terrorism Contexts

With a better understanding now of *methodologies* used for electronic security intelligence collection, this section will discuss the policy, political and ethical dimensions relevant to understanding why intelligence collection occurs in different contexts. The public debate over surveillance and collection after the Snowden leaks has focused almost exclusively on the NSA and other 'Five Eyes' sigint agencies (such as the UK's Government Communications Headquarters (GCHQ) and the Australian Signals Directorate (ASD)) and spying on citizens. What hasn't come out nearly as strongly in policy and public debates is a discussion of other areas in which security intelligence collection takes place beyond just 'spying on citizens' or terrorism. In the midst of the 'damage control' after Snowden, agencies in the 'Five Eyes' countries have been slow to inform the public about how the remit of electronic surveillance (security intelligence collection) goes beyond the simplistically perceived 'spying on persons of interest' to a broader range of foreign and national intelligence collection priorities and threats. Many of these threat types/issues have always been collected against using security intelligence collection methodologies as they are of enduring interest to policy makers whose primary responsibility is securing the state against such threats. The threat issues include: understanding states of concern, military readiness, troop movements, fragile states and weapons of mass destruction.

In the military context, intelligence is not just focused on gaining knowledge about the enemy but, as military historian John Keegan suggests, its function is more than this and it 'can only work through strength, power and force to resist and forestall the enemy'.[39] Hence, developments in communications technology from World War One to the Cold War and beyond became vital in preparing for battle with the enemy.[40] It should be no

[39]John Keegan, *Intelligence in War* (London: Hutchinson 2003) p.398.

[40]In 1945, as the hot world war turned into the Cold War, advancements in technology ensured sigint was to become a vital part of Warsaw and NATO pact countries and their militaries monitoring each other. Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press 1996) pp.66–9.

surprise, therefore, that the majority of the large scale security intelligence collection technology and efforts has taken place in agencies based in national defence architectures.

The end of the Cold War resulted in a refocusing of national intelligence collection priorities away from exclusively state based national defence threats towards non-state threat actors or 'global outlaws'. The events of 9/11 provided a further catalyst for security intelligence collection capabilities being not just directed at state based threats, but also transnational and sub-state threats such as terrorism, arms, drugs trafficking and the broader human security agenda. This broader understanding of 'national security' influenced intelligence policy making and the menu of work traditional war fighting and counter-espionage collection agencies started to deal with.[41] The events of 9/11 also showed a blurring of boundaries between 'foreign' and 'domestic' intelligence collection – resulting in greater connectivity between foreign security intelligence collection agencies (NSA, GCHQ, ASD) and their national (domestic) security services counterparts (FBI, MI5, ASIO).

The blurring of international and domestic security contexts presented opportunities and challenges to security intelligence collection agencies in dealing with terrorism but also other transnational crimes. A key opportunity was the scale and speed of collection efforts could be ratchet up. For example, the activities of an elaborate transnational drug smuggling syndicate could be more quickly and comprehensively disrupted if both foreign and domestic security intelligence collection efforts were targeted against their domestic and internationally based members.

Governments wanted to give more resources and tools to such proactive security intelligence collection methodologies. In particular, changes in legislation across the 'Five Eyes' countries reflected the desire by their intelligence communities and political masters to be proactive in security intelligence collection, humint collection and in investigations. For example, in Australia after 9/11 the conservative Howard Government legislated for two preventative measures to deal with the threat of terrorism: control and preventative detention orders to make it easier for law enforcement and national security intelligence agencies to have more time to question and gather information from terrorist suspects without formally charging them. There were other similar counter-terrorism legislative initiatives in the UK and other 'Five Eyes' countries as well as the major changes that occurred under the US Patriot Act for security intelligence collection discussed earlier.[42]

[41]The Human Security Agenda gained traction in the mid 1990s arguing for a wider, inclusive definition of security beyond traditional military, state based threats to the security of people within states from political violence, economic vulnerabilities and even diseases and natural disaster. See, the Human Security Centre, *Human Security Report* (Oxford: Oxford University Press 2005).

