COMPARATIVE REPORT

Big Data Technology and National Security

Comparative International Perspectives on Strategy, Policy and Law

Law and Policy Program
Data to Decisions Cooperative Research Centre

June 2018

Research Team

Professor Louis de Koker, Program Leader
Professor Janet Chan, Project Leader
Professor Danuta Mendelson, Key Researcher
Associate Professor Lyria Bennett Moses, Key Researcher
Dr Alana Maurushat, Key Researcher
Mr David Vaile, Key Researcher
Mr Mike Gaffney, Researcher
Mr Gregory Sadler, Researcher
Mr Patrick Grierson, Researcher
Mr Daniel Cater, Project Research Assistant

Other research assistants:
Ms Alana James
Ms Sonam Gordhan
Mr Jax Arnold

Interns (in alphabetical order)
Ms Kendy Ding
Mr Ciaran Finnane
Ms Monica Ma
Mr Kevin Tsu
Mr Atul Vidhata
Mr Vincent Wan
Ms Jacqueline Yip

Comparative Report

Authors
Chapter 1: Introduction – **Janet Chan**
Chapter 2: Big Data – risks and opportunities – **Alana Maurushat**
Chapter 3: Methodology
3.1 Empirical research: **Janet Chan and Lyria Bennett Moses**
3.2 Doctrinal research: Louis **de Koker, David Vaile, Lyria Bennett Moses, Alana Maurushat and Danuta Mendelson**
3.3 Comparative analysis: **Louis de Koker, David Vaile, Lyria Bennett Moses, Alana Maurushat and Danuta Mendelson**
Chapter 4: Country contexts – **Louis de Koker and Danuta Mendelson**
Chapter 5: Empirical findings – **Janet Chan and Lyria Bennett Moses**
Chapter 6: Legal analysis – **Louis de Koker, Alana Maurushat and Lyria Bennett Moses, except as noted**
6.1 Is access for data mining enabled?
6.2 Are legal controls comprehensive and proportional? **Danuta Mendelson, Louis de Koker, Alana Maurushat and Lyria Bennett Moses**
6.3 Are legal rules clear, principle-based, consistent and instructive?
6.4 Is integrity of data and analysis supported?
6.5 Are data and systems protected?
6.6 Is accountability maintained?
6.7 Are principles and rules regularly reviewed?
6.8 Is there a sufficient measure of transparency?
Chapter 7: Conclusion and Draft recommendations – **Louis de Koker and Lyria Bennett Moses**

Research assistance
Mr Daniel Cater

Technical editing
Mr David Vaile

Other Reports from this Project

Methodology Report
Australia Report
UK Report
Canada Report

Select Bibliography
Technical References [for Australia Report]

Table of contents

List of Tables

Comparative Report

1. INTRODUCTION

This report is part of a set of reports stemming from an independent study funded by the Data to Decisions Cooperative Research Centre and undertaken by a team of law and policy researchers from Deakin Law School and UNSW Law under the lead of Professor Janet Chan (UNSW). Officials of the Attorney-General's Department joined the research team to provide logistical support.

The main aim of the study (*Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law in Australia, the United Kingdom and Canada*) was to examine the policies, regulatory approaches, processes and strategies used by Australia, the UK and Canada to balance the management and exploitation of Big Data for national security and law enforcement (**NSLE**) purposes, while safeguarding confidentiality and security of sensitive personal information, as well as the accuracy of data sets.

The study focused on two key sets of research questions:

1. What are the current technological applications and future possibilities of Big Data for law enforcement and national security as perceived by designers, users and stakeholders? What are their perceptions of the social, legal or policy implications of Big Data in this context?
2. What are the strategies, policies, laws, regulatory frameworks, practices and technologies relevant to Big Data adopted by Australia, the UK and Canada, and are they perceived as effective in meeting social, legal or policy objectives, including, but not limited to, law enforcement and national security objectives? What responses are needed to deal with potential challenges?

The main objectives of the project were:

1. To scope and assess relevant international perspectives, policies, laws and practices that can inform Australian policymakers and support the development of law and best practices; and
2. To develop a comprehensive and contextual understanding of the current as well as the future direction of policy, law and practices in the relevant jurisdictions that will inform further work of the D2D CRC Research Program.

This report provides a comparative overview of the key findings and should be read in conjunction with the three country reports as well as the Methodology Report.

Upon conclusion of the study in June 2016 the reports were submitted to the Attorney-General's Department for review and comment. Comments were received from a number of agencies during the course of 2017, leading to their finalisation in June 2018. The limited review and revision process was aimed at ensuring that the reports present the legal framework correctly as at 30 June 2016, providing a reader with an overview of the legal position at the time that researchers were collecting the empirical data reflected in these reports.

The study was undertaken for the Attorney-General's Department but was conducted independently. The involvement of government officials in the logistics of the study, the

empirical interviews or the review process should not be interpreted as an expression of any view on the study or its findings, either by government agencies or any of their officials.

2. BIG DATA – RISKS AND OPPORTUNITIES

The capture and analysis of data is experiencing exponential growth. Advancements in data capture and storage technologies mean that more data is available to use and analyse. Datasets that may be available to government include but are not limited to open government datasets,[1] public datasets such as social media data, metadata, and datasets in new fields such as the 'Internet of Things,' or sensors in Smart Cities.[2] 'Big Data' is a term that is used to describe large and often disparate datasets that are able to be analysed using faster processing and advanced analytics.

The idea of Big Data has emerged from this growth and the proliferation of digitised information. Innovative technologies and processes are increasing the ability to accurately and speedily assess, interpret and understand Big Data in a variety of fields, professions and contexts. In a modern setting, Big Data and its analysis can play crucial roles in both commercial and government contexts; for example in the delivery of government services such as healthcare and transportation.

The use of Big Data in the intelligence and law enforcement fields was highlighted when in 2013 Edward Snowden leaked information about mass surveillance by the National Security Agency of not only American citizens' data but foreign citizens' data as well.[3] The interception practices of the scale revealed by Snowden necessarily involve the use of Big Data and Big Data systems. Against this backdrop, nations across the globe including Australia have begun not only to invest in big data and big data analytics, but to address legal and policy concerns. While there is a great deal of research and literature around general principles of surveillance, privacy, security and appropriate powers and investigatory frameworks for NSLE purposes, there has not been a great deal of specific research and publications focusing on the benefits and risks of big data in the NSLE space.

While there is no mutually-agreed rigorous definition of Big Data within the industry, the term generally denotes the following characteristics: volume, source variety, processing capacity, and smart analytics. 'Big Data' is a term that involves large and often disparate datasets that are able to be analysed using faster processing and smarter (autonomous and semi-autonomous) analytics. The idea of Big Data has emerged from this growth and the proliferation of digitised information. Innovative technologies and processes are increasing the ability to accurately and speedily assess, interpret and understand Big Data in a variety of fields, professions and contexts. In a modern setting, Big Data and its analysis can play crucial roles in both commercial and government contexts; for example in the delivery of government services such as healthcare and transportation.

While the project is concerned primarily with the use of Big Data for law enforcement, defence and intelligence in the context of national security, the use of Big Data analytics for other more general purposes can provide useful insights about its implications. This report has, therefore, referred to general principles and implications of Big Data, as well as to specific legal and policy issues arising when Big Data is used by law enforcement and

---

[1] V Mayer-Schönberger and K Cukier, *Big Data: A Revolution that will Transform How We Live, Work, and Think* (John Murray Publishers, 2013). R Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (Safe, London, 2014); Open Data Initiative, *Global Open Data Initiative* (June, 2013) <http://globalopendatainitiative.org/>

[2] R Kitchin, 'The Real-Time City? Big Data and Smart Urbanism' (2013) 79 *Geo-Journal* 1; M Batty, 'Big Data, Smart Cities and City Planning,' (2013) 3(3) *Dialogues in Human Geography*.

