Charles Sturt University

AUSTRALIAN GRADUATE SCHOOL OF POLICING AND SECURITY
FACULTY OF BUSINESS, JUSTICE AND BEHAVIOURAL SCIENCES

PO Box 168
Manly NSW 1655

PH: 02 9932 5210

RE: 2017 INDEPENDENT INTELLIGENCE REVIEW

Dear Mr. L'Estrange AO and Merchant PSM,

Attached is my submission to the 2017 Independent Intelligence Review. I have also attached two recent articles relevant to some aspects of answers provided which may be of some interest.

As a former intelligence analyst and now researcher in the area of intelligence reform, I do hope that my submission will be of some assistance. I am happy to meet with you personally to discuss this submission or other matters pertaining to the review if this would help too. I can be contacted by email (pawalsh@csu.edu) or mobile (0409042964).

I wish you the best of luck in this important review of our intelligence community.

Yours faithfully

Patrick F Walsh

A/Prof Patrick F Walsh
Associate Professor
Intelligence and Security Studies
21 December 2016

2017 Independent Intelligence Review Submission

Associate Professor Patrick F Walsh

Associate Professor, Intelligence and Security Studies

Australian Graduate School of Policing and Security

Charles Sturt University

pawalsh@csu.edu.au

Key recommendations

- Consider appointing an assistant minister for intelligence and security, to oversee regular intelligence governance issues (e.g. AIC tasking and coordination, priority setting, capability development, collection and assessment challenges).
- Consider commissioning an in-depth and independent review of AIC workforce planning to provide advice to government on how to prepare for the recruitment, and retention of the next generation of intelligence staff.
- The National Intelligence Community Training Secretariat (PM&C) should establish an education and training advisory committee with universities for the purposes of providing the government with advice on intelligence education and training development for the AIC.
- PM&C should provide a more strategic approach to the identification and coordination of AIC related research priorities and promote regular opportunities to disseminate this to universities and other relevant research institutions.
- Consideration should be given to extending the oversight powers of the PJCIS to allow operational review of *certain* AIC capability development activities.

2017 Independent Intelligence Review Submission

Associate Professor Patrick F Walsh

Associate Professor, Intelligence and Security Studies

Australian Graduate School of Policing and Security

Charles Sturt University

pawalsh@csu.edu.au

- **How the key aspects of our security environment and the nature of security threats have changed in recent times, including as a result of technological advancements, and how they are likely to change further over the coming ten years or so.**

The Australian Intelligence Community (AIC) operates now in a 'post-post 9/11 security environment–meaning the environment is less certain and more complex than it was in the initial years after 9/11. This is the case for a number of state and non-state actor threats. For example, in the case of the later, the immediate post 9/11 security environment (2001-2006) was largely dominated by Al Qaeda and its other franchisees across Africa and the Middle East. The AIC and other 'Five Eyes' partner countries demonstrated a degree of adaptation to this more diffuse threat environment. However, since the last intelligence review (2011) there has been a further splintering of transnational terrorism from the creation of ISIS to localised inspired lone wolves. Additionally, other long standing threats from global outlaws (e.g. arms traders, people smugglers, drug trafficking) continue to evolve in less predictable ways despite the best efforts of intelligence and law enforcement operational interventions.

The AIC's ability to respond to the global outlaws (or non-state actors) is also being challenged by a resurgence in a number of traditional state based threats, particularly in the last five years. These include an increasing bellicose Russia, a growing assertive and imperialist stance by China in the South China Sea and the dangerous proliferation efforts by North Korea. The unpredictability and fragility of political and economic institutions of important nearby neighbours continues to occupy the bandwidth of the AIC including PNG, Indonesia and the South Pacific.

In the next ten years, we are likely to see the continuation of the struggle against Islamo-facism. Loose virtual or physical extremist Caliphates will continue to come and go–facilitated by social-media, elaborate terrorism financing networks and political volatile fragile states such as Iraq, Syria, Libya, Afghanistan, Pakistan and Northern and Eastern Africa. State based threats will endure and in the case of China, the AIC

will play a vital role in helping the National Security Committee of Cabinet better understand both the opportunities and challenges in reconciling Australia's political and economic interests with a rising China.

Finally, the use of technology as an enabler of state and non-state threats will continue to further challenge the AIC's collection and analytical capabilities. Since the last independent review, we have seen how the capabilities of Australian and Five Eyes partners has been playing catch up in understanding how social media is being used politically (e.g. the Arab Spring) or in politically motivated violence for propaganda, recruitment, communications and targeting coalition forces (e.g. ISIS). Similarly, there has been a growing number of cyber-attacks and cyber-espionage from state and non-state actors. The AIC's ability to collect and assess cyber-threats has improved particularly with the development of the Cyber Security Operations Centre (CSOC) in 2010 and a growing government policy attention on cyber with the launch of the Australian Cyber Security White Paper in 2016. While progress has been made with CSOC, I have concerns about the overall capabilities of the AIC's collection and analytical workforce in cyber and other technology areas (including biotechnology), where more needs to be done to recruit and retain appropriately trained collectors and analysts from the private sector and scientific community. I will return to workforce issues in the next section.

- **How effectively the AIC serves (and is positioned to serve) Australian national interests and the needs of Australian policy makers.**

On the whole, the AIC does a good job of serving Australian national interests and the needs of Australian policy makers. The six core AIC agencies work well together in collecting and assessing against policy maker set national intelligence priorities. The habits of cooperation and coordination across the AIC has improved significantly since 9/11, particularly in areas which remain top priorities for government such as terrorism, maritime illegal immigration and cyber. This is in contrast to the US intelligence community, which has over double the agencies–making cooperation and coordination challenging in some areas between certain agencies (e.g. DHS vs. FBI and ODNI vs DOD). This is not to suggest that improvements in integration and coordination of intelligence capabilities across the US intelligence community has not improved. There have been some real improvements particularly under the outgoing DNI Jim Clapper and CIA Director Jim Brennan. Though the sheer size of the US Intelligence community and longstanding differing organisational cultures makes cooperation, coordination and de-confliction of missions sometimes challenging. It is even more challenging in the US if one also considers how the US intelligence community works with some 18000 city, state and tribal law enforcement agencies. The scale of the US intelligence enterprise, conflicting jurisdictional interests, legislation and differing capabilities all impact on the kind of collection and assessments senior decision makers receive.

Nonetheless, the volume, tempo and complexity of work now confronting the AIC underscores the need for periodic reviews such as this one as well as the AIC adopting a continuing improvement ethos. While it is unrealistic to expect that the AIC will be

able to interpret every potential threat/risk and warn policy makers every time, the intelligence community does need to continue to score highly on providing decision-maker support on those issues most vital to Australia' interests (including but not limited to: state based threats, terrorism, illegal immigration, WMD proliferation and cyber threats).

The AIC will only continue to effectively serve Australia's interests if it can demonstrate a growing ability to adapt to changes in the security environment. Serving Australia's interests and the needs of its policy-makers will always rely on how well heads of AIC agencies and the broader national security policy making process are able to reduce uncertainty and provide warning for policy makers. Anticipating changes in the security environment as well as understanding where policy maker's interests and knowledge deficits lie will remain critical. Equally of importance, however will be how intelligence leaders across the AIC are able to structure the community and the six core agencies to ensure that their operations are flexible, integrated and adaptive to the ever changing security environment. These issues are expanded further on in the next section.

- **Whether the AIC is structured appropriately, including in ensuring effective coordination and contestability**

I am pleased that Mr L'Estrange AO and Mr Merchant PSM are examining AIC structural issues. Reflecting back on my own career in ONA, the NCA and ACIC and now for 13 years as a researcher on intelligence reform, I believe that organisational structure is critical to understanding capability issues within intelligence communities and whether they can adapt to the changing security environment.

Organisational structural issues need to be examined holistically. Below I discuss briefly one way to consider whether the AIC is structured appropriately based on research I have completed. I hope that this approach might be of some use to the reviewers in their deliberations on 'structure'. In 2011, I developed a theoretical model (called an effective intelligence framework), which provides a diagnostic tool for exploring whether an intelligence organisation or community is operating effectively– as well as the extent to which it is likely to show signs of adaptability and sustainability. There is no need here to provide a full explanation of the model, though I have attached a recent article which explains it in greater detail (See, Appendix A). In summary, it was developed by interviewing 61 senior intelligence leaders across the 'Five Eyes' intelligence communities and by examining five specific intelligence contexts across the Five Eyes.[1] The research resulted in a modal (the effective intelligence framework), which incorporated both structural and functional aspects of each intelligence context studied.

As shown in Figure 1, all intelligence contexts regardless of parameters (national security, law enforcement, military, and private sector) are concerned with interpreting threats and risks in the security environment so this central concern is represented in the middle. It is the raison detre for any intelligence effort.

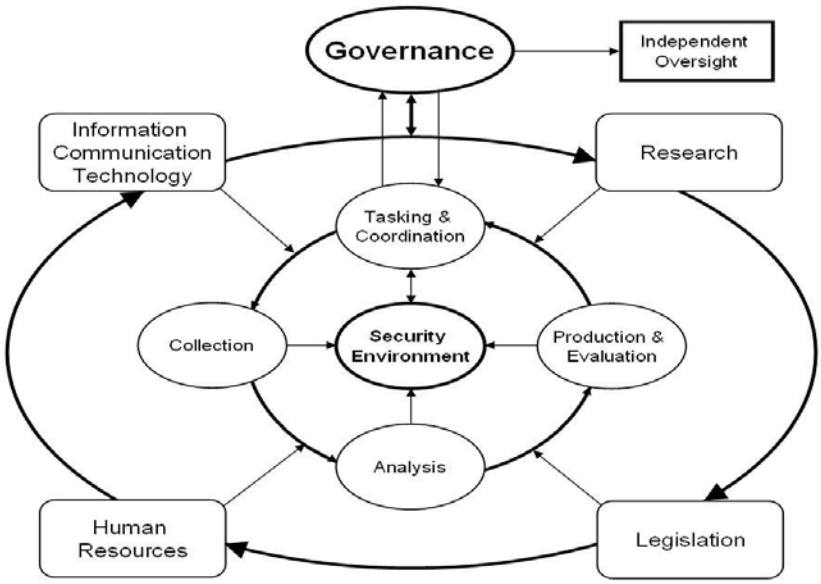


Figure 1: Effective Intelligence Framework

Source: Walsh, Intelligence and Intelligence Analysis, p. 148.

The framework is then completed with two additional overlays. The inner circle consisting of *tasking and coordination*, *collection, analysis,* production and evaluation are the ***core intelligence processes***, or the major process activities involved in the 'assembling of intelligence products'. The outer circle consisting of *governance, ICT, human resources, legislation and research* are the **five *key enabling activities*** of the intelligence enterprise. These are the *structural comp*onents of any intelligence framework, which support the core intelligence processes.