[42]Under the Australian Commonwealth Criminal Code (Cth) Divs 104–105 control orders allowed limits to be placed on the movement and activities of people who pose a terrorist risk to the Australian community. Preventative detention orders can be issued and a suspect held up

In summary, there was a policy urgency by governments after 9/11 to give intelligence agencies the 'right tools' and flexibility to do the job. It was only later in successive inquiries into intelligence failures both actual or perceived that it became clearer what some of the challenges are in security intelligence collection in 'Five Eyes' countries, particularly in dealing with counter-terrorism. Lowenthal provides a summary of these including the ability to intercept smaller signals from more remote terrorists groups, and the growing counter-intelligence challenge (i.e. the growing awareness of terrorists groups about security intelligence collection efforts by intelligence agencies).[43]

As discussed earlier, the 2013 President's Review Group Report identified many policy issues related to bulk metadata collection of telephone and other forms of communication. The report underscores the post 9/11 debate about what issues are in the national security interest to collect intelligence against. Some of these will be discussed shortly, but the report also highlighted other intelligence policy reform issues including: the effectiveness of intelligence oversight mechanisms, legislative instruments (for authorizing and constraining surveillance) and whether current intelligence collection guidelines, particularly for high value targets and/or political leaders, are adequate. Many of these intelligence policy reform issues started to get an airing during the Wikileaks episode, which revealed issues about vetting personnel, information security and sharing, and again these issues also surfaced again after the Snowden leaks.[44] Other ethical aspects also arose including privacy, the increasing role of proactive surveillance and increasingly public perspectives about what is legitimately a secret and what is in the public interest.

Counter-espionage

Counter-espionage has always been a key function of a modern state's intelligence enterprise. For example in 1909 the UK created the Secret Service Bureau (later to become MI5 and MI6). The role of this bureau, as Knightly succinctly puts it, was to 'steal secrets from other countries and to protect its own. It was also empowered to operate in peace as well as in war'.[45]

Footnote 42 continued

to 14 days when a terrorist attack is imminent or has occurred. The objective is to detain a suspect to preserve evidence relating to an attack or identify preparatory steps by those involved in planning an attack. See, Andrew Lynch, Edwina Macdonald and George Williams, *Law and Liberty in the War on Terror* (Sydney: Federation Press 2007) pp.4–6. For discussion of other legislative changes in other Five Eyes Countries see Walsh, *Intelligence and Intelligence Analysis*, pp.218–27.

[43]Mark M. Lowethal, *Intelligence from Secrets to Policy* (Thousand Oaks, CA: CQ Press 2012) pp.98–9.

[44]Clarke et al., 'Liberty and Security in a Changing World'. For a discussion on the policy issues arising after the Wikileaks episode see Walsh, *Intelligence and Intelligence Analysis*, pp.210–8.

[45]Phillip Knightley, *The Second Oldest Profession* (London: Pimlico 2003) pp.1–2. For a seminal history though of MI5 see Christopher Andrew, *The Defence of the Realm, The Authorised History of MI5* (London: Allen Lane 2009).

Traditional notions of counter-espionage conjure up images of the physical surveillance of hostile foreign intelligence services either in country or overseas, which was the hallmark of counter-espionage during the Cold War. For example, after 1945 Soviet agent Kim Philby working within MI6 was able to provide his KGB handlers crucial information on US and UK covert operations in the Baltic States and Russia compromising hundreds of American and British agents.[46] A discussion of this kind of humint is beyond the scope of this article, but counter-espionage can also collect intelligence via technical means. The purpose of counter-espionage are in part about knowing what collection priorities a foreign power has on your state, its leaders and military – but it also has a counter-intelligence function, which is more specifically focused on collecting intelligence on the 'adversary's intelligence service'.[47] As Loch Johnson suggests: 'counter-espionage represents the more aggressive side of counter-intelligence with the goal of penetrating with an agent and electronic surveillance "the inner councils of a foreign intelligence service or terrorist cell"'.[48]