[3] G. Greenwald, 'NSA collecting phone records of millions of Verizon customers daily'. *The Guardian* (June 6, 2013). 06.06.2013) < http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

intelligence in the context of 'national security'.

There are many benefits and risks in using Big Data for law enforcement and intelligence, as well as for national security purposes. While some of these benefits and risks are specific to the national security context, most are equally applicable to commercial and other governmental purposes. As Big Data analytics is evolving both in its use and through technical advancements, the perceived benefits and risks of Big Data may not eventuate as predicted. Further, some impacts may be perceived as both benefits and risks by different stakeholders. These overlapping impacts are: privacy, transparency, de-identification and re-identification, security, and data control.

There are many potential opportunities and benefits of Big Data. These include but are not limited to benefits derived from:

- **machine learning:** Machine learning algorithms 'learn' from data to identify correlations and patterns, often in order to make predictions.[4] One advantage of using machine learning is that, in theory, no human eyes would need to see personal information or sensitive data – the algorithm studies the data, determines its utility and relationship with other data and then spits out areas of concern.
- **smarter analytics:** 'Smart Analytics' is an umbrella term suggesting a qualitative difference between earlier data mining techniques.[5] Smarter analytics allows for improved predictive analysis, helps detect previously unknown patterns for analysis capabilities, produces results in new forms of visualisation, and produces scalable, integrated high performing analysis.[6]
- **effective search ranking and prioritisation:** Law enforcement and intelligent analysts receive large quantities of data, sometimes as changing data streams. One of the greatest potential problems in large volumes of data is the perception of 'drowning in data'. Big Data tools can aid the officer or analyst in producing better search rankings for data queries. The analyst then has a tool to assist them with where to prioritise their time and resources.[7]
- **privacy benefits**: Some technologists believe that Big Data has the ability to increase privacy protection through integrated tools and concepts such as privacy by design or privacy engineering.[8]

---

[4] Christopher Bishop, *Pattern Recognition and Machine Learning* (Springer 2006).

[5] J Manyika et al, *Big Data: The next frontier for innovation, competition and productivity*, McKinsey Global Institute (online), 2011 <http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation>.

[6] S Morgan and C Winship *Counterfactuals and Causal Inference: Analytical Methods for Social Research* (New York: Cambridge University Press, 2007).

[7] Vidit Jain and Manik Varma, 'Learning to re-rank: query-dependent image re-ranking using click data' (WWW '11, Proceedings of the 20th international conference on World wide web, 2011) 277-286 <http://dl.acm.org/citation.cfm?id=1963447>; H Chen, RHL Chiang, VC Storey, 'Business Intelligence and Analytics: From Big Data to Big Impact' *MIS quarterly* (2012)

[8] K Rannenberg, D Royer and A Deuker (eds), *The future of identity in the information society: challenges and opportunities (*Springer, Berlin, 2009); Michael Froomkin, 'Pets Must Be on a Leash: How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology' (2013) 74(6) *Ohio State Law* (October 1, 2013); Alana Maurushat, Lyria Bennett-Moses and David Vaile, 'Using "Big" Metadata for Criminal Intelligence: Understanding Limitations and Appropriate Safeguards' (ICAIL '15, Proceedings of the 15th International Conference on Artificial Intelligence and Law, June 2015) 196.

(cont.)

- **predictive policing:** Predictive policing is also being explored in some jurisdictions as a means of optimising police deployments to match predictions about *who* will commit crimes and *where*.[9] Previously undetected patterns may become critical aspects for further investigation which may lead to the identification of suspects and targets.[10]
- **prediction of imminent danger:** Big Data has potential ability in the the national security space as avoiding terrorist attacks and other terror related incidents.[11] Less known are the national security threats outside of terrorists plotting bombs, attacks and murders such as the use of Big Data in predict vulnerabilities in critical infrastructure, detect pandemics andrespond to natural disasters.[12]
- **identification of trends and patterns**
- **operational efficiency:** Evidence-based policy making is potentially transformed into something much greater with the possibility of lawmakers being able to supplement traditional studies with real-time analysis of issues and events. Data analytics should also enhance the ability of government to direct resources to areas most in demand. This strategic alignment of resources can assist both in short and long term resource management.[13]
- **security enhancement**: Big Data tools can be used to enhance security or can instead pose a security risk.[14] Again this is dependent on how the technologies evolve, and whose perception is being considered.[15]
- **monitoring authorised access and uses of data:** Big Data tools are said to be able to better monitor unauthorised access of data, unauthorised usage, and unauthorised distribution. This in return is said to aid in decreasing abuse of data – whether the abuse is accidental or deliberate.[16]

---

[9] Craig D Uchida, 'Predictive Policing' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer, 2013) 3871, 3871.

[10] P Alston, 'CIA and Targeted Killings beyond Borders' (2011) 2 *Harvard National Security Journal* 283 <http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2_Alston1.pdf>; BE Harcourt, *Against Prediction: Profiling, Policing and Punishing in an Actuarial Age* (University of Chicago Press, 2007).

[11] Babak Akhgar et al, *Application of Big Data for National Security A Practitioner's Guide to Emerging Technologies* (Elsevier, 2015).

[12] Fleur Johns, 'Data Mining as Global Governance' in *The Oxford Handbook on the Law and Regulation of Technology,* edited by Roger Brownsword, Eloise Scotford and Karen Yeung (Oxford University Press, forthcoming 2016).

[13] P Casanova, 'CAPER Regulatory Model: Platform to Fight Organised Crime, *AustLII Workshop on Privacy* (September 2014) <http://www.austlii.edu.au/austlii/seminars/2014/3.html>.

[14] Lei Xu, 'Information Security in Big Data: Privacy and Data Mining' (2014) 2 *IEEE Access* 1149 <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6919256&newsearch=true&queryText=Information%20Security%20in%20Big%20Data:%20Privacy%20and%20Data%20Mining>.

[15] Babak Akhgar et al, *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies* (Elsevier, 2015); Jane Bambauer, Krish Muralidhar, and Rathindra Sarathy, 'Fool's Gold: an Illustrated Critique of Differential Privacy' (2014) 16 *Vanderbilt Journal of Entertainment & Technology Law*; Laura Donohue, 'High Technology, Consumer Privacy, and US National Security' (2015) *Georgetown Law Faculty Publications*, 1457; Sean Richmond, 'National security debate misses big picture of 'balanced' response', *The Conversation* (online), 25 February 2015 <https://theconversation.com/national-security-debate-misses-big-picture-of-balanced-response-37923>.

[16] Council of Australian Governments (**COAG**), *Final Report of the COAG Review of Counter-Terrorism Legislation*, 1 March 2013 <http://www.ag.gov.au/Consultations/Pages/COAGReviewofCounter-TerrorismLegislation.aspx> or <http://www.ag.gov.au/Consultations/Documents/COAGCTReview/Final%20Report.PDF>; Robert

(cont.)