In short, without the *key enabling activities* it would be impossible to produce intelligence products. The naming convention of each key enabling activity is mostly self-explanatory. For example, *ICT* is concerned with all the information architecture and ecology used in the agency/community–and *human resources* includes workforce planning, recruitment and other activities such as continuing professional development. Full descriptions of each core intelligence process and key enabling activity can be found in Walsh.[2]

The most important aspect of the effective intelligence framework is *intelligence governance,* which I define as a 'set of attributes and rules pertaining to strong sustainable leadership, doctrine design, evaluation and effective coordination, cooperation and integration of intelligence processes[3]. Ultimately effective intelligence governance–relies on sound organisational (and community) leadership that can marshal both an organisation's core intelligence processes and key enabling

activities in ways that make organisations and communities responsive, effective, adaptive and sustainable as the security environment changes.

Intelligence governance has an external and internal dimension. External governance is that imposed on the intelligence leader by the political leadership. It could be cabinet level prescribed national intelligence collection priorities or a new ministerial directed mission. Internal governance are activities, policies, processes and initiatives that the intelligence leader is able to influence directly.

The reason I have included this framework here is not to be overly academic, but to provide the reviewers with another way to look at this issue of 'appropriate structure'. The key point is that while the reviewers will necessarily need to look at aspects of the AIC structure, this modal suggests that any review of the structure of an intelligence community needs to consider both the functional aspects (*the core intelligence processes*) and the structural aspects together (*key enabling activities*) which supports outputs from both agencies and the wider community. For example, the quality of intelligence products is influenced by training and experience (human resources) just as collection platforms rely on whether ICT architecture is fit for purpose. In addition to examining all core intelligence processes and key enabling activities separately and together, reviewing 'intelligence governance' across the AIC will be the most important way to assess whether structure is fit for purpose yet adaptable to the changing security environment.

One important area of intelligence governance that has gained prominence across Five Eyes countries is intelligence fusion or integration–both within and across agencies. In the US there are now over 70 fusion centres, which attempt to provide a connection between local/state (mainly law enforcement agencies) and some agencies of the US intelligence community. A key rationale for their establishment in the US was to avoid intelligence falling between the cracks and ensuring better sharing of intelligence post 9/11.

Since 9/11, the AIC has also either strengthened existing 'fused' arrangements or established new ones such as the National Threat Assessment Centre (NTAC) and the Counter-Terrorism Control Centre (CTCC) based in ASIO and the CSOC located in the ASD. While the 2011 reviewers (Cornall and Black) assessed that these key fused arrangements were working well, they did make the point that they would need to adapt in response to the future challenges they face.[4]

My own research into fusion centres in the US and official congressional reporting in recent years does suggest that in some contexts, just throwing people from different agencies together does not always mean better intelligence results than if the staff stayed located in their home agencies. It has been found that fusion sometimes, ironically leads to circular collection and reporting, poor analysis and unclear governance arrangements around shared resources.[5]

This is not to suggest that fusion efforts across AIC agencies are significantly flawed, however, given how dynamic the security environment has become, it would be useful for the reviewers to investigate the health of governance arrangements of key AIC

fusion arrangements. Fused terrorism, cyber and border protection are areas that warrant close attention, but others where there is cross-over from the AIC to law enforcement agencies (organised crime, financial intelligence and even biosecurity) would be worthwhile investigating. In particular, useful issues to examine would be:

- How are fused arrangements resourced by contributing agencies and do financial constraints impact on any agency's ability to cooperate and coordinate in the fusion centre?
- How are collection, analytical and operational priorities decided and how is this different from the process delivered from parent agencies?
- To what extent do fused arrangements work according to a common doctrine or concept of operations in order to promote better governance and intelligence processes/outcomes?
- What challenges are there in sharing in real time sensitive information particular to non-core AIC agencies such as the ACC, AUSTRAC, ATO or Department of Immigration and Border Protection?
- Are there any unnecessary ICT architectural or cultural constraints to sharing intelligence to appropriately cleared personnel in non-AIC agencies?
- To what extent are fused arrangements producing the right blend of products (tactical, operational strategic) for decision-makers and are there any gaps in current products being disseminated?
- Do any heads of agencies see the need for additional specialised fused intelligence groupings and why is such a structure necessary compared to informal ways of sharing collection or analytical resources such as inter-departmental committees or task forces? (For example, an argument could be made for a fusion centre for financial intelligence that promoted greater alignment between the AIC, ACIC, AFP and AUSTRAC on organised crime and countering terrorism financing).

As far as investigating AIC structural issues is concerned, these go beyond an investigation of fused arrangements. As discussed earlier, we have seen in the US a number of intelligence leaders (Lt Gen Flynn (former head of DIA now incoming NSA under Trump Administration) John Brennan (outgoing Director of CIA) and Jim Clapper (outgoing DNI) all attempt to integrate capabilities within and between intelligence organisations.

In interviews with heads of AIC agencies it would be useful to get a sense of what organisational structures individual agencies are adopting in order to better manage the complexities of the security environment. Do they see a greater integration between collection and analytical assets in some agencies as the best way forward?, What capabilities within their agencies (e.g. collection and analytical) would be better integrated under similar missions as John Brennan has attempted to do in the CIA, and what capabilities are best dealt with on an issue or geographic region basis? There will be no one size fits all approach across the six AIC agencies whose functions and missions overlap though have different roles. I think getting the heads to reflect on

whether current *internal* governance arrangements are fit for purpose would be an important output for the review.

Not all capabilities need to be integrated to improve the structural response of AIC agencies and the broader community. Sound intelligence governance is also the sum of effective leadership attributes as well as appropriate organisational reform.[6] It would be useful, then for the reviewers to look at how heads of agencies set strategic directions, build organisational trust and employee buy in as well as how they drive developments in both core intelligence processes and key enabling activities such as human resources, ICT and legislative reform.

The effective governance of the AIC is not at some adverse tipping point. Nonetheless the growing complexity of the security environment, limited resources, and the nature of many threats and risks that require an all-hazards approach means continuing to build effective intelligence governance is vital. Coordination mechanisms already exist between AIC agencies and in PM&C (e.g. the National Intelligence Coordination Committee) to monitor governance particularly coordination and priority setting issues. But truly effective intelligence governance requires a more detailed ongoing monitoring of both the *core intelligence proces*ses and *key enabling activities* of the AIC (see Figure 1).

The PM&C should continue its current role of facilitating and monitoring a range of governance issues, though I would argue overseeing intelligence governance if it is to be effective also requires direct ministerial oversight. There is a level at which decisions about intelligence reform (or even addressing challenges) need to be deferred to a relevant minister. The Prime Minister's office is likely in most cases not the most appropriate venue for taking on the oversight of day to day governance oversight of the AIC. However, consideration should be given for the appointment of an assistant minister for intelligence and security, who can speak with the authority of the Prime Minister and National Security of Cabinet to advise on intelligence development and oversee regular intelligence governance issues (e.g. AIC tasking and coordination, priority setting, capability development, collection and assessment challenges).

The assistant minister could also with the advice of PM&C, proactively evaluate capability gaps (e.g. training/workforce planning, technological constraints, legislative problems, research priorities) to ensure the AIC continues to have the structure most appropriate for the evolving security environment. The objective is not to replace the Prime Minister, Defence, Foreign Minister or Attorney General's responsibilities for individual AIC agencies, rather to ensure that there is ministerial oversight over governance issues that impact *all* agencies across the entire AIC. In other words, the minister would identify coordination, and capability gaps across the entire community. The Assistant Minister for Intelligence and Security could chair a regular meeting with Heads of agencies to provide advice to them on the government's changing collection priorities and intelligence policies. Equally, the committee could be an opportunity for heads of agencies to lobby for new capabilities, legislation or policies that are directly relevant to the entire AIC. The appointment of the assistant minister would not mean that the independent review of the AIC every 5 years was no longer required. Such

reviews should continue to be part of the institutional arrangements of AIC accountability and oversight, though the assistant minister would play an important role in corralling and coordinating efforts to ensure the AIC's structure and institutional arrangements are appropriate between independent reviews.

- **Whether legislative changes are needed, including in the *Intelligence Services Act 2001***

The ISA Act 2001 overall, continues to serve ministers and AIC agencies well in outlining their roles and functions in a general sense. Other than three possible scenarios, I cannot envisage major changes being required in the foreseeable future. The first scenario would be if the government appointed as suggested above, an assistance minister for intelligence and security then this role would need to be reflected in the Act. Second, I argue below for a greater role by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). Again this would require amendments to the ISA Act. Finally, though very unlikely in the next few years, the ISA may need amending if the Government wanted ASIS to play a greater role in para-military drone attacks in declared and undeclared war zones.

However, it is the large volume of new or amended legislation particularly related to counter-terrorism that has created a more complicated operating environment for many AIC agencies.[7] I believe on balance that many of the new powers in recent legislation (e.g. control orders, preventative detention, proscribed regions and data retention) are necessary to allow the AIC and the broader intelligence enterprise including the AFP to proactively collect intelligence and disrupt terrorist plots. Nonetheless, the volume and complexity of counter-terrorism legislation alone and the ability by the AIC to operationalise it all consistently correctly needs ongoing monitoring.

I am not suggesting that AIC staff would be deliberately violating provisions of CT acts, rather I believe there may be some cases where confusions around some legislation could be presenting challenges to some agencies. For example, the Clarke Inquiry into the wrongful arrest and detention of Dr Haneef in 2007 demonstrated a lack of knowledge of amendments (Divisions 104 and 105) to the Criminal Code by the AFP. Although the AFP is not a core AIC agency it is nonetheless part of the broader intelligence enterprise, and it would be useful for the reviewers to discuss with heads of agencies if there has been any challenges in using new powers ascribed in amended or new legislation since the last review period. No doubt the IGIS will also be able to comment on this. Compared to other Five Eyes partner countries, Australia is considered to have a very muscular legislative response to many evolving threats such as counter-terrorism, organised crime and illegal immigration. Many of the proactive and flexible powers enshrined particularly in counter-terrorism legislation since 9/11 have sunset clauses which are appropriate in a liberal democracy.

The PJICS, government and IGIS will continue to play their vital roles in reviewing sunset clauses in a range of post 9/11 CT legislation. More broadly, these oversight and accountability institutions will need ensure that legislation which lowers the

threshold for probable cause or reasonable suspicion remains proportionate to the evolving threat yet preserves as much as possible the privacy of law abiding Australians. Finally, in the broader context of oversight of relevant legislation, it would be worthwhile for the reviewers to discuss with the IGIS and Commonwealth Ombudsman whether they saw any conflict between their review roles articulated in recent CT legislation such as the Foreign Fighters Act and Data Retention Act.

- **Whether capability gaps, including technological, are emerging and how these might be met, noting potential efficiencies and that any new proposals would need to be consistent with the Government's overall fiscal strategy**.

As noted earlier, my effective intelligence framework is one way to conceptualise capability gaps across the AIC and its agencies. From the broadest perspective, there are likely to be capability gaps in different areas of the *core intelligence processes* (tasking and coordination, collection, analysis, production and evaluation) and the key enabling activities (governance, ICT, human resources, legislation and research).

I am sure that the reviewers will examine each of these areas for where vulnerabilities and gaps are located. Technological capability generally is an area that any intelligence community is trying to build as the security environment becomes more complex. For example, since 9/11 there has been a significant increase in the investment in data mining and analytics in both national security and law enforcement agencies, though I do not see a common or coordinated effort in this area across the AIC.