The nature of counter-espionage and counter-intelligence operations are high stakes for both the country using them to collect intelligence (if found out, agents can lose their lives) and or the foreign intelligence service targeted (based on knowledge about intelligence technological capabilities exposed). Hence the ability to undertake counter-espionage or counter-intelligence requires protecting sources, and methods which frequently involve deception and betrayal. In the game of deception, 'Five Eyes' countries may not spy on each other but others, including as discussed later allies, may be 'fair game'. The legislation of several security intelligence agencies outline their counter-espionage roles and describe the 'legal' means for them to engage in collection and operational activities that prevent or disrupt foreign powers working internationally or domestically against the interest of the state. Much of the legislation governing counter-espionage is necessarily broad and does not provide detailed description on the scope of activities 'Five Eyes' intelligence agencies may engage in. For example the *Intelligence Services Act (2001)* of Australia and the *Intelligence Services Act (1994)* of the UK both provide very broad descriptors for the functions of their humint (ASIS, MI6) and sigint (ASD, GCHQ) agencies – using phrases such as 'undertaking activities relating to the *actions or intentions* of *persons or organisations* outside these countries and at the discretion of relevant ministers'. Broadly drafted language provides agencies with maximum flexibility to interpret and act on ministerial directions, including if intelligence gathering might be directed at perhaps friendly leaders.[49]

---

[46]Abram Shulsky and Gary Schmitt, *Silent Warfare Understanding the World of Intelligence* (Virginia: Potomac Books 2002) p.109.
[47]Ibid., p.110.
[48]Loch K. Johnson (ed.), *Handbook of Intelligence Studies* (Abingdon: Routledge 2007) p.10.
[49]For a detailed review of the functions of Australia and the United Kingdom's key foreign intelligence collection agencies, see Part 2 (Functions of Agencies), the Intelligence Services Act (2001) and Sections 1 and 3 the Intelligence Services Act (1994), respectively.

While counter-espionage collection activities may be one area of legislation where it is necessary for operational security to keep collection functions and methods vague, the deception, deniability, lying and cheating which goes into the collection of intelligence via espionage from other states, people and organizations has long been one critical point of tension about what is considered the appropriate role of intelligence gathering in democratic societies. Since the end of the Cold War, counter-espionage has continued to focus on traditional threats, i.e. state based ones of a political, strategic and military nature, but the revolution in ICT has also meant counter-espionage is increasingly not only about humint ('spies on the ground') but also the exploitation of electronic surveillance to understand state's intentions, as well as defensive and offensive counter-intelligence.[50] As technology has increased it has helped counter-espionage 'go online', resulting in many security intelligence collection agencies now actively monitoring 'cyber space' to identify penetration attempts by foreign powers (including rogue states) and increasingly non-state actor groups like hacktivists to 'steal' information about decision-making processes, intellectual property. The stakes in 'online' counter-espionage may be great between countries. For example, during an interview in May 2013 former NSA chief General Alexander warned that North Korean cyber-attacks on South Korea in 2013 could have easily led to war.[51]

Economics and Trade

Another important context in which security intelligence collection is practiced is the areas of economics and trade. International commerce and globalized technology have facilitated opportunities for economic intelligence and industrial espionage particularly as many large companies such as Apple outsource their production to several countries placing them at risk for foreign industrial espionage at the design and production stages.[52] There are a number of issues where intelligence agencies from all countries (both friends and others) have historically collected information on strategic markets, trade access, products and proprietary information on things like drugs, dual use technology such as computer microprocessors (that could be used in defence applications) and green field research projects. Given a lot of business practice occurs on open information networks: 'both military friends and foes may be adversaries in the economic arena of espionage'.[53] However it would be simplistic to portray that only public sector intelligence agencies are involved in economic espionage. The 'espionage activities' of private sector organizations are also making it difficult to assess sometimes whether the collection of sensitive trade information by either or both the public and