There are also many potential risks to using Big Data, including:

- **drowning in data:** Some users of datasets and data analytics are concerned that the volumes involved in Big Data will lead to significantly more data to analyse with minimal gain in benefits, hence the term 'drowning in data'.[17]
- **lack of trained professionals in data analytics**
- **use of local cultural patterns as basis for interpreting foreign behaviours:** When agencies look at inferences drawn from Big Data by foreign counterparts, they need to recognise that these patterns may not be accurate in a local cultural context.[18]
- **reliability and accuracy of data:** There has been some minor concern that a move to Big Data systems will undercut the reliability and accuracy of data within datasets but support of this theory are few.[19]
- **privacy (uncontrolled sharing and de-identification):** Concerns have been raised as to whether the current privacy framework in virtually all nations is adequate for Big Data.[20] Some have argued that once data has been collected, there is no control over who uses it or how it is used; there is no privacy.[21]
- **discrimination:** there is a growing concern that machine learning Big Data systems could systemically build in correlations that become discriminatory.[22]
- **escalation of cross-border surveillance:** With leaks to the media and online leak sites detailing Big Data capacities of governments and organisations, there is a risk that the adoption of Big Data will proliferate, promoting an escalation of cross-border surveillance.[23]
- **unregulated public partnerships using commercial data:** Private corporations are free to share information with government agencies provided that they comply with

---

Bloom and William Dunn, 'The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment' (2007) 15 *William and Mary Bill of Rights Journal* 147 <http://lawdigitalcommons.bc.edu/lsfp/163/>; Roger Clarke, '*Privacy Impact Assessments as a Control Mechanism for Australian National Security Initiatives,'* Xamax Consultancy (2015) <http://www.rogerclarke.com/DV/IANS.html>.

[17] Adrian Lawrence and L Lim, *Privacy and Security: Introduction – Privacy in Cyberspace,* Law of E-Commerce (2015 Lexis Nexis).

[18] Kate Westmore and Gail Kent*, International Law Enforcement Access to User Data: A Survival Guide and Call for Action* (8 January 2015) <http://ssrn.com/abstract=2547289> or <http://dx.doi.org/10.2139/ssrn.2547289>.

[19] J Laurila et al, 'The Mobile Data Challenge: Big Data for Mobile Computing Research', conference paper EPFL-CONF-192489, *Pervasive Computing* Workshop*,* Newcastle (2012) <http://infoscience.epfl.ch/record/192489>.

[20] Jarrod Bayliss-McCulloch, 'Risks and opportunities in Big Data — how well adapted are Australia's privacy laws?' (2015) 20(1) *Media and Arts Law Review*.

[21] Craig Sebastopol, *Privacy and Big Data: The Players, Regulators, and Stakeholders* (O'Reilly 2011); Erika McCallister, Timothy Grance and Karen Scarfone, 'Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)' *National Institute of Standards and Technology* (2010) <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.

[22] Mark Burdon and Paul Harpur, 'Re-conceptualising Privacy and Discrimination in the Age of Talent Analytics' *UNSW Law Journal* 37(2) (2014); S Morgan and C Winship, *Counterfactuals and Causal Inference: Analytical Methods for Social Research* (New York: Cambridge University Press, 2007).

[23] P Alston, 'CIA and Targeted Killings beyond Borders' (2005) 2 *Harvard National Security Journal* 283 <http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2_Alston1.pdf>; Allie Coyne, 'AFP reports data sharing with Russia, China', (18 June 2015) *iTnews* <http://www.itnews.com.au/News/405403,afp-reports-data-sharing-with-russia-china.aspx>.

(cont.)

privacy law but there is little examination of the effectiveness of such arrangements.[24]

- **freedom of expression and other civil liberties affected negatively:** Privacy is often seen as the parcel that reveals all of the other human rights and civil liberties such as freedom of expression, freedom of association, freedom of religion and other human rights and civil liberties.[25]
- **fear of living in a mass surveillance society:** There is the risk that any forms of Big Data expansion will be conceived as Orwellian and therefore undesirable.[26]
- **erosion of trust**: Erosion of trusts refers to trust of law enforcement within the community, and the other facet is where face-to-face community policing is reduced or replaced by relying more on data analytics. In the context of Big Data, trust issues manifest in two main areas - mass surveillance[27] and reduction in human interaction, particularly in contexts such as policing.
- **accountability:** There are different facets of accountability including the inadequacy of privacy and security legal frameworks, making intelligence agencies actions more visible and accountable, lack of publicly available impact assessment tests and the relationship with transparency and oversight.[28]
- **transparency**: Transparency is tied to effectiveness, acceptability and accountability. Transparency is linked to public confidence and trust in law enforcement and intelligence, [29]
- **scope creep:** There is a general concern that if a technology or type of data analytic is developed for one purpose, that this purpose could be used for other applications.

---

[24] Joel Reidenberg 'International Approaches to Public and Private Sector Data Privacy and Security' in Peter M Shane, John Podesta and Richard C Leone *A Little Knowledge: Privacy, Security, and Public Information after September 11* (Century Foundation Press, 2004) 98–9.

[25] Marko Milanovic 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' in his paper on the Social Science Research Network (March 31 2014) <http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2418485>. Jane Bambauer, 'Other Peoples' Papers' (2015) 94 *Tex. L Rev*; Rice, Simon, ANU Brandis receives long list of rights-limiting laws – now can he justify them? The Conversation, 6 August 2015 <https://theconversation.com/brandis-receives-long-list-of-rights-limiting-laws-now-can-he-justify-them-45645>; Ian Brown et al, *Towards Multilateral Standard for Surveillance Reform*, January 2015, Centre for the Internet and Human Rights <https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf>.

[26] Chalmers, Robert, 'Orwell or all well? The rise of surveillance culture' (2005) 30(6) *Alt LJ* 258 <http://www5.austlii.edu.au/au/journals/AltLawJl/2005/77.pdf>.

[27] Judy Putt (ed), 'Community Policing in Australia', *The Australian Institute of Criminology* (2010) <http://www.aic.gov.au/media_library/publications/rpp/111/rpp111.pdf>; Sean Richmond, 'National security debate misses big picture of 'balanced' response', *The Conversation* (25 February 2015) <https://theconversation.com/national-security-debate-misses-big-picture-of-balanced-response-37923>.

[28] Hal Abelson, Ken Ledeen and Harry Lewis *Blown to Bits: Your Life, Liberty and Happiness After the Digital Explosion* (Addison-Wesley 2008) 48–55; Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W W Norton & Company 2015) 74–6. Department of Finance and Deregulation, AGIMO/ Marc Vickers. (2014) *Draft Guide to Responsible Data Analytics*, 26 June 2014 <http://www.finance.gov.au/node/34900/> and <http://www.finance.gov.au/sites/default/files/Responsible%20Data%20Analytics%20Draft.pdf>.

[29] Lyria Bennett Moses, and Janet Chan, 'Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools,' (2014) 37(2) UNSW Law Journal 643.

[29] Keiron O'Hara, *Transparent government, not transparent citizens: a report on privacy and transparency for the Cabinet Office* (London, GB, Cabinet Office, 2011) 84.

(cont.)

This is potentially problematic if scope creep occurs without proper debate and risk assessments given the potential harms that could result for Big Data usage.[30],

- **understanding correlation and causation for decision makers:** the distinction between correlation and causation is sometimes poorly understood, particularly among those without data science expertise and there is concern that many decision makers will not sufficiently understand this difference and its implications.[31]
- **data quality assurance:** Analytics relies on quality of data. Any inferences drawn from data are dependent on the quality of the data, or at least the absence of systemic bias within the data.[32]
- **asset exposure:** De-identification and re-identification were considered as benefits previously where suspects could be potentially re-identified based on de-identified data. The risk is that the inverse is also true. Critical assets and targets may also be re-identified risking their safety and security.[33]
- **security:** There are many security concerns when using and storing large volumes of data such as the inadequate ability to store data, the possibility of data theft and misuse.
- **risk of not using big data.**

Big Data's opportunities and risks are still not fully tested. It is a evolving field in terms of the technologies as well as the policies and frameworks that support Big Data.