In the sigint space, much of this early investment was an attempt to collate the massive amounts of data as much as it was to try and analyse it. The trend now is with knowledge discovery and even more ambitiously predictive analytics. Much is promised, particularly by the vendors of platforms, but the use of such technology including social media/sentiment analysis is still being used to varying degrees of effectiveness and understanding across the AIC. It would be useful for the reviewers to examine how data mining and analytics technologies are being deployed across the AIC, where challenges reside and whether there are opportunities for more coordinated approaches to their deployment across the community. This investigation may well be best completed as a standalone follow up to the general review. However, in this section on capability gaps, I wish to focus on two key enabling activities (human resources and research) where I argue gaps remain in performance.

Human resources

Human resources includes key issues such as: workforce planning, continuing professional development and recruitment/attrition. I have studied these issues across the 'Five Eyes' and each country is confronted with similar human resourcing challenges. Workforce planning remains an ongoing capability issue for the AIC. There is no quick fix nor can AIC agencies plan to recruit for every potential evolving threat

in the security environment. Though we have seen that some AIC agencies over the last decade have been caught short in developing capabilities in particular collection and analytical roles. For example, many non-military AIC agencies have only recently started to develop or recruit more cyber skilled staff. There are other specialised areas such as biosecurity and biotechnology, financial crime, forensics and language skills where AIC agencies continue to struggle to attract, train and retain qualified staff.

Another related workforce issue, which impacts on analysts is the debate on whether agencies need more generalist vs subject matter experts–the former getting rotated around to work on different issues while the later tends to stay in the one area. This issue remains a big debate in the US intelligence community with recent moves in the CIA to move analysts around to different accounts compared to the INR (State Department) where analysts tend to specialise. There are pros and cons for each argument and likely a balanced approach is what is needed. But the concern in the US has been that many analysts are increasingly not experts in anything, which impacts on the kinds of judgments they are able to make on complex issues.

The ONA has always had a good track record of employing analytical expertise, but in other areas of the AIC it is likely that there are more generalist analysts. Again it would be useful to investigate how decisions are made about the mixture of generalist vs specialist staff. A useful outcome of independent review would be to recommend to government that a further independent review of AIC workforce planning issues is completed to provide advice to government on how the community can best plan for recruitment and retain the next generation of intelligence staff. This review could also investigate strategies for how the AIC can attract this next generation of staff particularly in specialised areas (cyber, science and technology) where potential candidates have often better remunerated options in the private sector. An AIC wide investigation into workforce planning issues is needed as each member agency tends to plan (quite naturally) for their own needs rather than what the whole community requires.

The other human resources issue that needs investigating is AIC intelligence training and education capabilities. Some agencies in the AIC such as ASIO and ASIS have well-articulated entry level intelligence officer training, while in others less formal training pathways exist. A more strategic approach to education and training is required across the AIC. By this I mean common training and competency standards should be agreed upon for different roles (e.g. analysts, collectors, managers, generalists vs specialists) so that all intelligence staff meet broad basic standards and have skills that are transferable (except in specialist roles) to another agency. The Australian law enforcement community has also been plagued by the same issue though in the last year has started to examine common standards for intelligence analysts. I have been involved in this process.

Another issue is that perhaps with the exception of defence, which offers a number of intelligence courses for its staff through the Defence Force School of Intelligence at Canungra, there are is still a lack of a strategic approach to intelligence training across the AIC. What seems to be missing is a coherent professional development pathway for AIC staff that provides solid introductory training to working in the AIC, specialised

training and clear articulation pathways to higher education courses in the area of intelligence or related national security areas. The National Intelligence Community Training Secretariat (located in Department of Prime Minister and Cabinet) hosts a short introductory course to the AIC and sponsors a diverse range of courses from cyber to radicalisation that members of the AIC can attend.

However, the introductory training course is mainly an introduction to the roles and functions of each of the AIC agencies, and there does not seem to be a strategic approach to how other training is hosted by the Secretariat. This is not to blame the Secretariat, it is a small unit taking whatever directions it gets from heads of agencies, though I suspect executives have not been as engaged in identifying strategically common training standards given other pressing operational matters. The current real lack of a strategic approach to training and education standards across the AIC does not suggest that individual AIC agencies should do away with their own intelligence officer training which suits their unique circumstances. Internal training however, is only one aspect of someone's continuing professional development in the AIC. There also needs to be some (community wide) basic analytical and collection training offered to ensure common standards. This should be amplified by other training opportunities in areas where individual agencies may not have the capacity to train staff and are of common interest to all agencies in the community including in: languages, data mining/analytics, strategic intelligence, national security policy making, counterintelligence, leadership/management.

While my own University has a long history with intelligence training for security and policy agencies (since 1999) as does the National Security College (ANU), more work is needed to help create continuing professional development pathways for AIC staff to attract, retain and re-skill as necessary. I do not think we need to go down the US route and create a National Intelligence University at great expense. Nonetheless, it would be advantageous if the National Intelligence Community Training Secretariat could establish an education and training advisory committee with universities who have developed credibility with intelligence training to mutually share latest developments in training and education and to help develop a continual professional development pathway that all AIC agencies can benefit from.

Research

In my 2011 book *Intelligence and Intelligence Analysis*, I dedicated an entire chapter to research in the intelligence context. The chapter argued that while intelligence practice has always been informed by the physical and social sciences, intelligence related research has often been disaggregated, adhoc and completed in secrecy. There will always be sensitivities around some research commissioned by the AIC– particularly in collection/interception technology, counterintelligence and defence areas. Such research will likely always need to be done in-house by the AIC or DSTO. Though there are many areas across the *core intelligence processes* and *key enabling activities* (see Figure 1), which would benefit from more explicit and strategic partnerships between researchers in universities and the AIC. There a number of research partnerships that could be formed to work on an unclassified basis on issues relevant to the AIC. For example, just taking the first two parts of the *core intelligence*

processes (tasking and coordination and collection), AIC-university partnerships could investigate: better modelling of risk and threat methodologies, evaluate the impact of structure analytical techniques on decision-making, evaluate the use and integration of forensic data, biometrics, health, corrections and private sector information into AIC systems and, develop better early warning surveillance systems, border security detection and biosensor equipment) for the AIC and broader law enforcement agencies.

Additionally from a *core intelligence processes perspective*, there is an almost endless number of complex analytical problems that the AIC could partner with appropriate research institutions. These include but are not limited to: radicalisation, country studies in strategic areas, identity fraud, and money laundering methodologies, biotechnology and bioterrorism. Many of these areas are being explored by researchers currently, but there needs to be more opportunities to investigate complex threat issues in partnership with the AIC thus ensuring that outcomes and impact are relevant for the community.

Key enabling activity areas for possible AIC-research community partnerships could include: cyber resilience of ICT systems, improving predictive analytics and social media sentiment analysis, evaluating educational and training standards, evaluating governance issues around fused intelligence practice.

Historically, the AIC has been more insular and risk adverse in its approach to external research collaboration than other Five Eyes partners such as the US and Canada. The Canadian Security Intelligence Service (CSIS) has had for many years an academic outreach program, which actively engages with the academic and research community. I have had dealings with them over the years and their work on sponsoring workshops on complex strategic issues is bringing dividends for both CSIS in getting access to experts, but also building strong links with the academic community. ASIO and ONA could consider a similar program in Australia.

Australia does not need to establish the equivalent to the US Intelligence Advanced Research Projects Activity (IARPA) initiative to marshal government, researcher and intelligence community resources for intelligence research, however, the AIC needs a more strategic approach to setting research priorities. The Information Sharing and Intelligence Division of PM&C is probably the right functional area to identify national security and intelligence research priorities and provide this information to universities and other relevant research institutions. PM&C has provided in the past a national security science and innovation strategy, which listed some intelligence related research priorities. It would be excellent if PM&C could provide an annual national security and intelligence research priorities list that will guide researchers when applying for research grants. PM&C may also like to consider establishing a committee where key university researchers operating in the intelligence area can discuss intelligence relevant research as well as work with AIC representatives to ensure research is relevant and impactful. Intelligence related research should also be highlighted as a national research priority by the Australian Research Council.

- **The effectiveness of current oversight and evaluation arrangements**

The AIC has all the necessary levels of oversight: legislative, ministerial, parliamentary and independent. Evaluation is part of oversight at each of these levels, but it is also a function of good leadership (intelligence governance) and monitoring by PM&C. Legislative oversight is currently working reasonably well though all levels (ministerial, parliamentary and independent) must continue to be engaged in monitoring that the AIC's operational activities conform to all relevant legislation not just the ISA Act 2001. As noted earlier, since 9/11 successive Australian Governments have introduced or amended several pieces of legislation that provide the AIC and law enforcement agencies greater powers particularly in counter-terrorism and to some extent organised crime. It would be useful for the reviewers to interview the independent monitor on national security legislation to assess whether the expansion in legislation remains appropriate and where key challenges remain in the AIC's use of new or amended legislation.

Similarly, the Inspector General of Intelligence and Security (IGIS) will likely also have an opinion on current/anticipated challenges to recent legislation (particularly that enacted in the Abbott/Turnbull Governments). Certainly the role and funding of the independent monitor on national security legislation has been inconsistent since its creation under the Gillard Government in 2011. I see that the independent monitor and IGIS together can play a vital role in ensuring that not only does the AIC operate within the letter of legislation, but that any breaches (however unintentional most will be) are reported and rectified quickly.

Parliamentary oversight is mainly conducted through the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and to a lesser extent the Parliamentary Joint Committee on Law Enforcement for the AFP and ACIC. The PJCIS has increasingly played a more active role in the oversight of intelligence related administration, expenditure and legislative matters. In particular, I believe the PJCIS has played an effective bi-partisan role in providing reasonable amendments to the Foreign Fighters and Data Retention Acts in 2014. Over the next few years, the PJCIS is expected to continue to play a key role in the reviewing a number of the proactive intelligence collection provisions included in recent counter-terrorism legislation such as ASIO's questioning detention powers, control and preventative detention orders and declared areas. The PJCIS role in legislation oversight is welcome and helps build trust between the Australian public and the government that the AIC is accountable in its operations.

However, the ISA Act, which established the PJCIS does not allow it to initiate its own inquiries into the AIC, review the operations of AIC members; including assessments made by ONA and DIO or review coordination efforts by the ONA. The Parliamentary Joint Committee on Law Enforcement allows in contrast a bit more leeway for it to examine the operations of the AFP and ACIC. While, the PJCIS gets some idea about the operations of the AIC through reviewing agency annual reports and regular testifying on a range of matters by heads of AIC agencies, the question is should it have the ability to commission its own inquiries without ministerial approval or regularly

review classified operational matters in the manner of the two US Congressional Intelligence Select Committees?

The US Congressional oversight committees rose in the last 1970s on the back of the excesses of executive over-reach particularly with the role played by the CIA and FBI in illegal or unaccountable intelligence operations domestically and foreign. Oversight committee members do receive regular classified intelligence briefings and regularly conduct self-initiated inquiries into all aspects of US intelligence community operations not just on budget or administrative matters. Historically, the overall effectiveness of Congressional oversight has been mixed. Some committees have been fully engaged and have helped the intelligence community identify issues before they result in failure. However, others have been marred by bitter partisan-ship or members have been disinterested in providing effective oversight. For many US politicians being on either the House or Senate intelligence oversight committee is considered a mixed blessing as the nature of secrecy means members are not able to attract the same political limelight they may working on other committees with more public legislative agendas.