[50]For a brief discussion of the differences between offensive and defensive counterintelligence, see Sims and Gerber, *Vaults Mirrors and Masks*, pp.22–3.
[51]Joye and Smith, 'Most Powerful Spy Says Snowden Leaks Will Cost Lives', p.1.
[52]Harvey Rishikof, 'Economic and Industrial Espionage' in Sims and Gerber (eds.) *Vaults Mirrors and Masks*, p.200.
[53]Ibid., p.201.

private sector is really in the economic national interest (i.e. a matter of national security) or more narrowly in the interest of a 'multinational conglomerate'.[54] In many 'Five Eyes' countries, intelligence legislation stipulates that collection is also for economic as well as political or military priorities and this has been used as rationale for security intelligence collection involving economic and trade relations between friends as well as less trusted trading countries. Knowing the strategy of another country ahead of trade negotiations is clearly advantageous. The use of intelligence gathering in the trade context featured out of Snowden revelations in February 2014, when leaked reports showed the Australian sigint agency ASD spied for the NSA on Indonesia during US-Indonesia trade talks. When the information was made public, Australian Prime Minister, Tony Abbott, said that the government does not comment on operational intelligence matters, but added: 'we don't use intelligence for commercial purposes'.[55] These revelations have raised further discussion about the 'legal' and international norms around spying on friends and neighbours and where the limits should be on the use of security intelligence collection for economic and trade issues.

Thus far we have differentiated a variety of contexts of surveillance and data collection and it is evident that from an ethical perspective these contexts vary greatly: what is morally permissible in war-time is not permissible in peace-time, and what is morally permissible in the investigation of serious crime is not permissible in pursuit of a commercial advantage. However, as we have seen, in recent years intelligence gathering for the purpose of combating terrorism has muddied the waters. On the one hand, combating terrorism is a matter for domestically focused law enforcement agencies such as the FBI and, therefore, intelligence gathering is, or ought to be, constrained by morally based legal principles, and subject to accountability mechanisms, built into the criminal justice system (as outlined above). On the other hand, combating terrorism – notably international terrorism – is a matter for externally focussed national security focused agencies such as the CIA and, as such, intelligence gathering is not, and perhaps ought not to be, subject to the same stringent moral and legal constraints and accountability mechanisms. However, post 9/11 the lines between domestic law enforcement intelligence gathering and foreign intelligence gathering have become blurred, notably in the legal sphere. For example, under the provisions of the above-mentioned Patriot Act, arguably law enforcement agencies were subject only to the wiretap provisions of the Foreign Intelligence Surveillance Act (FISA) and, as such, not subject to the normal judicial controls operating in the criminal justice system. Nor is the blurring restricted to the legal sphere. Whatever the moral principles governing intelligence-gathering in domestic law enforcement, they surely differ to some degree from those governing foreign intelligence-gathering. However, the phenomenon of international terrorist groups who perpetrate terrorist attacks on domestic soil muddies the waters

[54]Ibid., p.213.

[55]Australian Prime Minister's comments were quoted in the *Australian*, 'Australia Spied on Indonesian Trade Talks', 16 February 2014.

and, as a result, the specification of appropriate moral principles for the collection of intelligence in relation to such groups is problematic, as it is in other areas of counter-terrorism.

Targets of Intelligence Gathering: Policy Overview

In this last section we discuss who the targets for security intelligence collection are in three contexts: *military and counter-terrorism, counter-espionage,* and *economics and trade*. In the military context, as noted earlier, there are multiple targets for security intelligence collection: fragile/vulnerable states, non-state actors (terrorists and transnational criminals) and states of concern (Russia, China). The national security committees or equivalent in each 'Five Eyes' countries ultimately decide which nation-states and non-state actors are targeted. National intelligence collection priorities are then actioned by the respective military intelligence agencies in each country (for example, the Defense Intelligence Agency in the US (DIA) and the (DIO) Defence Intelligence Organisation in Australia) in order to support operational and tactical decision-making by military personnel in an operational environment or battle.