---

[29] National Audit Office. (2012) *Implementing Transparency* <http://www.nao.org.uk/report/implementing-transparency/>; Attorney-General's Department *Information security management guidelines,* Australian Government (1 November 2014) v2.0 <https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf>.

[30] Anne-Marie Oostveen and Diana Dimitrov, ' scanners can now identify us from 40 feet away', *The Conversation* (21 May 2015) <https://theconversation.com/iris-scanners-can-now-identify-us-from-40-feet-away-42141>.

[31] Harry Surden, 'Machine Learning and the Law' 89 Washington Law Review 1 (2014).

[32] Roger Clarke, 'Big Data Quality Assurance' (2015) <http://www.rogerclarke.com/EC/BigDataQA.html>; U Fayyad, G Piatetsky-Shapiro and P Smyth (1996) 'From Data Mining to Knowledge Discovery in Databases ' AI Magazine 17, 3 (1996). http://aaaipress.org/ojs/index.php/aimagazine/article/download/1230/1131; Laura Sebastian-Coleman, *Measuring Data Quality for Ongoing Improvement: A Data Quality Assessment Framework* (MK 2013).

[33] Jiuyong Li et al, 'Current Developments of k-Anonymous Data Releasing', *National e-Health Privacy and Security Symposium* (2006) <http://eprints.usq.edu.au/1307/1/13.pdf>.

3. METHODOLOGY

In order to assess how relevant international perspectives, policies, laws and practices that can inform Australian policymakers and support the development of law and best practices, the research team implemented three methods of enquiry: Empirical, doctrinal and comparative:

3.1. Empirical research

The study applied a theoretical framework that takes account of the diversity in technologies and practices associated with Big Data in different jurisdictions and organisations, as well as differences in legal frameworks and social context. The design of the empirical inquiry acknowledged the contingency and variability of technological design and practices.[34] In order to meaningfully explore, contextualise and map differences and agreements in the policy, laws and risk assessment and compliance practices in different jurisdictions and organisations, differences in 'technological frames' (being assumptions, expectations and knowledge about a technology) were taken into account.[35]

Interviews were conducted with key stakeholders, technologists, and users in each country in relation to their understanding of the capabilities and uses of Big Data, their perception of issues and challenges in relation to Big Data, their perception of existing and proposed strategies, policies, laws and practices, and their recommended responses to perceived challenges. Interviews were conducted face-to-face where possible and via Skype or video-conferencing where feasible. A total of 63 research participants took part in the research project: 38 from Australia (interviewed from 25 March 2015 to 13 November 2015), 14 from the UK (interviewed from 24 February 2016 and 18 March 2016) and 11 from Canada (interviewed from 15 October 2015 to 26 February 2016).

The goal of this report is to capture understandings, perceptions and views of individual research participants on a range of issues. I**t is important to emphasise that the empirical findings presented in this report provide a snapshot of the *views and perceptions* of research participants only. These views and perceptions may or may not be based on a comprehensive or accurate understanding of the issues involved. Given that the sample size is relatively small and not necessarily representative of the population of stakeholders in each jurisdiction, the findings are meant to indicate issues and not to be read as a comprehensive coverage of all relevant information. We do not attempt here to evaluate or correct research participants' views, although we have included cross-references to other sections in the report where appropriate.**

3.2. Doctrinal research

The legal and policy analysis for this study was undertaken to develop a contextualized understanding of the policy, legislation and regulatory frameworks relevant to Big Data adopted by Australia, the UK and Canada relevant to NSLE security objectives, especially to

---

[34] Lyria Bennett Moses**, '**Bridging distances in approach: Sharing ideas about technology regulation' in R Leenes and E Kosta (eds), *Bridging distances in technology and regulation* (Wolf, 2013) 37-51.
[35] Wiebe Bijker**,** *Of bicycles, bakelies, and bulbs: Towards a theory of sociotechnical change* (MIT Press, 1995); Wanda J Orlikowski & Debra C Gash, **'**Technological frames: Making sense of information technology in organisations' (1994) 12(2) *ACM Transactions on Information Systems* 174; Janet Chan, 'The technological game: How information technology is transforming police practice' (2001) 1(2) *Criminal Justice* 139.

identify potential policy options for Australia. This analysis reflects the law as at 31 March 2016 (Australia), 26 May 2016 (UK) and 1 June 2016 (Canada).

The three countries do not have an explicit Big Data legal framework for NSLE but do have a host of measures that are directly or indirectly relevant to Big Data application in that context. To assist in identifying measures that are of greater relevance to such a framework the researchers identified a set of preliminary indicators of an appropriate overarching legal and policy framework. Collectively the presence of these indicators would indicate a framework that supports the effective use of advanced analytics and large data sets for NSLE purposes, while respecting the rights and interests of all stakeholders (including data subjects, the broader community and the economy), addresses proportionality and evidence-based justification, and ensures comprehensive identification and management of risk and opportunities.

The indicators were jointly used as a lens to provide the researchers with the following lines of inquiry:

a) Is access for data mining enabled?

The framework would enable access to relevant datasets held by government agencies (domestically and internationally), to open source data and to relevant privately-held data in a manner that allows data mining subject to the governance and control mechanisms set out b)-h) below.[36]

b) Are legal controls comprehensive and proportional?

The framework would ensure that proportional legal controls inform and guide the design, operation and management of (i) data mining and analysis, (ii) data collection, (iii) data retention and deletion, (iv) data aggregation and (v) disclosure (domestically and, where required, internationally), NSLE objectives as well civil liberties, other legal rights and individual and commercial interests.[37]

c) Are legal rules clear, principle-based, consistent and instructive?

The legal rules of the framework would be clear, principle-based and consistent, providing officials with appropriate guidance to take reasonable decisions and perform their functions correctly and efficiently in a dynamic environment. These rules would be challenged to provide 'future proofing' while being specific enough to avoid ambiguity, and so maintain auditability.[38]

d) Is integrity of data and analysis supported?

The framework would support the integrity of data collected, retained and accessed by government for NSLE purposes, and the integrity of analytical and decision-making uses of such data and systems. Where integrity is assessed as low, data usage will reflect that fact and the principles in f) will apply.

---

[36] The enquiry into access to data also extends to the use and abuse of mechanisms such as encryption, for instance key escrow and end-to-end encryption.

[37] While the researchers agreed that it was important to consider 'other legal rights and individual and commercial interests' the vagueness of this phrase was appreciated. It was identified as one that would need to be revisited once the study enabled it to be defined with greater clarity.

[38] This also implies a consistent employment of the principles in relation to different agencies and data sets where objectives and risk are sufficiently similar.

e) Are data and systems protected?

The framework would protect the security of relevant data and systems. Appropriate measures would enable individuals to report concerns or breaches internally in a manner that supports integrity and governance.

f) Is accountability maintained?

The framework would ensure that access to data and data analysis and use for decisions is tracked and audited for justification, security and intrusiveness, and that decisions are subject to appropriate internal governance as well as independent oversight and accountability.[39] Decision-makers should remain accountable for their decisions, which imply an understanding of the provenance and integrity of data and awareness of any biases in the analytic process.

g) Are principles and rules regularly reviewed?

The framework would require the regular, transparent review of principles and rules to ensure that the system delivers intended results efficiently and reliably, proportional to impacts on civil liberties, other legal rights and individual and commercial interests.

h) Is there a sufficient measure of transparency?