Given the US experience, I do have mixed reservations in considering whether the PJCIS should be given more power to self-initiate inquiries and receive regular classified briefings (even if the latter are done behind closed doors). I would particularly be concerned that national security and intelligence became a political football by extending such powers. However, we have to recognise the public trust levels in the intelligence communities of liberal democratic states has decreased significantly since 9/11. The WikiLeaks episode and the Snowden leaks exacerbated an already underlying tension in the community between privacy and secrecy. Added to this tension, is both the growing complexity of intelligence related legislation with greater powers and several public, judicial or independent inquiries into various episodes of ‘intelligence failure’ across the ‘Five Eyes’ countries. The net effect has been that intelligence issues and policy making are much more in the public discourse than pre 9/11. The public is increasingly educated about intelligence matters. It wants to be reassured that the AIC is operating lawfully, ethically risk manages operational decision-making, and is value for money just like any other government entity.

Right now there are gaps in oversight and evaluation in what operational aspects of the AIC can be reviewed. IGIS has very strong coercive powers to investigate a range of operationally related matters, but these relate largely to their legality, and whether they comply with human rights and ministerial guidelines. IGIS has in the past reviewed issues that go to operational performance such as whether ONA assessments were politicised though generally its mandate is not to evaluate *specific aspect of intelligence practice or capability* including issues discussed earlier such as intelligence coordination, workforce planning. These issues tend to get investigated less frequently and usually only as part of the independent review process every five years.

I do believe that despite it being seen by some as a major shift in the PJCIS’s functions, consideration should be given to extending the oversight powers of the Committee to allow operational review of ***certain*** AIC activities. An extension of oversight powers

would mean an amendment to the ISA Act, and would require careful deliberation by the government. I do not have in mind a carte-blanch extension of the PJCIS's oversight powers, where they could probe any and all sensitive operational matter across the AIC.

Details of *specific ongoing intelligence operations (particularly covert ones),* technical collection issues, humint collection methodologies, and other matters where sources and methods would be revealed would generally be off-limits unless referred to the PJCIS by government. Though broad discussions on issues about coordination, intelligence priority setting, training, capability gaps, and intelligence alliances may from time to time benefit from oversight from qualified Committee members working in a bipartisan manner. The PJCIS in these areas could play a useful proactive role in monitoring capability issues to ensure they are cost effective and represent best practice.

The key to this working effectively in a way that does not reveal sources, methods and sensitive information in an adverse manner would be to make sure PJCIS members are all appropriately security cleared and receive a weekly security briefing from ONA on current threats and risks. This will help them understand the broader work of the AIC so that they can better provide appropriate oversight. The PJCIS' role should be one of guardianship in that Committee members should provide effective oversight but their involvement should be to promote better practice not to undermine a vital part of Australia's national security interests. If consideration of this idea is recommended in the reviewer's final report then quite naturally any extension of the PJCIS's ability to probe some operational matters would also need to include that such investigations would need to be held behind closed doors. Some sensitive matters may even need to be discussed in an appropriately security certified SCIFF environment.

An alternative, to extending current oversight powers to the PJCIS would be to expand the IGIS's role in reviewing particular intelligence performance matters beyond whether the AIC is following appropriate legislative provisions and acting with propriety. To be effective this option would require additional recruitment of specialised staff to support the IGIS in evaluating intelligence performance matters some of which the Inspectorate has currently no expertise. This option has merits given the independence of IGIS, but may result in additional costs of hiring staff or external experts to ensure the Inspector-General has the capability to look at a fuller suite of intelligence capability issue than is currently the case. This option may be less attractive given the constraints of the current fiscal environment.

- **The development path of overseas intelligence partners and lessons for Australia**

Australia's partnership with the other Five Eyes countries remains critical for securing the strategic and operational objectives of the AIC. The division of labour in terms of collection and to some extent analysis across the Five Eyes ensures Canberra maintains a global perspective on the most important intelligence priorities. The level

of cooperation, coordination and even integration of intelligence assets across the Five Eyes will continue to be vital for the AIC particularly in complex, technological focused threats and risks such as: terrorism, cyber, WMD proliferation and joint operational military support.

Since the last independent review in 2011, there have been many developments in the capabilities, legislation and policies of Five Eyes partners, which are important for the AIC to understand as some of these changes have impacted on Canberra's approach to intelligence. Other developments have less of a direct impact yet are important to be aware of as they present opportunities for the AIC to learn from and adopt if positive and fit for purpose; or to avoid if they may have a negative impact on the operation of the intelligence community here.

In the US, as noted earlier, there has been an increased focus on organisational structure with outgoing DNI Jim Clapper and Director CIA both leading major efforts to better integrate mission activities within and across intelligence agencies. These reform measures are still works in progress and it would be useful for the AIC to study them in detail to see if there is anything in the fine detail that may be of use. Though it is likely that these reform measures may well cease or even be reversed by the incoming Trump Administration. On a much smaller scale, since the last independent review there have been significant review of legislation in New Zealand (e.g. GSCB Amendment Act 2013) and review of governance arrangements around GCSB (The Kitteridge Review), with additional reviews into national security arrangements and the NZSIS.

In Canada, there has been the enacting of the publically contentious legislation C-51, which will result in a major revamp of national security and intelligence laws– not seen since Ottawa passed its Anti-Terrorism Act of 2001. C-51 seeks to provide better information flows between Canada's national security agencies and others such as immigration. It also contains features of the Australian Foreign Fighters Act. Ottawa will shortly also establish a parliamentary committee to oversee intelligence, which it has not had in the past. So it would be useful for PM&C to watch developments of this committee, particularly if changes to the PJCIS were contemplated. In the UK the release of the long awaited Chilcot Inquiry may result in further reforms of the UK intelligence community. Again the issue of how government members interpret or use intelligence politically was at the heart of this inquiry and there will always be lessons for our government and community in such inquiries.

The main development however, which seemed to grab the most headlines was the Snowden leaks in 2013. The earlier Wikileaks episode in 2011 was troubling enough for Australia and its allies, but the Snowden leaks were in a historical league of their own given that they consisted not only of large volumes of classified information, but also hitherto largely unknown (by the public) information about collection methodologies. The damage to collection efforts by the AIC and the larger Five Eyes alliance is difficult to determine, but I have no doubt that the revelations have changed how some threat actors communicate. There is now more encryption of social media and telecommunication devices and the intelligence community does struggle to access some platforms.

Much of the public debate about the impact of the Snowden leaks at first remained simplistic, i.e. how do we balance privacy and secrecy. A colleague and I have written a paper about this (see Appendix B), which in essence argues that different kinds of threats, contexts and the methods related to intelligence collection throws up different policy and ethical dilemmas and these need to be studied in greater detail. Understanding the differing policy and ethical dilemmas will be important if the AIC wants to better risk manage intelligence collection efforts[8]. The Obama Administration provided some initial steps towards reforming the bulk data collection previously done by the NSA, but further research needs to take place about what other accountability measures could be adopted in Five Eyes countries to maintain public trust in the intelligence community–yet address privacy issues to the extent that this is possible.

While the Snowden leaks saw a major review of risk areas for leaks across the US intelligence community, leaks have continued with the recent high profile arrest of NSA contractor Harold T Martin. There is no doubt that further research should be commissioned to better understand the profile of leakers (and whistle-blowers) and to determine if there are early warning pathways for intervention. Some attention to restricting access on an individual basis may be prudent, but a return to siloing of information access would be worryingly be a U turn back pre 9/11 days.

Counterintelligence is also another area where the AIC must continue to learn from developments across the Five Eyes. Counterintelligence has become even more complex with the intersection of state and non-state sponsored cyber-hacking and economic espionage. The AIC should consider developing a community-wide counterintelligence strategy for addressing these issues.

In summary, there is always something to learn from partners even if sometimes the lesson is not to follow the path of some developments in other countries. The Smith Review of 2008 thankfully put to bed the need for the creation of a supra-agency such as the DHS or the establishment of the ODNI in Australia. Both would have been unnecessary given coordination levels across the AIC work relatively well. Though there are also positive lessons to learn particularly in the US, where many intelligence agencies have greater public engagement– allowing external expertise and ideas to be more routinely and actively encouraged.

---

[1] See Walsh, *Intelligence and Intelligence Analysis,* 132-51; Walsh, "Building Better Intelligence Through Effective Governance,"123-42.
[2] Ibid.
[3] Walsh, "Building Better Intelligence Through Effective Governance," 135.
[4] Cornall and Black, *Independent Review of the Intelligence Community Report*, 31.
[5] Walsh, "Building Better Intelligence Through Effective Governance,"123-42.

[6] Walsh, “Making Future Leaders in the US Intelligence Community: Challenges and Opportunities,” 1-19.

[7] Walsh, “Australian National Security Intelligence Collection Since 9/11: Policy and Legislative Challenges,”51-74.
[8] Walsh and Miller, “Rethinking ‘Five Eyes’ Security Intelligence Collection.”345-368.

References

Cornall, Robert, and Rufus Black, *2011 Independent Review of the Intelligence Community Report.* Canberra: Australian Government, 2011.

Walsh, Patrick F, and Seamus Miller. “Rethinking ‘Five Eyes’ Security Intelligence Collection.” *Intelligence and National Security* 31 (2016):345-368.

Walsh, Patrick F, “Australian National Security Intelligence Collection Since 9/11: Policy and Legislative Challenges.” In *National Security, Surveillance and Terror Canada and Australia in Comparative Perspective,* edited by Randy K. Lippert, Kevin Walby, Ian Warren and Darren Palmer. USA: Springer International Publishing.

Walsh, Patrick F, “Making Future Leaders in the US Intelligence Community: Challenges and Opportunities.” *Intelligence and National Security* (2016): 1-19.

Walsh, Patrick F, “Building Better Intelligence Through Effective Governance.” *International Journal of Intelligence and Counterintelligence* 28(2015):123-142.

Walsh, Patrick F, *Intelligence and Intelligence Analysis*. Abingdon: Routledge, 2011

Notes on contributor

Patrick F Walsh, PhD, a former intelligence analyst, has worked in Australia’s national security and law enforcement intelligence environments. He is an associate professor in intelligence and security studies at the Australian Graduate School of Policing and Security, Charles Sturt University, Australia. He is course coordinator for its post-graduate intelligence analysis program and has taught widely across Australia and internationally. He is also consultant to government agencies on intelligence reform and capability issues. His book, *Intelligence and Intelligence Analysis* (Abingdon, UK: Routledge, 2011), examines a range of intelligence reform issues post-9-11 across Australia, Canada, New Zealand, the United States and the United Kingdom. Patrick is also on the editorial board of the premier international journal for intelligence studies, *Intelligence and National Security.*

APPENDIX A

International Journal of Intelligence and CounterIntelligence
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ujic20

Building Better Intelligence Frameworks Through Effective Governance

Patrick F. Walsh

Published online: 20 Nov 2014.