As noted earlier, since 9/11 there has been a growing focus on pro-active collection and targeting to prevent, disrupt and contain terrorism and other threats.[56] A more pro-active policy and legislative response to security intelligence collection targeting has in turn brought a number of challenges. One challenge has been improving the overall governance arrangements, particularly in the tasking and coordination of security intelligence collection involving an increasing multiple of agencies both within and outside the 'Five Eyes' countries. How do multiple national agencies involved in foreign and domestic security intelligence collection as well as state and local law enforcement coordinate their collection efforts against a target? While national intelligence collection priorities may be agreed to at executive (cabinet) level, as one moves away from the strategic decision making level to operational and tactical levels these 'national intelligence collection priorities' find expression in different ways and are interpreted and operationalized in various ways.

The creation of national counter-terrorism (fusion centres) in the 'Five Eyes' countries sought to develop this common understanding and coordination of target collection prioritization. Fusion centres are works in progress and issues remain about how collection is tasked, prioritized and operationalized amongst 'traditional' members of intelligence communities and outer or emerging intelligence practice areas such as taxation, biosecurity and corrections.[57]

---

[56]Innes and Sheptycki, 'From Detection to Disruption: Intelligence and the Changing Logic of Police Crime Control in the UK', pp.1–24.

[57]For example in 2010 ASIO developed the Counter Terrorism Control Centre in order to better coordinate and set counter terrorism intelligence collection priorities across the entire national security community. For a further discussion of emerging intelligence practice areas see Walsh, *Intelligence and Intelligence Analysis*, pp.34–67.

A second challenge has been concerns about the provenance of intelligence. The role of coercive interrogation in intelligence collection during the Bush Administration impacted adversely on how the US intelligence community was seen by citizens and internationally – resulting in the practice being stopped under the Obama Administration.[58] Coercive interrogations, facilitated or carried out by Middle Eastern intelligence services with varying accountability standards for human rights caused a 'rethink' ethically, procedurally and legally in 'Five Eyes' countries about the manner and the source of human intelligence collection. For example, the Canadian Security Intelligence Service (CSIS) developed greater risk management processes to assess the kinds of information it could use from certain source countries in the Middle East.[59] While coercive interrogation relates to human intelligence collection (humint) it raises broader policy and ethical issues about how 'Five Eyes' countries engage with the security intelligence collection efforts of agencies from other countries that are not liberal democratic and whose collection practices are not aligned with adequate legislative and oversight mechanisms. The July 2014 Snowden revelations that the NSA has increasingly worked closely with Saudi Arabia's Ministry of Interior – an agency which has been known to use torture during investigations – underscores the ethical, policy and legal challenges of cooperating with non-democratic states in security intelligence collection.[60]

A third challenge is managing the ethical, legal and policy issues of target hardening. Increasingly since 9/11 targets such as terrorists have become aware of traditional national security and law enforcement interception techniques such as wiretaps. Hence, legislation was enacted in 'Five Eyes' countries to provide intelligence agencies more flexibility to 'get around' such target hardening. This included, for example, the ability to intercept multiple call wiretaps attached to the one person and a greater number of social media sources without having to apply for single warrants for each interception. What has lagged behind though in some 'Five Eyes' countries is sufficiently coherent policy oversight to ensure counter-terrorism legislation and other intelligence policy guidelines for security intelligence collection are inspected periodically for their effectiveness, privacy and human rights impacts. The evidence across the 'Five Eyes' shows a more ad hoc approach to legislation and policy for security intelligence collection. For example, the collection of bulk telephone metadata has been sanctioned by orders of the Foreign Intelligence Surveillance Court (FISC) pursuant to Section 215 of the USA Patriot Act since 2001. The original sunset on Section 215 was December 2005, but it has been reauthorized several times without any root and branch

[58]For a discussion of coercive interrogation under the Bush Administration see Walsh, *Intelligence and Intelligence Analysis*, pp.196–204.

[59]For a further discussion of emerging intelligence practice areas see Walsh, *Intelligence and Intelligence Analysis*, pp.202–3.