To the extent consistent with the need for operational secrecy, the framework would ensure that the nature of data accessed, analytic processes employed, and who has access are as transparent as feasible for those potentially affected by decisions, and those with an interest in policy- and rule-making.

3.3. Comparative analysis

The empirical and doctrinal methodologies employed in relation to Australia were also used to examine current legislative and policy frameworks in the UK and Canada. Findings and insights from the studies informed the conclusions regarding the development of law and best practices for consideration of to be considered by Australian policymakers. Canada and the UK were selected for comparison with Australia for the following reasons:

a) The three countries are bound by the multilateral United Kingdom – United States of America Agreement [UKUSA Agreement].[40]

---

[39] 'Appropriate' in this document means reasonable and justifiable in an open and democratic society. Where relevant, it reflects proportionality principles.

[40] This treaty, known as Five Eyes, for cooperation in signals intelligence between the United States [National Security Agency (NSA), Defense Intelligence Agency (DIA), Federal Bureau of Investigation (FBI), and Central Intelligence Agency (CIA)], Australia [Australian Signals Directorate (ASD), Defence Intelligence Organisation (DIO), Australian Security Intelligence Organisation (ASIO) and Australian Secret Intelligence Service (ASIS)], Canada [Communications Security Establishment (CSE), Chief of Defence Intelligence (CDI), and Canadian Security Intelligence Service (CSIS)], the United Kingdom [Government Communications Headquarters (GCHQ), Defence Intelligence (DI), Security Intelligence (MI5), and Secret Intelligence Service (MI6)], New Zealand [Government Communications Security Bureau (GCSB), Directorate of Defence, Defence and Security (DDIS), and New Zealand Security Intelligence Service (SIS)]. The scope and time-frame of the Report required the team to choose three countries. General differences and similarities between the 5 countries led to the decision not to include the USA and New Zealand in the current study.

b) Australia, the United Kingdom, and Canada (like the other members of the UKUSA agreement) belong to the common law family of legal systems; are constitutional monarchies, and share common legal, cultural and political heritage and values.

4. COUNTRY CONTEXTS

Policymakers in Australia, Canada and the UK – like their global counterparts – are challenged to ensure that the data retention, access and usage regime is appropriate to enable NSLE agencies to counter terrorism and other crimes effectively, without disproportionally impacting on the rights of individuals. While technological developments have impacted on data generation, retention, accessibility and mining,[41] legal frameworks ensuring proportional access to data have not kept pace. Agencies in some cases employed data practices that, though legal, did not necessarily meet with large-scale public approval and threatened to undermine public trust in NSLE agencies.[42] This became clear after the June 2013 release of a cache of classified documents by Edward Snowden, a US employee of contractors for the US National Security Agency.[43] Increasing crime and terrorism concerns escalated the need for appropriate solutions. In Australia, for example, organised crime,[44] the rise of ISIS (also known as Da'esh), internal 'radicalisation', Australians joining foreign conflicts, a number of foiled plans for terrorist attacks on Australian soil and the Lindt Café siege[45] are major drivers of the NSLE agenda.

In Australia these concerns led to a Parliamentary inquiry into the gathering and use of criminal intelligence;[46] the decision to merge CrimTrac, the national policing information agency, and the Australian Crimes Commission, the federal agency investigating serious and organised crime;[47]and the adoption of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth), to ensure that commercial telecommunications data that would otherwise not necessarily be retained, is preserved for potential NSLE inquiries.

After the 2014 shooting incidents on Parliament Hill in Ottawa and in Montreal,[48] Canada introduced the so-called Bill C-51, a controversial[49] Omnibus bill with complex legislative amendments to several Acts, including the *Anti-Terrorism Act 2001.* The bill also led to the

---

[41] See Section 2.

[42] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015)Cite RUSI.

[43] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 0.7.

[44] Australian Crime Commission, *Organised Crime in Australia* (2015) 1 <https://www.crimecommission.gov.au/publications/intelligence-products/organised-crime-australia/organised-crime-australia-2015>.

[45] Commonwealth of Australia and the State of New South Wales, *Martin Place Siege: Joint Commonwealth - New South Wales Review* (2015) 2 <http://www.dpmc.gov.au/pmc/publication/martin-place-siege-joint-commonwealth-new-south-wales-review>.

[46] Parliamentary Joint Committee on Law Enforcement, Parliament of Australia, *Inquiry into the Gathering and Use of Criminal Intelligence* (2013).

[47] Michael Keenan (Minister for Justice), 'New Super Agency to Tackle Emerging Threats' (media release, 5 November 2015).

[48] The shootings occurred on 22 October 2014. See generally the Wikipedia entry at https://en.wikipedia.org/wiki/2014_shootings_at_Parliament_Hill,_Ottawa.

[49] According to Canadian Q.C. and prominent privacy expert Clayton Rice, 'Canada's Bill C-51: An Attack on the Rule of Law' (March 2, 2015) <http://www.claytonrice.com/canadas-anti-terrorism-bill-attack-rule-law/>. See also prominent privacy scholar Michael Geist, 'Why the Anti-Terrorism Bill is Really an Anti-Privacy Bill: Bill C-51's Evisceration of Privacy Protection,' (March 12, 2015) <http://www.michaelgeist.ca/2015/03/why-the-anti-terrorism-bill-is-really-an-anti-privacy-bill-bill-c-51s-evisceration-of-government-privacy/>.

(cont.)

enactment of a new piece of legislation, the *Security of Canada Information Sharing Act 2015* (SCISA).

In the UK, a series of events led to three 2015 reports on a more appropriate legislative framework.[50] The April 2014 judgment of the Grand Chamber of the Court of Justice of the European Union in the *Digital Rights Ireland* case[51] declared the EU Data Retention Directive[52] invalid, created a legal dilemma for the UK.[53] The Directive provided the legal basis for UK regulations requiring service providers to retain communications data for law enforcement purposes. As a consequence of the case, the UK was under pressure to promptly enact the *Data Retention and Investigatory Powers Act 2014* (**DRIPA**). To secure cross-party support, it was agreed that DRIPA would expire in December 2016 and that there would be a report by the Independent Reviewer of Terrorism Legislation.[54] This meant that the government was under pressure to present more appropriate and comprehensive legislation for implementation in 2016. In November 2015 the UK government presented a *Draft Investigatory Powers Bill* to Parliament. This *Investigatory Powers Bill 2016* was still being debated by the UK Parliament when this report was produced.

4.1. Constitutional frameworks

The constitutional framework of Australia, the United Kingdom and Canada governs the legal controls that inform and guide the design, operation and management of large datasets.

Under the Australian Constitution legislative powers to enact laws relevant to the ability of federal agencies to access and manage data-sets for the purpose of safeguarding national security and enforcing Australian law are vested in the Commonwealth, subject to the States' concurrent powers where relevant.[55] At the same time, States have inherent, residual powers (powers not included in section 51 of the *Constitution*) over criminal law enforcement within their respective jurisdictions. As a result, powers over State policing and powers over the Commonwealth NSLE (ASIO, Australian Federal Police etc) are limited to their particular jurisdictions. However, these boundaries are blurred when State police agencies are involved in the administration and enforcement of federal as well as State criminal law[56] or where data is shared between State and Commonwealth agencies.

Similar to Australia, Canada is a federation of ten provinces and three territories. Its *Constitution Act*, 1982 contains the Canadian Charter of Rights and Freedoms, which

---

[50] Intelligence and Security Committee of Parliament (ISC), Privacy and Security: A modern and transparent legal framework (2015); David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015); RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015).