To cite this article: Patrick F. Walsh (2015) Building Better Intelligence Frameworks Through Effective Governance, International Journal of Intelligence and CounterIntelligence, 28:1, 123-142, DOI: 10.1080/08850607.2014.924816

To link to this article: http://dx.doi.org/10.1080/08850607.2014.924816

International Journal of Intelligence and CounterIntelligence, 28: 123–142, 2015

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2014.924816

Routledge
Taylor & Francis Group

PATRICK F. WALSH

Building Better Intelligence Frameworks Through Effective Governance

Since 11 September 2001 (9/11), extensive intelligence reform has brought many changes to the ''Five Eyes/5 Eyes'' intelligence communities.[1] For example, one major theme in the reform agenda has been to ''fuse'' intelligence more effectively within intelligence agencies and across communities. Questions remain however, as to whether such reform efforts have been effective. Has the rush to fusion resulted in greater effectiveness or additional fragmentation of intelligence?

9/11 AND POST-9/11 INTELLIGENCE FRAMEWORKS

Seven years after 9/11 many researchers were still focused on the intelligence failures which resulted in 9/11.[2] But in 2008, I argued that the debate needed to move beyond "what went wrong" before, during, and after 9/11. I also thought some of the journalistic commentary about some intelligence agencies being broken beyond repair was too simplistic.[3] By 2008,

Dr. Patrick F. Walsh is a former intelligence analyst who has worked in Australia's national security and law enforcement agencies, the Office of National Assessments, the National Crime Agency, and the Australian Crime Commission. Since 2003 he has been a Senior Lecturer in Intelligence and Security Studies at the Australian Graduate School of Policing and Security of Charles Sturt University, Bathurst, New South Wales, Australia, and course coordinator for the post-graduate intelligence analysis program. Dr. Walsh, the author of Intelligence and Intelligence Analysis *(London: Routledge, 2011), is also a consultant to government agencies on intelligence reform and issues of capability. He earned his B.A. and M.A. degrees at the University of Queensland, and his Ph.D. at Charles Sturt University.*

sufficient reform agendas were well underway in ''Five Eyes'' countries, and scholars needed to shift their focus to the future–specifically what governments were in fact doing to address failures and whether these remedies were effective.

From 2008 to the present, several events have driven reform initiatives across the ''Five Eyes'' intelligence communities. Some reforms have had a major impact on the various agencies. Establishment in the United States of the Office of Director of National Intelligence in 2004 is a good example. Other more recent events (e.g., Wikileaks and Edward Snowden) have left unclear how accompanying reform measures will impact on the effectiveness of intelligence.[4]

Not all the drivers for intelligence reform have been or are political. The 2008 Global Financial Crisis (GFC) significantly influenced debates about intelligence effectiveness and reform across the ''Five Eyes'' communities. After 9/11, most ''Five Eyes'' countries increased funding to their intelligence agencies, particularly for counter-terrorism.[5] In 2008, however, the impact of the developing GFC on public sector financing began to usher in the opposite fiscal paradigm, with intelligence communities now becoming less immune from the spending cuts affecting other government agencies across the ''Five Eyes'' communities.[6] Austerity has continued to impact the intelligence activities of national security and policing agencies in the network. For example, David Cameron's government in Great Britain has sought to continue reductions in frontline policing by six percent (8,100 people), and non-front line staff (including intelligence personnel) by 33 percent (20,300 people) between March 2010 to 2015.[7]

The growing public fascination with the workings of the intelligence agencies has increasingly transformed the services into ''public commodities.'' This public interest continues to fuel debates among citizens, scholars, and policymakers about the nature of national intelligence operations and their effectiveness. The political and economic drivers for intelligence reform have made public significantly more details of various reform initiatives than would ever have been possible pre-9/11. The debates are now not only more public, but have shifted away from ''what went wrong in 9/11'' towards assessing whether the various reform initiatives underway across the ''Five Eyes'' intelligence communities are creating more effective intelligence agencies.[8]

The challenge incives determining which approaches are most appropriate for understanding and evaluating post 9/11 reform agendas across the ''Five Eyes'' network. My own research on this aspect has included interviewing senior intelligence managers to evaluate what they are doing to address effectiveness in their agencies.[9] Evaluating ''intelligence effectiveness'' can arguably be addressed only holistically rather than by a piecemeal approach. As shown in the next section,

I suggest that a better approach to evaluating intelligence effectiveness can be accomplished by seeing intelligence agencies and communities as consisting of both structural and functional components that work together as part of an overall intelligence framework. Any evaluation of reforms and their impact on the effectiveness of intelligence agencies and communities, therefore, needs to consider both structural and functional components.

EXAMINING FIVE INTELLIGENCE FRAMEWORKS

Determining whether intelligence is effective requires a theoretical approach that can explore both the structural and functional dimensions of intelligence operations in agencies or across entire communities. This study used five examples (i.e., five intelligence frameworks) to explore how structural and functional dimensions of intelligence capabilities interact to address overall effectiveness. Prior to reviewing each framework, clarification is required on how the term ''intelligence framework'' is used here. A cursory review of the five frameworks shows that each is referred to differently by its designers. For example, the UK's National Intelligence Model (NIM) and the Canadian Criminal Intelligence Model (CCIM) are referred to as "models." In contrast, the two U.S. fusion centers discussed, the Joint Regional Intelligence Center in Los Angeles (JRIC) and the Regional Operations Intelligence Center (ROIC) in New Jersey, have more functional names. Again in contrast, the Australia's evolving intelligence framework is referred to as a "project"—Project Sentinel.

This variety in nomenclature suggests considerable variation in how the architects of these five examples define their approaches to intelligence reform. It also indicates that the term ''model'' lacks clarity in describing the context of all five examples. Though numerous other ''models of intelligence'' and ''networks'' are discussed in the literature, they are arguably at best models for components of intelligence practice rather than a whole framework.[10]

Despite the merits of some theoretical approaches to intelligence architectures, the term ''framework'' is more appropriate here. This study required a classifier that is sufficiently generic to apply to all the different contexts in the five examples. Additionally, ''framework'' encapsulates the holistic approach to intelligence practice herein considered.

Methodology

As indicated, the five intelligence frameworks explored here are the UK's National Intelligence Model (NIM), the Canadian Criminal Intelligence Model (CCIM), two U.S. fusion centers (the Los Angeles Joint Regional Intelligence Center [JRIC] and the New Jersey Regional Operations

Intelligence Center [ROIC], the New Zealand Police Intelligence Framework, and the Australian Crime Commission (ACC) Project Sentinel.[11] All five represent a mixture of national security and policing intelligence contexts, and were selected for three reasons.

First, since 9/11 notions of what strictly fits into "the national security intelligence" and "policing intelligence" categories (particularly with issues such as counter-terrorism and organized crime) have become blurred. I sought to explore how these allied intelligence frameworks which overlapped both categories interacted in each country. Second, each of the five frameworks was deliberately selected from a different "Five Eyes" country. This allowed some cross-comparison among the five countries—each with a history of sharing aspects of its intelligence arrangements with the other four. Yet each "Five Eyes" country is still sufficiently distinct in how it has managed intelligence reform since 9/11 to show variations in their approaches to building intelligence frameworks. Third, each example at the time of data collection constituted a contemporary intelligence framework that had evolved (with the exception of the UK's NIM) in part or perhaps entirely since 9/11. The currency of the examples was useful in capturing contemporary intelligence reform rather than using historical ones.

Rather than starting with a pre-determined theoretical perspective for "testing" what constitutes an effective intelligence framework, I employed three methods (semi-structured interviews, document analysis, and case analysis) to explore what the contemporary intelligence contexts may themselves indicate are important components for an effective intelligence framework. A full explanation of methodology used in the study can be found in my monograph, *Intelligence and Intelligence Analysis*.[12]

In summary, 61 interviews of executives, managers, and senior analysts were conducted across Australia, Canada, New Zealand, the UK, and the U.S. in 2009 and 2010. The interviews helped identify similar themes relevant to assessing what components make intelligence effective in the five intelligence frameworks. Four key themes arose out of analyzing interview transcripts: (1) *tasking and coordination*; (2) *collection*; (3) *analysis and intelligence production*; and (4) *strengths and weaknesses*. Assigning data collected during interviews to one or more of those themes allowed some analytical generalizability across each framework.

OVERVIEW OF FIVE FRAMEWORKS

A detailed analysis of each framework and an assessment as to their relative effectiveness is provided in *Intelligence and Intelligence Analysis*.[13] This section provides a brief outline of each framework and summarizes some key findings from each. While each was conceptualized and implemented in a different national context (underpinned by diversity in political

culture, legislation, and organizational priorities), they share numerous similarities. For example, all the tasking and coordination processes that have been (or are being) developed in each intelligence framework, despite some variations, show the importance of improving these critical intelligence processes to better integrate their results in decisionmaking.

Similarly, across each framework a common effort has been made to articulate more corporatized or standardized approaches in a range of core intelligence activities, including but not limited to, analytical methodologies, intelligence products, and collection techniques. In all five examples, standardized doctrinal approaches to intelligence processes are clearly being linked to consistent training standards.[14]

Despite some clear broad similarities in the approaches taken in each "framework," a great deal of variation can be found in the structures and functions adopted in each framework. Even within individual countries, the research disclosed variations in how the frameworks are being interpreted by the agencies using them.

UK NIM

The United Kingdom's NIM, since its establishment in 2000, has provided the most standardized doctrinal approach to core intelligence processes in UK policing. But the NIM's detailed approach has resulted in variations in "attitudes" toward it and the way it has been implemented and used by different policing agencies.[15] At the earlier stages of the NIM's implementation across the UK's policing agencies, these included variations in the quality of the new tasking and coordination group meetings and cultural attitudes by some non-intelligence staff personnel about the "value" of intelligence. In 2010, the NIM was again reviewed by staff from the UK's Metropolitan Police and the UK's policing standards-setting agency—what, for a time, was known as the National Policing Improvement Agency (NPIA). Results of the review are not publicly available, though it was expected to examine a range of issues including reducing bureaucracy, organized crime, cross-border issues, neighborhood policing, and citizen focus. Since the election of the Cameron Conservative government in 2012 significant changes have been made to policing arrangements in the UK, in addition to the continued funding cutbacks. For example, the former organized crime fighting agency, the Serious Organised Crime Agency (SOCA), was replaced with a new body—the National Crime Agency (NCA) in 2013. Additionally, the NPIA, which played a significant role in producing and monitoring intelligence standards across UK policing, was replaced by the College of Policing. How the College will review or build on the NIM in the future is not clear.