[60]'NSA Partnering with Saudi Regime-Snowden Leaks', *RT News*, 26 July 2014 <*http://rt.com/usa/175712-snowden-nsa-saudi-partnership*> (accessed 26 September 2014).

review.[61] Further, as anti-terrorism legislation was enacted post 9/11 in Australia it wasn't until 2010 that the government decided to establish an independent (judicial) national security legislation monitor. In May 2014, the new Liberal National coalition government has decided to abolish this office, though the monitor now seems to have received a stay of execution as the Australian Governments seeks to now further expand the surveillance capabilities of the country's national security framework including enhancing ASIO's ability to monitor 'targets' computers and computer networks.[62]

A final challenge is how 'Five Eyes' governments manage policies and procedures for security intelligence collection against allies particularly political leaders. Are such leaders legitimate targets? It is common knowledge that most states have active counter-espionage targeting campaigns which support a range of decision-making processes of government: political/diplomatic and economic. Security intelligence collection targeting historically has provided states an advantage in gaining a better understanding of the political and economic intentions of foreign political leaders (friendly and less friendly). 'Five Eyes' countries are going to continue wanting to target authoritarian (China, Russia, Iran) and rogue states (North Korea, Syria) and states of concern (Libya, Iraq, Afghanistan). The ongoing instability along the Russian and Ukraine border is also a good example of the importance of having viable counter-espionage security intelligence collection efforts to better understand the secret (not public) agendas of foreign leaders. But the Snowden revelations, particularly those relating to the NSA intercepting very close allies such as German Chancellor Angela Merkel's cell phone, do show a lack of poor judgement. As President Obama commented in July 2013, no doubt in part to reduce the fall out in relations between Berlin and Washington, if he is interested in what Merkel thinks he will pick up the phone. While it is unlikely that no political leader would ever categorically rule out 'spying on other allies', the threshold for such a decision needs to be much higher and for exceptionally critical national security reasons – not just because the technology exists. So the Snowden leaks will influence the development of stricter policy and risk management guidelines, including most likely cabinet authority for future communication interceptions of political leaders who are close allies. The NSA Special Review recommended that a policy be established that would define the process on when intelligence can be collected against political leaders of friendly and allied countries.[63]

Beyond the four challenges discussed above, the Snowden revelations have sparked broader debate about the adequacy of existing oversight mechanisms for security intelligence collection; in particular, whether current mechanisms for oversighting collection that involves foreign and national targets are

[61]Edward Liu, Andrew Nolan and Richard Thompson, 'Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments', CRS Report 7-5700. Congressional Research Service, April 2014, p.2.

[62]Katherine Murphy, 'Attorney General to Decide Who is Charged Under National Security Plans,' *The Guardian*, 31 July 2014.

[63]See Recommendation 16 in Clarke et al., 'Liberty and Security in a Changing World', p.31.

sufficient to protect privacy and human rights. The 'hunters vs. passive' collectors ethos that arose across intelligence agencies after 9/11 is now being challenged in some 'Five Eyes' countries. In the US following on from Presidential Policy Directive 28, the Senate is set to vote on a new bill (the USA Freedom Act) in late 2014 which would no longer allow the NSA to systematically collect bulk metadata. Such data would have to stay with the phone companies and the NSA would instead need to get orders from the FISC to obtain call data on specific numbers. In Australia, the government has recently introduced a bill to parliament containing several intelligence reforms – particularly to boost ASIO's ability to monitor computers, computer networks and a mandatory data retention by companies to hold IPS and phone data for two years. A further interesting side to the suite of measures contemplated is to legislate against potential future Mannings and Snowdens from inside the intelligence community disclosing unauthorized intelligence. There is now a debate amongst Australian media whether they could under such legislation also be imprisoned for receiving any leaked intelligence.[64] Similarly, in July 2014, the UK Data Retention and Investigatory Powers Act (2014) was rushed through parliament further clarifying what the government argues are existing surveillance powers, but what privacy and some legal advocates suggest is providing intelligence agencies with powers well beyond the existing surveillance legislation (i.e. the RIPA 2000).[65] At this point, however, it remains unclear how recent post-Snowden legislative changes will precisely impact on how security intelligence collection methodologies are deployed against targets.