[51] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger and others*, EU: C:2014:238.

[52] Directive 2006/24/EC.

[53] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) 1.4.

[54] DRIPA s 7.

[55] *Australian Constitution*, s 51(v): 'Postal, telegraphic, telephonic, and other like services'; s 51(vi): 'The naval and military defence of the Commonwealth and of the several States, and the control of the forces to execute and maintain the laws of the Commonwealth'; s 51(xxix): 'External affairs'; and s 51(xxviii): 'The influx of criminals'.

[56] *Coleman v Power* [2004] HCA 39; 220 CLR 1 at [80].

(cont.)

enshrines the constitutional guarantee of the civil rights and liberties of every citizen in Canada, including freedom from unreasonable search and seizure.[57]

The three major features that distinguish the United Kingdom from Australia and Canada are (1) its constitutional status as unitary state (albeit with some powers delegated to Scotland, Wales and Northern Ireland),[58] (2) membership of the European Union and the acceptance by the Supreme Court of the United Kingdom of the Court of Justice of the European Union's jurisdiction[59] in relation to the interpretation of the Treaties; and the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union; and (3) the *Human Rights Act 1988* (UK), that enables individuals to seek remedy in the UK courts for breaches of their rights under the European Convention of Human Rights. This includes Article 8.1 of the ECHR, which provides an explicit right to respect for one's 'private and family life, his home and his correspondence' that are subject to restrictions 'in accordance with law' and 'necessary in a democratic society'. Article 8 also incorporates a right to be free of unlawful searches. Although like Australia, the English common law does not recognise a discrete tort of privacy, the United Kingdom's courts are required to 'have regard' to the ECHR in developing the law.[60]

[57] *Canadian Charter of Rights and Freedoms*, cl 8.
[58] Though the Parliament of the United Kingdom has devolved some its powers to the Scottish Parliament, the National Assembly for Wales, and the Northern Ireland Assembly.
[59] By virtue of Article 267 of the Treaty on the Functioning of the European Union.
[60] *Mosley v MGN* [2008] EWHC 1777.

5. EMPIRICAL FINDINGS

A total of 63 research participants took part in the research project: 38 from Australia, 14 from the UK and 11 from Canada. Research participants covered a range of stakeholders including law enforcement and intelligence officials, oversight officials, policymakers, computer technologists (for the Australia study), and representatives of citizen groups. For details of the recruitment, consent and interview processes, see the Methodology Report.

The goal of this chapter is to capture understandings, perceptions and views of individual research participants on a range of issues. I**t is important to emphasise that the empirical findings presented in this chapter provide a snapshot of the *views and perceptions* of research participants only. These views and perceptions may or may not be based on a comprehensive or accurate understanding of the issues involved. Given that the sample size is relatively small and not necessarily representative of the population of stakeholders in Australia, the findings are meant to indicate issues and not to be read as a comprehensive coverage of all relevant information. We do not attempt here to evaluate or correct research participants' views, although we have included cross-references to other sections in the report where appropriate.**

We classified research participants in accordance with their role and the nature of the organisation for which they worked. In each case, there were three potential classifications: Operational (O), Technical (T) and Policy (P). The Policy classification was broad, and included individuals and agencies with a legal or policy role, community organisations and NGOs and individuals and agencies with an oversight role over operational agencies. Where a research participant was being interviewed in relation to a recent former role, the coding matched the former role and organisation rather than current role and organisation.

Table 5-1 summarises the numbers of research participants by type of organisation for each country. All were selected because they were able to provide relevant information on the use of data or regulation of data use for law enforcement or security intelligence. Time and resource constraints necessitated relatively modest sample sizes for the UK and Canada components of the study. Although the Australian, UK and Canadian samples were drawn from broadly similar types of organisations (technical organisations were excluded in the UK and Canada), there were some notable differences in the research participants. The three samples may therefore not be directly comparable.

Table 5-1: Number of Research Participants by Organisation Type and Country

	Operational	Technical	Policy	Total
Australia	19	7	12	38
UK	5	-	9	14
Canada	6	-	5	11
Total	30	7	26	63

It is important to emphasise that the empirical findings presented in this section provide a snapshot of the *views and perceptions* of research participants only. These views and perceptions may or may not be based on a comprehensive or accurate understanding of the issues involved. The findings are therefore meant to be *indicative*, rather than representative, of the views of the populations of stakeholders in these countries.

5.1. Current use of data in law enforcement and national security agencies

The results in this section are based on 19 research participants in Australia, five in the UK and six in Canada who were working or had worked in operational organisations. Given the small sample sizes in the UK and Canada components, the main findings reported are based on the Australian sample, with notable differences in the UK and Canada briefly mentioned.

5.1.1 Types of data used

Research participants from all three countries reported working with a wide range of data, from telecommunication metadata, official data, data from international partners, internal databases, information provided by the community, geospatial or financial data to open source or online data and communication signals.

5.1.2 Sharing of data

The sharing of data between agencies domestically and internationally is a highly curated process in all three countries. There are often different rules for different agencies (based on legislation or memoranda of understanding), and different levels of access depending on classification (nationally) and international partnerships (internationally). In Australia these may be informed by particular concerns around issues such as implicit disclosure of agency capabilities and exposing Australians to risk of the death penalty. Data sharing among agencies and with foreign counterparts involves decisions that are not easily automated.

Most of the data shared among agencies in Australia relates to identifiable individuals. Data may also be shared with the public, either directly, or through the media or social media, for example in response to emergency situations.

One noteworthy element of UK data sharing arrangements is that the principle of proportionality seems to have an impact on data sharing arrangements among government departments, particularly for research and evaluation rather than directly operational concerns. In particular, the amount of data shared may be minimised, so that the least amount of data is shared to facilitate a clear purpose. However, much crime data is shared automatically through the use of shared databases such as the Police National Computer.

The default rule in Canada is that sharing between domestic agencies is allowed unless expressly prohibited. In the international context it was more complicated. Research participants pointed out that there had been problems with sharing in the past leading to Charter of Human Rights violations including torture. Some participants in Australia and Canada mentioned that over-classification of data had prevented sharing.

5.1.3 Main purpose of using data

Research participants from operational organisations in Australia nominated using data for a range of past-focused and future-oriented purposes. Past-focused purposes include investigation, arrest and prosecution, reporting, and event evaluation; while future-oriented purposes include prevention or disruption of incidents or mitigation of risks, intelligence gathering, identification of trends or risks, policy or service decisions and trust building. Even where research participants described using data for future-focused activities, the analysis primarily revolved around investigating individuals for past conduct or identifying individuals who may be involved in future conduct rather than understanding broader trends among groups. As a result, almost all research participants were only interested in identified, rather than de-identified, data.

In the UK, apart from the use of data for crime prevention, criminal investigation and security intelligence, research participants reported using crime and offender data to conduct research on offending trends and to evaluate criminal justice programs. It is possible that evidence-based policy in criminal justice research is more developed in the UK than in Australia, although further investigation into the Australian situation would be required to draw any conclusions given differences in sample composition between the two components of the study and the small sample size.

Only three research participants in the Canada component of the study responded to this question; the purposes of using were also diverse including predicting trends, disruption, intelligence for investigations, business intelligence and efficiency metrics.

5.2. Current concerns regarding access to and sharing of data

Three main concerns were raised in all three countries: legal requirements including privacy issues (real or perceived), technical issues, and issues relating to ownership of data and trust.