Canadian Criminal Intelligence Model

During interviews in 2009, the CCIM had not been fully implemented, making difficult a precise assessment of the strengths and challenges of the framework.[16] A few early challenges about its implementation were, however, identified during interviews with key project personnel. The first involved the culture change required to achieve the CCIM's vision of intelligence-led policing as a community. A fully operational CCIM would rely on an even greater willingness to share information among Canada's 380 policing agencies. But interviews clearly disclosed that many members of the Canadian law enforcement agencies still needed to revise their long-held views towards information sharing from "need to know" to the "responsibility to share." A second challenge for the successful implementation of the CCIM came from the further adjustments required of the law enforcement community to better align intelligence with operations across many policing agencies. CCIM architects suggested that this would compel that all law enforcement personnel learn and understand their role in a broader intelligence-led policing philosophy.[17]

A third identified challenge was compliance. Unlike the UK, Canada cannot federally legislate national changes in policing intelligence standards given that policing is the responsibility of the country's provinces. The CCIM's implementation staff located at Royal Canadian Mounted Police (RCMP) Headquarters in Ottawa did caution me that this impediment would make both the implementation and the agency's compliance to the model difficult since it cannot force common processes and standards upon the agencies. Communication and marketing were therefore deemed essential by the framework's architects in persuading people of the model's benefits. Implementation of the CCIM would be, in contrast to the UK's NIM, on a larger scale, with 400 different agencies involved—another factor contributing to the complexity of reaching all Canadian policing agencies, and all the right people within these agencies.

The centralized approach taken in the UK to implement NIM standards is not applicable to the Canadian law enforcement context. Hence, the CCIM established an advisory board with representation from various agencies, jurisdictions, functions, and levels to ensure that the principles of partnership and good governance would be practiced when implementing standards, guidelines, or strategies. But the CCIM ultimately failed to go to the scheduled implementation stage in 2011 after some key staff left the project.

New Zealand Police Intelligence Framework

Like many other policing agencies around the world, intelligence in the New Zealand Police (NZP) was historically used for case support, and its

development was focused mainly on local initiatives, at the District and Area levels. Overall, intelligence processes were ad-hoc and fragmented. This environment is described well by the National Manager, Intelligence for NZP, Mark Evans, who commented that:

> Management had little (or isolated) knowledge of what intelligence could do for crime and crash reduction. While examples of excellent intelligence *products* did exist, there were no minimum standards and many lacked focus and credibility with police decision-makers. There was a lack of what intelligence meant or was intended for.[18]

Many of the problems associated with the NZP's traditional approach to intelligence had also been raised in an earlier study completed by Jerry Ratcliffe in 2002.[19] But, in October 2006, the Policing Development Group (PDG) was directed to develop a business case for a national intelligence development project. The case was approved by the NZP executive, and in September 2007, Mark Evans of the Police Service of Northern Ireland was appointed to lead the project. A National Intelligence Office (NIO) was quickly established and set out ''15 project deliverables,'' which formed the basis of an initial twelve-month action plan. In October 2008, following extensive review and consultation, the Police Executive endorsed an NZ Police Intelligence Framework and approved the creation of a Police National Intelligence Centre (NIC) at Police National Head Quarters (PNHQ) to lead its strategic development.[20]

The NZ Police Intelligence Framework resulted in a number of important initiatives which are described fully in my book.[21] In brief though, tasking and coordination arrangements reforms were designed to ensure that the link between intelligence and operational outcomes would be clearly understood at all levels across the organization. Another was to put in place robust intelligence collection capabilities. Mark Evans reports that the focus for improving intelligence collection processes is ''based on the principle of collect information once and use it many times.'' Examples of specific collection initiatives can be found in my book.[22]

In addition to significant changes to tasking and coordination and collection approaches, the new Framework has resulted in some major changes to the way the NZP assesses and produces intelligence. In 2009, it invested heavily in the recruitment of 14 District Managers: Intelligence (DMIs) in addition to the twelve Districts, DMIs were appointed for Auckland Metro and AMCOS) at the Inspector level (or police employee equivalent). This has provided, for the first time, a clearly identifiable ''professional head of intelligence'' across every District. The DMIs have been selected mostly for their change management and people skills, rather than pure technical intelligence skills. Other intelligence reform initiatives followed in late 2009, including investing more in improving intelligence

related technology (data mining capabilities) and the development of the New Zealand Police Professional Development in Intelligence Programme (PDIP).[23]

ACC Project Sentinel

The Australian Crime Commission (ACC) is Australia's major organized crime fighting body. Since its establishment in 2003, the ACC has implemented a series of intelligence frameworks, including those that organizationally resulted in a split between intelligence and investigative functions and later iterations that focused on a thematic approach (i.e., based on classifying crime issues into groups and targets, commodities, or methodologies). By 2007, the ACC's Executive had become dissatisfied with both its thematic and bifurcated views of organized crime, which had the agency organized into two broad functions: intelligence and operations.

A key concern in 2007 was that both configurations resulted in a siloing of intelligence and investigations. Project Sentinel was designed to remove these. Sentinel, inspired originally by the UK's SOCA's Integrated Lifetime Management Programme (ILM), was modified significantly as the ACC does not have the same legislation as that underpinning the SOCA. The ethos of Sentinel was to make investigations a part of the intelligence cycle and to make intelligence part of the investigative cycle.[24]

Put simply, Sentinel was a framework developed to provide better support for the agency's new focus on complex (organized crime) investigations. These investigations used big data sets, including those from other agencies, particularly on abnormal patterns in money or trade movements. This data was combined with other specialized operational intelligence capabilities to identify targets and groups involved in any illicit transactions that were thus revealed. A senior ACC official described the new approach to me as looking for the ''criminal footprints'' in the data in order to identify more proactively serious and organized crime.[25] Project Sentinel consists of three phases: collection and analytics (phase 1); target development (phase 2); and intervention and prevention (phase 3). These phases were progressively established, starting with collection and analytics in October 2009.

The ACC's Project Sentinel represents a novel shift in how the service now conducts its intelligence business, but also potentially the Australian government's approach to organized crime. In 2009, the Australian government, through its Organised Crime Strategic Framework, gave the ACC a central intelligence role in the fight against organized crime.[26]

Sentinel's three phases give the ACC the flexibility to run its intelligence business in a way that potentially best contributes to the four areas noted earlier. The new framework will also seek help the agency utilize more

effectively its niche capabilities such as coercive powers and intelligence operations.

But the ACC's tactical, operational, and strategic intelligence tasking and coordination capabilities are also the result of a series of other priority setting mechanisms, both internal and external. Externally, the agency's work is now increasingly driven by a range of whole of government initiatives, including the government's Organized Crime Strategic Framework and a national criminal intelligence priority setting process, which seeks to articulate priority areas for all territory, state, and federal agencies to guide their strategic and operational planning for combating organized crime. These external processes are largely driven by some key risk and threat assessment mechanisms, developed within the ACC on behalf of the broader Australian policing and law enforcement intelligence community.

Los Angeles and New Jersey Regional Centers

The idea of multiple agencies represented in one physical location working on intelligence collection and analytical issues of mutual concern is not a new concept invented after 9/11. For example, the British response to World War II, as coordinated by the newly established (in 1939) Joint Intelligence Committee (JIC), brought representatives from both military and civilian intelligence agencies together in order to obtain a complete military, political, and economic assessment of the Nazi enemy.[27] Since World War II, each "Five Eyes" country has used "fused intelligence arrangements" on a range of issues (among them, counterterrorism, drug trafficking, and such major security events as the Olympic Games), though arguably post-9/11 the scale and extent of fused intelligence arrangements has proliferated.

Many "fusion versions" for counterterrorism (CT) intelligence have been developed in recent years. In addition to the U.S. National Counter Terrorism Center (NCTC), similar joined-up arrangements have been established such as the UK's Joint Terrorism Analysis Center (JTAC) and Canada's Integrated Threat Assessment Center (ITAC), as well as similar versions in Australia and New Zealand (the National Threat Assessment Centre (NTAC) and the Combined Threat Assessment Group (CTAG) respectively). Yet, the lexicon "fusion centers" is still largely equated as a U.S. approach in practice, and the two outlined here show some of the different configurations and variations that exist over the 72 fusion centers set up across the U.S.

America's fusion centers actually emerged pre-9/11. One of the earliest versions, the Los Angeles Terrorism Early Warning Group (TEW), begun as early as 1996, was a multi-agency, multi-disciplinary "fusion center" for all 88 cities in Los Angeles County.[28] The TEW once served as a model

for the development of other fusion centers elsewhere in the U.S., but its CT functions have now been incorporated into the Los Angeles Joint Regional Intelligence Center (JRIC). Since 2001, the U.S. Department of Justice and the Department of Homeland Security (DHS) have been building on the emerging common intelligence standards by creating further guidelines for state and local authorities on how to establish a fusion center.[29]

Both the JRIC and New Jersey Regional Operations Intelligence Center (ROIC), located in large U.S. metropolitan areas, have provided a good opportunity to allow a diverse number of federal, state, county, and city-based agencies to work together in one location. Discussions with relevant intelligence managers at both centers suggested that federal agencies such as the Federal Bureau of Investigation (FBI) were now working better with state and local units in sharing intelligence, a key objective of fusion centers. The two centers earlier seemed to have a different focus in their intelligence operations, with the JRIC more focused on counterterrorism and the ROIC utilizing a more all-hazards approach. Key staff indicated that the ROIC's operational activity generated more intelligence of its own, whereas the JRIC appeared to rely on assessing intelligence collected by other federal, state, and local agencies.

ANALYSIS OF FIVE FRAMEWORKS

The collected data showed the diversity of intelligence operations across each of the five frameworks. Yet, the analysis also highlighted common themes among them. Their significance to building better intelligence frameworks will now be explored.

One common theme was the need to consider strategies for communicating the benefits of new intelligence frameworks to non-intelligence officers who were required to engage with them. The UK NIM example made clear that well-crafted intelligence doctrine can provide a common set of policies and procedures on intelligence for use by diverse policing agencies across the UK. But intelligence frameworks designed by central implementation teams, comprised almost exclusively of intelligence officers, must ensure that non-intelligence staff (particularly operational officers and managers) using intelligence are sufficiently engaged throughout all stages of implementation once these frameworks are operationalized at the agency and/or local levels.

A second common theme shows that, although intelligence frameworks are useful in helping agencies improve the policies and processes supporting intelligence practice, they need to be sufficiently flexible, particularly when designed for their participation in the framework of multi-agencies such as the UK NIM, the CCIM, and the U.S. fusion centers. For example, the interviews showed that some operational police from UK policing

agencies, having found the NIM over-engineered, were developing their own ways of ''doing intelligence.''[30]

A third theme common to all five frameworks dealt with personnel training requirements and how their implementation would assist in improving intelligence results. Both the Los Angeles and New Jersey fusion centers seemed not to offer any in-house training. Yet, centers where local and federal sources of intelligence analysis are ''fused'' provide good opportunities to offer a full suite of products, including strategic assessments on issues of common relevance and priority to federal and local agencies. The importance of training for fusion staff has subsequently been advocated by others.[31] Additionally, unclear at this project's data collection stage (2009–2010), was the extent to which analysts working in the new Project Sentinel framework were receiving training in the specialized data mining and analytics which had become the focus of intelligence work in the ACC framework. Finally, although in some frameworks (e.g., the NZ Police Intelligence Framework and the CCIM), specific mention was made of providing professional development pathways, in most cases these were still in developmental stage.

A fourth theme related to information communications technology (ICT). Most intelligence agencies, wherever they operate in the national security and policing intelligence contexts, have problems with legacy ICT, which makes the storage, retrieval, and sharing of intelligence difficult. This problem occurs within as well as across agencies. This in itself was not a great revelation. But the extent to which ICT still presents barriers to the efficient production and dissemination of intelligence in agencies in the five frameworks underpins the need to seek coordinated solutions to these impediments when designing an effective intelligence framework.