In addition to legislative changes, Snowden's revelations are also influencing other aspects of intelligence oversight and accountability, particularly whether current organizations, processes and institutions are effective in protecting privacy and upholding human rights. For example, the President's Review Group on Intelligence and Communications Technology suggested establishing an independent Civil Liberties and Privacy Protection Board (PCLOB) that could 'review government activity relating to foreign intelligence and counterterrorism whenever that activity has implications for civil liberties and privacy'.[66] The March 2014 release of the Kitteridge Review into New Zealand's sigint agency (Government Communications Security Bureau GCSB) – sparked by the discovery that GCSB had unlawfully intercepted communications of a New Zealand permanent citizen – has been the catalyst for a wider review of intelligence community arrangements including strengthening the capabilities of the country's main intelligence oversight body the Inspector General of Intelligence and Security.[67] The Snowden leaks now provide the opportunity for 'Five Eyes' governments to

[64]Ibid.

[65]Alan Travis and James Ball, 'Unprecedented New Powers in Surveillance Bill Campaigners Warn', *The Guardian*, 14 July 2014. See also, Data Retention and Investigatory Powers Act (2014), Chapter 27 (Explanatory Notes).

[66]Clarke et al., 'Liberty and Security in a Changing World', p.23.

[67]Rebecca Kitteridge, 'Review of Compliance at the GCSB', New Zealand Government, March 2013, p.50.

do a root and branch review of current organizational, ministerial, parliamentary and other standing oversight bodies to ensure they remain fit for purpose. As argued elsewhere, accountability mechanisms have grown organically rather than strategically over recent years. In particular in the US they have become increasingly fractured with little thought to the extent they remain effective and in some cases independent.[68]

We have identified a number of problems in relation to the targets of surveillance and data collection each of which warrants detailed attention; yet these tasks are beyond the scope of this paper. However, we do have a couple of suggestions in respect of the general approach to these issues:[69] (1) the clustering of nation-states and (2) a demarcation between government and security personnel on the one hand, and ordinary citizens on the other.

As discussed, under existing arrangements the 'Five Eyes' share information gathered from other states. These nation-states are, so to speak, allies in espionage; for example, they share intelligence. They are the members of our first cluster. There are, of course, other liberal democratic states outside the 'Five Eyes', such as various EU countries, which have 'shared core liberal democratic values' with one another and with the 'Five Eyes' and, specifically, a commitment to privacy rights. This is a second cluster.

The members of these two clusters ought to make good on their claims to respect privacy rights by developing privacy-respecting protocols governing their intelligence-gathering activities in relation to one another. Of course, determining the precise content of such protocols is no easy matter given, for example, that there are often competing national political interests in play, even between liberal democracies with shared values and many common political interests. But there does not appear to be any in-principle reason why such protocols could not be developed, and the fact that this might be difficult is no objection to attempting to do so. Since adherence to the protocols in question would consist, so far as it is practicable, in ensuring compliance with some of the standard moral principles protecting privacy and confidentiality rights, such as probable cause/reasonable suspicion and use of judicial warrants, these two clusters would essentially consist of an extension of the law enforcement model to espionage conducted within and between these countries.

Further, each of these nation-states would need to agree to, and actually comply with, the privacy respecting protocols in question. What of authoritarian states known to be supporting international terrorism and/or engaging in hostile covert political operations, including cyber-espionage, for example China and North Korea?

In respect of authoritarian states of this kind, the principle of reciprocity reigns: an eye for an eye and a tooth for a tooth. Accordingly, there are few, if

[68]Walsh, *Intelligence and Intelligence Analysis*, pp.231–2.