Legal requirements: The most frequently cited concern in all three countries (equal with technical issues in the UK) related to real or perceived legal requirements, including in relation to privacy issues. In Australia legislative requirements are compounded when attempts are made to share data across State and Territories under our federated system. A small number of participants were sceptical whether legal restrictions were real and whether the interpretations giving rise to concerns about data sharing barriers were accurate.

Technical issues related mainly to matters such as data format, data 'silos', non-availability of historical data, and their agency's ability to deal with the volume of data.

Data ownership and trust between agencies or individuals were the two factors that appear to explain some of the reluctance to share data. Reference was made to **cultural issues** (turf protection, gender hierarchy, agency rivalry) that could make data sharing difficult.

Most of the identified barriers to data sharing in the UK were similar to those mentioned in the Australian study. Issues raised in Australia but not the UK include federalism, legal limits on process, different interpretations of legal requirements, compatibility of data formats, handling data volume, reliance on personal relationships, and over-classification. Issues raised in the UK but not Australia include the time taken to negotiate inter-agency agreements, difficulty cross-linking data, technical issues with data extraction and the challenge of knowing what to ask for. While the small sample sizes mean differences should not be over-emphasised, it is possible that these can be explained to some extent by Australia's federal system and the existence of CrimTrac, as well as the possibility that some legal ambiguities are clarified through inter-agency agreements in the UK. UK participants provided useful details on rules that apply to international data sharing including the focus on location rather than citizenship for categorising data, the third party rule, the risk of compromising operations, and limitations on data sharing on sensitive topics. These rules are likely also applicable to Australia.

5.3. How problems can be overcome

In Australia, some of the participants concerned with legal barriers to data sharing proposed legislative change, which may require an appropriate political environment and/or engaging the public around questions of privacy and security needs. Other Australian participants recognised that cultural, as well as legal, change may be required and that there may be a role for better education on the operation of the current legal regime. Proposed solutions to

technical barriers included compliance with data format standards, better training, communication and support for frontline officers, better data management and systems integration. Addressing cultural barriers to data sharing was seen as crucial in overcoming perceptions about legal, technical and institutional barriers to sharing.

Common threads between the suggestions from Australian and British research participants, include a desire to change the political environment (and a recognition this was likely linked to external events). The most useful new insight from the UK study is the suggested formal and informal means through which trust can be built between agencies, including a combination of time, data sharing agreements and joint mission management. The suggestions to move terminology away from 'data sharing' and to engage in comparative risk assessment are also worth noting.

While only two research participants in Canada directly answered this question, there were points in the interviews when discussing other concerns and risks where solutions to problems were identified. The two participants both identified cultural change as important in addressing concerns including change in sharing, ownership and trust, as well as resolving technical concerns. Other inferences drawn generally from the other interviews included resolutions to concerns through providing sufficient resources both for the staff and for acquisition of technologies.

5.4. Big Data: potentials, limits and risks

5.4.1 What is Big Data?

'Big Data' is a term without a single precise meaning; rather it is used to articulate a range of practices. In the context of national security and law enforcement in Australia, research participants' definitions of Big Data were focussed on both technical and user requirements. The main requirements relate to handling volume, analytic capacity to provide useful and reliable information, dataset integration, embracing new technologies and processing speeds. A number of participants in technical organisations regarded Big Data as mostly a marketing term that captures the current trend of generating and making use of large volumes of data.

There are no significant differences in the understanding of Big Data between UK, Canadian and Australian research participants. However, there was much scepticism about the term among operational and policy participants in the UK; some would prefer the more precise terminologies used in legislation or operations.

5.4.2 Capability of Big Data

In terms of capability, Big Data was seen by Australian research participants as involving more advanced analytic capacity, more 'complete' and 'rich' data, the ability to cross-check information, the ability to identify new targets through the existence of common features, improved efficiency and effectiveness, improved accuracy of inferences, and enabling better decisions and enhanced service delivery. Not every participant saw an advantage to Big Data, and one cautioned against unrealistic expectations. There is some evidence that the potential advantage of Big Data was perceived differently between participants from different organisations in Australia: those from operational organisations generally saw the investigative advantage that Big Data could bring, while those from technical organisations envisaged that Big Data could offer a more proactive way of doing policing and intelligence work.

In the UK, at least in law enforcement, bulk personal datasets (non-specific to intelligence targets, such as telephone records) seemed to be used for specific queries only. Some specific advantages of Big Data mentioned by UK participants include: not requiring an advance hypothesis but rather allowing for unforeseen insights; using Big Data as evidence; facilitating more data-driven decision-making; identification of targets and identification of patterns and trends – these were all raised by UK participants but not in Australia (at least not in those terms). However, scepticism about capabilities was quite strong in the UK, with 4/14 participants making the point that there was a need for caution about expectations.

In Canada three participants cautioned against unrealistic expectations while two believed that governments would be very slow to uptake Big Data, and even slower to do so in a cost effective way. They thought that a lack of culture and training could make Big Data less relevant as decision-makers were more likely to be from traditional social science backgrounds.

5.4.3 Use of Big Data and data analytics

More than half of the participants working in law enforcement and national security agencies in Australia said that they were not currently using Big Data. This suggests that their conceptions of Big Data and its capability and value were not necessarily based on first-hand knowledge or experience with this technology. In spite of this, a variety of data analysis and visualisation tools were 'currently used' in these agencies. Participants more frequently reported use of data visualisation/ mapping tools and data browsing/searching/ sorting/ linking and summarising tools than machine learning or automated analytic tools.

A significantly higher proportion (11/14) of research participants in the UK compared to Australia (14/38) reported that Big Data was being used in their own (operational) work or that they believed it was being used for law enforcement and/or security intelligence purposes. This is consistent with the view of all UK research participants who commented that the UK is internationally a leader on data and analytics for law enforcement and national security. Most of the examples of Big Data use were focussed on investigating past events or understanding the present; only three examples concerned predictive analytics. As in Australia, operational organisations in the UK seem to be using a variety of data analysis and data visualisation tools. Many (3/5) UK operational participants are relying on traditional statistical analysis rather than newer data science techniques.

In Canada only three participants out of six from operational organisations stated that they were using Big Data, while the other participants stated that they were just starting to us Big Data visualisation tools, but the uptake had so far been slow. However, two of the participants worked with Big Data on a daily basis and one programmed bespoke tools used within their organisation. Four out of six participants from operational organisations in Canada indicated that they have been using data analytics and statistical analysis for quite some time, but the use of machine learning or predictive tools was not mentioned.

5.4.4 Barriers/challenges to using Big Data

Many of the barriers and challenges to the use of Big Data listed by Australian participants resembled those raised in relation to data sharing. These include legal and privacy issues and inconsistent data formats. A significant number of research participants also raised concerns about public acceptability of agencies' use of Big Data. Technical problems were also linked the challenge of obtaining and maintaining resources, including human resources with technical skills, and correct understanding of user needs. The need to communicate the uncertainty inherent in inferences drawn from Big Data was also suggested as a challenge.

Research participants in Australia identified a variety of cultural barriers to greater use of Big Data for law enforcement and national security. These include the fact that Big Data is unlikely to be used unless there is institutional support and appropriate levels of confidence in technology among users. This is not necessarily a question of changing cultures since some barriers may be appropriate. Research participants stressed the potential negative impacts of both false positives and false negatives, and the adverse reputational impact that could follow.