The fifth, and most important, common finding involves a group of issues related to the leadership or management of intelligence frameworks. Each framework showed the importance of having sustainable leadership across an agency or community to drive its implementation. This leadership cannot merely arise from those in intelligence executive roles who have responsibility for the framework's implementation. It requires leadership from other executives and non-intelligence management as well. Examining all five examples made clear that, while one or two ''senior intelligence champions'' may have sought to implement the new frameworks, no uniform whole-of-agency/community approaches were available for their implementation. Heads of agencies may be initially engaged in, or see the need for, development of a more coherent intelligence framework, but at that level sustaining this attention among other competing priorities and diminishing funding is difficult.

Senior leaders working on the design or implementation of the other frameworks expressed similar views about how to ensure that intelligence

reform initiatives will gain traction over the long term. On the point of effective leadership, a number of other common issues became evident. These included challenges to intelligence collection priority setting, and the tasking and coordination of intelligence at the strategic, operational, and tactical levels. These issues become even more difficult when the framework involved the participation of more than one agency such as fusion centers.

For example, in the case of the two U.S. fusion centers studied here, I was not shown formalized guidelines on intelligence priority setting, monitoring, and coordination or agreements on resource sharing. They may have existed, but the interviews and secondary data sources revealed a number of challenges, suggesting that further work was required on constructing common approaches or guidelines on the operations of agencies in both fusion agencies. In particular, discussion with key fusion staff and secondary data sources indicated that issues such as different legislation, agency dissemination memoranda of understanding (MOUs), variations in security clearances, and differences among the organizational cultures of agencies (e.g., the role of the FBI vs. DHS), were testing just how "fused" or "joined up" these centers really were.

In summary, the analysis of these various themes led to a synthesis of the most important variables in providing an effective intelligence framework. The five frameworks demonstrated conclusively that, while the intelligence cycle shows conceptually how intelligence is produced in an agency or community, good intelligence does not develop in a vacuum. It relies on a range of supporting activities which must also be operating effectively. Needed for an effective intelligence framework therefore are both a well-working intelligence production cycle (combining the core enabling activities (see the inner circle in Figure 1), and five key enabling activities (the outer part of Figure 1), if an intelligence framework is to remain relevant and sustainable.

The core intelligence processes and key enabling activities must work in concert to produce an effective intelligence framework. But the results produced strong evidence that leadership and the coordination of intelligence frameworks were critical in ensuring their effectiveness. My research also indicated that several connected leadership issues required being investigated together. Conceptually, these leadership issues can be referred to as "governance" (see Figure 1).

INTELLIGENCE GOVERNANCE

Gerry Stoker has defined "governance as ultimately being concerned with creating the conditions for ordered rule and collective action."[32] Intelligence governance consists of attributes and rules pertaining to strong

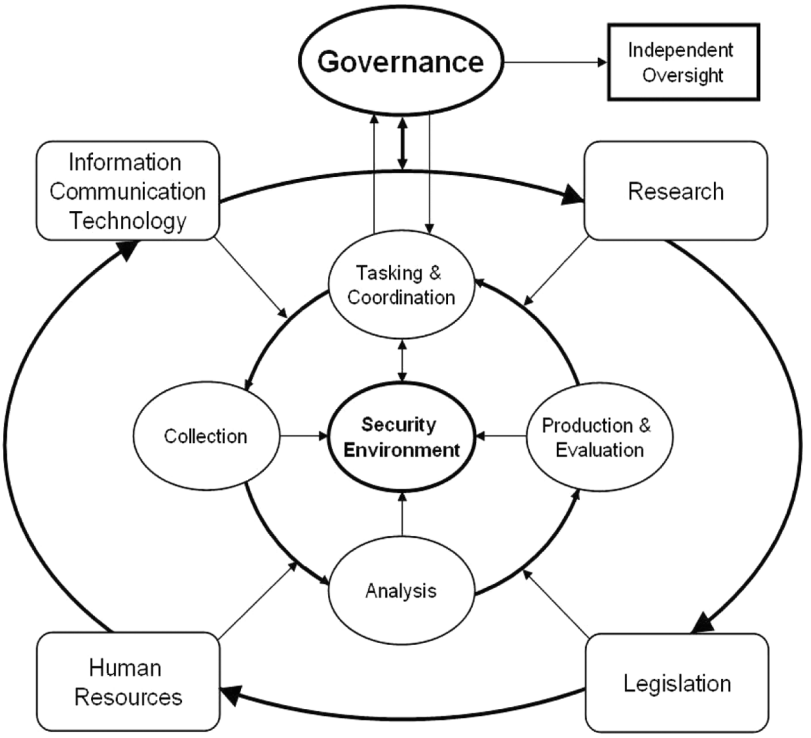


Figure 1. Components of an effective intelligence framework (*Source*: Walsh, 2011, p. 148).

sustainable leadership, doctrine design, evaluation, and effective coordination, cooperation and integration of intelligence processes. Intelligence governance also has external and internal dimensions. The external dimension relates to governance issues that impact on the framework from the government, decisionmakers, or other agencies outside the framework. Internal governance issues are those generated by an agency or a community's internal management processes, for example, the development and implementation of an effective strategic intelligence capability that informs agency planning. A governance issue can cut across both external and internal dimensions, particularly in the setting of intelligence collection priorities. Figure 1 features one arrow pointing away from governance toward the tasking and coordination phase, and another in the other direction toward the governance circle. This display shows that while internal governance arrangements can and do set an agency's intelligence priorities, the government and other external stakeholders also play important roles in articulating priorities.

In summary, without good governance, the core intelligence components and the other key enabling activities of the framework cannot function

effectively and intelligence failure will soon result. The rationale is that the key enabling activities in any framework should not operate in isolation, with each instead connected to the other as part of a dynamic set of constantly changing processes. For example, governance influences ICT solutions, and they in turn impact on human resources capabilities, with the same in reverse. Thus, key enabling activities both interact with and are influenced by, each other, though governance has a *primus inter pares* role since it provides the strategic leadership to develop all aspects of the framework in a coordinated and sustainable manner.

Based on my interviews with framework architects, a number of issues at the core intelligence and key enabling activity levels clearly require attention. Their sound governance will be essential to build an effective and sustainable framework. Significant issues remain, for example, around how U.S. fusion centers might build on early successes in information sharing by producing better value-added intelligence in comparison with what fusion agencies could do by operating on their own. In general, the interviews indicated the growing evidence of a better sharing of information between, for example, the FBI and some fusion centers, particularly through local JTTFs. Yet, the DHS, which has placed a great emphasis on the fusion centers being vehicles for channeling intelligence from the intelligence community to local police, has not been as effective in using the centers to facilitate the funneling of local intelligence to Washington, D.C. At the time of the original data collection, my observation was that better governance and support of fusion centers was required from the DHS's own Office of Intelligence and Analysis, which in 2009 was still building its own capabilities.

In both cases (JRIC and ROIC), and in other fusion centers not discussed here, a number of challenges still need to be overcome for these units to be fully effective intelligence frameworks. Some of these remaining challenges have been pointed out by others.[33] Additionally, in late 2012, the U.S. Senate's Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations released an uncomplimentary assessment of U.S. fusion centers that provided further evidence about the challenges they face—particularly on a range of governance issues. For example, the Senate report found poor leadership efforts on improving information sharing, funding oversight (at the fusion centers and in the DHS headquarters), and questions about the "value added" that fusion centers intelligence was providing from an analytical perspective.[34]

"Governance tensions" between participating agencies in U.S. fusion centers will likely continue given the differing federal, state, and local agencies' views on such issues as intelligence collection and analytical priorities, resource sharing, and training standards. For example, since both the DHS and the FBI have "domestic intelligence" roles operational

tensions between them may, in some fusion centers, continue to impact on whether staff members can effectively agree on the center's intelligence collection and operational priorities.

Current funding restraints on the U.S. Intelligence Community and in state and local law enforcement may require the DHS to take a greater leadership role in developing both the intelligence capabilities and mandates of fusion centers around the country. Effective internal (among fusion agencies) and external (between fusion centers and their sponsors and/or funding agencies) governance arrangements of U.S. fusion centers will help ensure that they become a stronger bridge between federal and state sources of intelligence.

Similarly, in the other ''Five Eyes'' frameworks challenges to good intelligence governance remain. For example, the ACC continues to face a number of internal and external governance issues, including some related to intelligence collection priority setting and the timely sharing of intelligence nationally among all federal and state law enforcement agencies.[35] In recent years the ACC and other Australian and state law enforcement agencies have been working on these and other governance issues. In 2012, the ACC published a high-level strategic document, *The Australian Criminal Intelligence Management Strategy (2012–2013)*, that examined several intelligence governance issues common to all Australian law enforcement agencies.[36] In the NZP Intelligence Framework, a more recent study by Steve Darroch and Lorraine Mazerolle, exploring the uptake of intelligence-led policing (ILP) in New Zealand, did show some variability across the country in how it had been applied across some districts. ILP underpins the NZP Intelligence Framework, and this study concluded that ''leadership stood out as important to the innovation process.''[37] Darroch and Mazerolle then discussed a range of governance issues important in the successful implementation of ILP in the New Zealand Police:

> What is clear is that the effectiveness of changes in *police organisational arrangements* (emphasis added) determines the course of police innovation. As our research demonstrates, innovations such as ILP are brought to life through changes in leadership, goals, technology, boundaries, practice and management arrangements.[38]

ENHANCING INTELLIGENCE GOVERNANCE

A number of factors can help develop intelligence governance, both as a theoretical concept and in its practical application inside intelligence agencies and communities. The first relates simply to having a realistic perspective. Improving intelligence governance in individual agencies and

intelligence communities is a long term project. No ''quick fixes'' are available for building better governance and intelligence frameworks in the ''Five Eyes'' intelligence communities, which developed over decades partly by design but also organically. Building better frameworks means striving for good practice, but also starting with what is already in place–even though some of these measures were implemented by political leaders as a knee-jerk reaction to the events of 9/11 without deeper reflection as to what was needed. Although the word ''framework'' does not immediately evoke a sense of flexibility, a flexible and pragmatic approach is required to theorizing and implementing better intelligence structures and functions that improve overall governance. The two components of the framework in Figure 1 (core intelligence processes and key enabling activities) provide a flexible and less prescriptive approach.

The second point relevant to enhancing intelligence governance is further refinement of the concept and its underpinning by other components of the intelligence framework. The key enabling activities (governance, ICT, human resources, legislation, and research) are critical to building an effective foundation on which intelligence production can prosper. Yet further testing of the validity of these key enabling activities is required. For example, post-9/11 are these key enabling activities still important enablers for timely and ''decisionmaker focused'' intelligence production? Recent evidence suggests that they may in fact be relevant to how U.S. fusion centers, Project Sentinel, and the NZ Police Intelligence Framework evolve.

But the question remains as to the extent that these key enabling activities are *the most critical* factors in the ongoing implementation of the frameworks studied. Or are there others which further study will show to be as equally important or more important? Also relevant is the issue of reliability. If this framework was applied to other intelligence contexts would it help to ''diagnose'' their relative effectiveness? While this study explored some of the key issues which seemed to be important to developing effective intelligence frameworks—regardless of the context (whether national security or policing intelligence)—the extent to which results are generalizable to other intelligence contexts (e.g., military or private sectors) can be known only by studying further contemporary examples.