[69]Seumas Miller, 'Cyber-attacks and "Dirty Hands": Cyberwar, Cyber-Crimes or Covert Political Action?' in F. Allfhoff, A. Henschke and B.J. Strawser (eds.) *Binary Bullets: The Ethics of Cyberwarfare* (Oxford: Oxford University Press 2014).

any, constraints on intelligence-gathering and analysis, including cyber-espionage, if it is done in the service of a legitimate political interest such as national security. Nevertheless, it is important to demarcate within such an authoritarian state between the government and its security agencies, on the one hand, and private citizens, on the other. Notwithstanding the applicability of a reciprocity principle, the need to respect the privacy rights of private citizens in authoritarian states remains; perhaps all the more so given these rights (and, for that matter, human rights in general) are routinely violated by their own governments.

So a stringent principle of discrimination ought to govern espionage directed at authoritarian states. At the very least, the citizens of these states ought to be able to differentiate between morally justified infringements of the privacy and confidentiality rights of members of their government and its security agencies, on the one hand, and violations of their own privacy and confidentiality rights, on the other, and be justified in believing that whereas the former might be routine the latter are few and far between.

Conclusion

In this article, we argue that in the wake of Snowden a more nuanced understanding of the ethical and policy dilemmas confronting security intelligence collection by 'Five Eyes' countries is required. We have provided a schematic framework (*methods, context* and *target*) in which to make sense of the different ethical and intelligence practice issues arising from various types of security intelligence collection. As the current security environment, particularly in the Middle East, becomes more complex, policy makers and heads of intelligence agencies will need to do a better job of 'taking their citizens with them' when arguing the case for the application of various new security intelligence methodologies. From a policy maker's perspective we have in mind the need for politicians (of all persuasions) to allow sufficient time for the careful explanation of benefits versus costs of any additional security intelligence collection measures. This means clearly making the case for new measures and allowing sufficient time for public and legislative debate. Heads of intelligence agencies also now have an increasing role (whether they like it or not) to explain and educate the public about why additional legislative or policy steps may be necessary and how they will seek to maintain public trust. In late 2014, the outgoing head of ASIO did a good job in various media appearances explaining from his perspective the merits of new metadata retention legislation in Australia. The Snowden leaks also mean that heads of intelligence agencies will need to show more openness than traditionally has been the case in discussing the ethical and policy impact of security intelligence collection practices. This will be a cultural shift for some. It is also clear that accountability mechanisms across many 'Five Eyes' countries also need to be reviewed. The overview of the ethical and policy dilemmas presented here is only a first step. What is also needed is a further conceptual and empirical investigation of specific security intelligence collection policies and procedures across the 'Five Eyes'. Only then will it be

possible to identify common ideas/characteristics/components that could go into an ethically informed set of policy guidelines to help decision makers better navigate between citizen's two basic rights – security and privacy.

Notes on Contributors

Dr. Patrick F. Walsh is a former intelligence analyst who has worked in Australian national security and law enforcement intelligence environments. Since 2003, he has been a senior lecturer, intelligence and security studies at the Australian Graduate School of Policing and Security, Charles Sturt University, Australia. He is course coordinator for the post-graduate intelligence analysis programme and has taught widely across Australia and internationally. Patrick is also a consultant to government agencies on intelligence reform and capability issues. His most recent book, *Intelligence and Intelligence Analysis* (Abingdon: Routledge, 2011) examines a range of intelligence reform issues post 9/11 across Australia, Canada, New Zealand, the US and UK.

Seumas Miller is a professorial research fellow at the Centre for Applied Philosophy and Public Ethics (CAPPE) (an Australian Research Council Special Research Centre) at Charles Sturt University (CSU) (Canberra) and the 3TU Centre for Ethics and Technology at Delft University of Technology (The Hague). He is the Foundation Director of CAPPE, Foundation Professor of Philosophy at CSU, and served two terms as a head of the School of Humanities and Social Sciences at CSU. He is the author of co-author of over 200 academic articles and fifteen books, including *Social Action* (Cambridge University Press, 2001), *Corruption and Anti-corruption* (Pearson, 2005), *Terrorism and Counter-terrorism* (Blackwell, 2009), *Moral Foundations of Social Institutions* (Cambridge University Press, 2010) and *Investigative Ethics* (Blackwell, 2014).