By definition, research into any aspect of contemporary intelligence practice has its limitations in terms of access to people and data, but even limited access can help in theorizing about contemporary barriers to intelligence reform. Certainly, the granting of access to intelligence environments, and any conditions attached to that access, present real methodological dilemmas for researchers wishing to evaluate contemporary intelligence frameworks, particularly around the validity of data collected. Yet senior management in some intelligence agencies have begun asking to

bring in ''trusted outsiders'' to work on identifying, evaluating, and improving their intelligence frameworks.

In Australia, I am currently working as an advisor on developing better intelligence frameworks for two major public agencies. Opportunities exist in such contexts to apply the theoretical perspectives developed herein, and then to evaluate the evidence that they do assist the development of better intelligence processes and frameworks.

The intelligence framework in Figure 1 is only a start, but it provides a theoretical guideline that, with further testing, may result in more refined and grounded theory approaches to building better intelligence frameworks. This in turn, and more importantly, may lead to better intelligence capabilities and, also in turn, better decisionmaker support.

REFERENCES

[1] The ''Five Eyes'' intelligence communities is a descriptor used by national security intelligence agencies of Australia, Canada, New Zealand, the UK, and U.S. It describes a special relationship that the intelligence agencies of each country have shared since the end of the Second World War. This relationship has been built around formal and informal agreements allowing each country to share signals and human intelligence gathered with other ''Five Eyes'' member countries. The term ''Five Eyes'' is used here as a shorthand way to refer to the national policing agencies of these countries, which share intelligence as well—though in its strictest sense, the term refers to the national security intelligence communities of each listed country here and not their policing communities.

[2] See Arthur S. Hulnick, ''Intelligence Reform 2008: Where to From Here?'' *International Journal of Intelligence and CounterIntelligence*, Vol. 21, No. 4, Winter 2005–2006, pp. 621–635; Joshua Rovner and Austin Long, ''Intelligence Failure and Reform: Evaluating the 9/11 Commission Report,'' *Breakthroughs*, Vol. 14, No. 1, 2005, pp. 10–21; Amy Zegart, *Spying Blind* (Princeton, NJ: Princeton University Press, 2007).

[3] *Ibid.*; see also Tim Weiner, *Legacy of Ashes: The History of the CIA* (New York: Doubleday, 2007).

[4] Since 9/11, several events and issues have resulted in reforms across the ''Five Eyes'' communities, including Iraq, coercive interrogation, Abdulmutallab, WikiLeaks, and Edward Snowden. On role of intelligence assessments on the invasion of Iraq see, United States Senate, Select Committee on Intelligence, 108th Congress, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq* (Washington, DC: Government Printing Office, 2004). Phillip Flood, *Report of the Inquiry into Australian Intelligence Agencies*. (Canberra: Australian Government, 2004); John Morrison, ''British Intelligence Failure in Iraq,'' *Intelligence and National Security*, Vol. 26, No. 4, 2011, pp. 509–520.

On role of torture, see U.S. Senate Committee on the Judiciary, *Senate Committee on the Judiciary Concerning Detainee Interrogation Techniques. Do They Work, Are They Reliable and What Did the FBI Know About them*? (Washington, DC: Government Printing Office, 2008), at http://judiciary.senate.gov/hearings/hearing.cfm?.id=3399; Philippe Sands, *Torture Team: Rumsfeld's Memo and the Betrayal of American Values* (New York: Palgrave Macmillan, 2008); Dennis O'Connor, *A New Mechanism for the RCMP's National Security Activities, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (Ottawa: Public Works and Government Services Canada, 2006), at http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf

On the attempted bombing by Umar Farouk Abdulmutallab see, U.S. Senate Select Committee on Intelligence, 111th Congress, 2nd Session, *Attempted Terrorist Attack on Northwest Airlines Flight 253. United States Senate Together with Additional Views* (Washington, DC: Government Printing Office, 2010). On WikiLeaks see, Patrick F. Walsh, *Intelligence and Intelligence Analysis* (Abington, UK), pp. 210–218. On planned reforms to the National Security Agency post-Snowden, see Richard Clarke, Michael Morell, Geoff Stone, Cass Sunstein, and Peter Swire, Report and Recommendations of the *President's Review Group on Intelligence and Communications Technologies* (12 December, 2013). See also, *Presidential Policy Directive/PPD-28 Signals Intelligence Activities* (17 January 2014).

[5] U.S Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 107th Congress, 2nd Session, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* (Washington, DC: Government Printing Office, 2002), p. 257.

[6] By way of illustration of this point, the U.S. combined intelligence budget (military and civilian agencies) is expected to be around $71 billion—down 10 percent from 2012. See ''DNI Releases Budget Figure for FY 2013 Appropriations Requested for the National Intelligence Program, (February, 13 2013),'' at http://www.dni.gov/index.php/newsroom/press-releases/96-press-releases-2012/337-dni-releases-budget-figure-for-fy-2013-appropriations-requested-for-the-national-intelligence-program

[7] HMIC, *Policing in Austerity: One Year On* (London: Home Office, 2012).

[8] Patrick F. Walsh, *Intelligence and Intelligence Analysis*, pp. 159–165; David Lonsdale, ''Intelligence Reform: Adapting to the Changing Security Environment,'' *Comparative Strategy*, Vol. 31, No. 5, 2012, pp. 430–442.

[9] The research in this article is part of a larger research project which resulted in the monograph, Patrick F. Walsh, *Intelligence and Intelligence Analysis*.

[10] For example, the acronym ''SARA'' or, *Scan, Analyse, Respond, and Assess* introduced by Eck and Spelman has been referred to as a model or methodology. See John Eck and William Spelman, *Problem Solving: Problem Orientated Policing in Newport News* (Washington, DC: Police Executive Research Forum, 1987). More recently, other novel models have been

developed, such as the fractal intelligence model. See, Michael Hawley and Bradley Marden, ''FIM: A Business Information System for Intelligence,'' *International Journal of Intelligence and CounterIntelligence,* Vol. 19, No. 3, Fall 2006, pp. 443–456. On Ratcliffe's 3-I model, see, Jerry Ratcliffe, *Intelligence Led Policing* (Cullompton, UK: Willan, 2008), p. 110. On ''networks'' see, Peter Gill and Mark Phythian, *Intelligence in an Insecure World* (Cambridge, UK: Polity Press, 2006), pp. 39–61.

[11] Patrick F. Walsh, *Intelligence and Intelligence Analysis*, p. 92.

[12] *Ibid.*

[13] *Ibid*., pp. 89–131.

[14] *Ibid*.

[15] Mike Maguire and Tim John, *The National Intelligence Model: Early implementation Experience in Three Police Forces* (Home Office Online Report, 30, No. 4, London: Home Office, 2004); Patrick F. Walsh, *Intelligence and Intelligence Analysis,* pp. 95–104.

[16] *Ibid.*, pp. 104–110.

[17] There are many definitions of intelligence-led policing, but in simple terms it is the proactive application of intelligence collection and analysis to have the greatest impact on decisions about where to deploy resources, particularly in areas with the greatest crime recidivist offenders.

[18] *Ibid*., pp. 117–118.

[19] Jerry Ratcliffe, ''The Effectiveness of Police Intelligence Management: A New Zealand Case Study,'' *Police Practice and Research,* Vol. 6, No. 2, 2005, pp. 435–451.

[20] Patrick F. Walsh, *Intelligence and Intelligence Analysis*, pp. 117–123.

[21] *Ibid.,* pp. 135–136.

[22] *Ibid*., pp. 117–123.

[23] *Ibid*., pp. 123–130.

[24] *Ibid.*, p. 124.

[25] Attorney General's Department, *Organized Crime Strategic Framework* (Canberra: Commonwealth of Australia, 2009).

[26] The ACC Act, allows the agency to demand financial documents and witnesses to appear before an examiner to answer questions. Failure to surrender documents or appear in person to the ACC examiner can result in a fine and or imprisonment.

[27] Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), p. 26.

[28] John Sullivan and Alain Bauer, *Terrorism Early Warning: Ten Years of Achievement in Fighting Terrorism and Crime* (Los Angeles, CA: Los Angeles County Sheriff's Department, 2008), p. 23.

[29] U.S. Department of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington, DC: U.S. Department of Justice, in collaboration with the Department of Homeland Security, 2006);

DOJ, *Baseline Capabilities for State and Major Urban Area Fusion Centers* (Washington, DC: Department of Justice and Homeland Security, 2008).

[30] Patrick F. Walsh, *Intelligence and Intelligence Analysis*, p. 103.

[31] Justin Abold, Ray Guidetti, and Doug Keyer, ''Strengthening the Value of the National Network of Fusion Centers by Leveraging Specialization: Defining Centers of Analytical Excellence,'' *Homeland Security Affairs,* Vol. 8, No. 7, 2012, pp. 1–29.

[32] Gerry Stoker, ''Governance as Theory: Five Propositions,'' *International Social Science Journal*, Vol. 50, No. 155, 2002, p. 18.

[33] Justin Abold, Ray Guidetti, and Doug Keyer, ''Strengthening the Value of the National Network of Fusion Centers by Leveraging Specialization: Defining 'Centers of Analytical Excellence'''; Robert Taylor and Amanda Russell, ''The Failure of Police 'Fusion' Centers: The Concept of a National Intelligence Sharing Plan,'' *Police Practice and Research*, Vol. 13, No. 2, 2012, pp. 184–200.

[34] U.S. Senate Permanent Sub-Committee on Investigations, *Federal Support for the Involvement in State and Local Fusion Centers* (Majority and Minority Staff Report) (Washington, DC: Senate Committee on Homeland Security and Governmental Affairs, 2012).

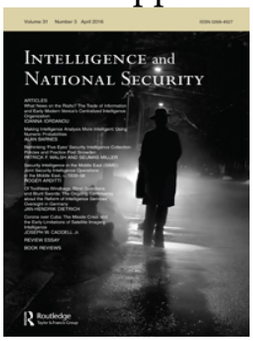
[35] Patrick F. Walsh, *Intelligence and Intelligence Analysis*

[36] Australian Crime Commission (ACC), *Australian Criminal Intelligence Management Strategy 2012–2015* (Canberra: Commonwealth of Australia, 2012).

[37] Steve Darroch and Lorraine Mazerolle, ''Intelligence-Led Policing: A Comparative Analysis of Organizational Factors Influencing Innovation Uptake,'' *Police Quarterly*, Vol. 16, No. 3, 2012, p. 25.

[38] *Ibid.*, p. 26.

Appendix B



Intelligence and National Security

ISSN: 0268-4527 (Print) 1743-9019 (Online) Journal homepage: http://www.tandfonline.com/loi/fint20

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

Patrick F. Walsh & Seumas Miller

To cite this article: Patrick F. Walsh & Seumas Miller (2016) Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden, Intelligence and National Security, 31:3, 345-368, DOI: 10.1080/02684527.2014.998436

To link to this article: http://dx.doi.org/10.1080/02684527.2014.998436

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

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).

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).