Research participants in the UK reported similar types of barriers to the use of Big Data; for example, they operated under resource constraints. UK participants were more likely than Australian ones (9/14 vs 8/37) to focus on technical and resource issues. Legal issues that were identified in this study reflected the nature of the UK regime, including the requirement for necessity and proportionality. UK participants were more aware than their Australian counterparts that some of the data collected may be incomplete or biased. This concern was not raised by the Australian participants.

Legal requirements were presented as a challenge to the use of Big Data in Canada. Ironically it was a lack of adequate privacy laws that was perceived as the barrier; not that privacy laws prevented Big Data usage. Some research participants discussed how the *Privacy Act* was out of date and unsuited to technologies in general. These problems generated a hesitancy and reluctance to move toward more invasive technologies, and that the Act contained much weaker provisions than the *Personal Information Protection and Electronic Documents Act 2000* which governs private organisations. Research participants in Canada identified cultural and technical barriers as a significant challenge. A variety of cultural barriers to greater use of Big Data for law enforcement and national security include the fact that Big Data is unlikely to be used unless there is institutional support and appropriate levels of trust, and confidence in technology among users.

5.4.5 Risks of using Big Data

In Australia, privacy, data security and integrity, misuse of data and misplaced trust in technology or algorithms were raised as the most significant risks of Big Data, while only one research participant was concerned about the risk of discrimination. Those in operational organisations seemed to be less concerned about misuse of data and more concerned about harm to their own organisations (through political and reputational risks, negative public perceptions and information overload) compared to other groups. Of particular interest is the fact that those in operational and technical organisations were conscious of misplaced trust in technology, an issue of less importance to those in policy organisations. The variability of identified risks between individuals and organisations suggests that broader awareness of the diversity of risks across sectors would be beneficial.

Most of the risks identified in by Australian research participants were also mentioned by the UK participants. The exception was 'overload' (which was mentioned by 4 Australian participants), but while that was not recognised as a risk in the UK, constraints on human resources were mentioned as a barrier. In the UK sample, data issues were mentioned more often than legal and privacy issues. Further, some new issues were raised, in particular the risk of a negative impact on freedom of speech, risk of proliferation, the possibility that the outputs would not be usable as evidence in court, and the potential for resources to be misdirected. Some differences in identified risks could be due to the European human rights framework within which the UK operates, and the history of colonialism which gives the UK continuing international influence. The potentially limited use of the outputs of data analytics as evidence in court exists in both countries, but this type of use is not the primary objective in either jurisdiction. Similarly, balancing resourcing demands is likely relevant in both jurisdictions. We cannot draw conclusions from risks omitted in UK interviews due to small sample size.

In Canada, the main identified risks of Big Data related to privacy, data integrity and and general technical issues. Both operational and policy groups expressed the view that there were risks to privacy. A participant who both worked with Big Data on a daily basis and who developed Big Data tools, stated that privacy was less of an issue than discrimination. Other participants used the term 'harm' to include privacy risks.

5.4.6 Who is exposed to these risks?

Research participants identified a broad range of groups who may be subject to the risks associated with Big Data. The most popular response to the question 'who is exposed to the risk?' was 'everyone' (or related terms) by research participants in all three jurisdictions.

In Australia, various groups were mentioned specifically including government and government workers, law enforcement and security agencies and personnel (particularly informants and undercover police), minorities and those at the margins, children and young people, and people of interest to the agencies.

Research participants in the UK were equally concerned as those in Australia about the broad risk to the community and the risk to disadvantaged groups. UK participants were also concerned about the potential for poor quality decisions if data analytics was done badly and the impact on government of mistakes.

5.4.7 Management of Big Data risks

A wide variety of suggestions were offered by participants on how different types of risks might be managed. These included legal change (balancing benefits and risks), clear public communication, constant adaptation, technical controls, sophisticated de-identification, technical education for users and ongoing use of oversight agencies and monitoring. Many of these were suggested as responses to more than one category of risk.

The main differences in relation to the management of Big Data risks between the Australian and the UK participants were the following: the UK sample had a greater focus on international law and human rights frameworks in the context of regulation, a broader understanding of the different groups that might benefit from education or training, and more emphasis on the idea of public and multi-stakeholder engagement (two way rather than one way communication) combined with greater government transparency. Existing UK initiatives on a data ethics framework, evaluation processes and minimisation of data sharing are also worth noting, as is the suggestion for system warnings when data requests are excessive.

Research participants in Canada suggested that access controls should be more in line with the restraints imposed on the private sector, and restrictions on third party data sales should be tightened. More data security requirements were also suggested, as was better education of the public about the actual versus perceived risks of Big Data.

5.5. Regulation

5.5.1 Laws, regulations, and internal guidelines

Research participants were asked to identify laws, regulations and procedures governing the use of data by law enforcement and security agencies.

In Australia, participants from government and independent oversight agencies were more likely to mention agency-specific legislation, the *Archives Act* and internal documents or memoranda of understanding than other participants. Some participants stated that they relied directly on legislation whereas others relied primarily on internal documents (such as manuals) that were themselves designed to conform to legislative requirements. This raises the possibility that differences in the understanding of what makes up the legal framework explains some of the differences in perceptions about the adequacy and effectiveness of that framework. It also suggests that, within agencies, internal documents and manuals may be the primary reference point rather than the legislation on which such documents may be based. Overall, the *Privacy Act* and *Australian Privacy Principles* were mentioned most frequently, albeit often in the context of inapplicability to particular government agencies.

Research participants in the UK identified a wide range of legislation and regulatory instruments governing the use of data. Differences between the research/NGO sector and the government sector were limited to the least mentioned categories: European human rights instruments, the Telecommunications Act and national security directions (research/NGO only) and memoranda of understanding, dataset specific legislation, ethical codes and information management requirements (government sector only). As in Australia, internal guidelines are often a primary reference point within operational agencies. Also similar to Australia, most existing UK laws focus on data collection and access, not data analysis. There were some examples given where the law did potentially restrict data analysis, including the general proportionality requirement, the right to challenge automated decisions and a requirement for 'fair' processing. There are further provisions in the *Investigatory Powers Bill*.[61] Perhaps most significant is the fact that the requirement for proportionality was mentioned very frequently, cutting across particular identified legislation. The principle would seem to be very familiar within the UK context across a broad range of roles and organisations. This may be due to the fact that the concepts of necessity and proportionality are embedded 'in the practices and training materials of all public authorities who apply [RIPA]' (Anderson 5.18). Conversely, the principle of proportionality was only mentioned in two Australian interviews.

Two frameworks were identified by 9 out of the 11 research participants in Canada. These were Privacy (Privacy Act and privacy frameworks in general) and Sharing (C-51 / *Security of Canada Information Sharing Act 2015*). Approximately half of the participants also identified the Charter, and Treasury Board Policies and Directives (these formed the main types of general guidelines for issues) and agency specific legislation. Participants in different roles and sectors equally recognised Privacy legislation, sharing legislation of C-51/ *Security of Canada Information Sharing Act 2015*and the Charter.

[61] *Investigatory Powers Bill* cls 134, 151, 170, 190 and 191.

5.5.2 Accountability, transparency and oversight mechanisms

Research participants in Australia discussed a range of accountability mechanisms, both external and internal, that form an important component of the regulatory framework for agency use of data. External oversight comprised Parliament, independent officers and agencies such as the Inspector-General of Intelligence and Security (IGIS), warrant requirements and transparency reporting. Internal oversight included agency processes, complaints mechanisms, audit trails, mandated action in the event of mistakes, and training and assessment. In addition, there were personal factors, such as fear of publicity and a strong sense of professionalism that work against the misuse of data. This illustrates that legislation cannot be viewed in isolation from other regulatory elements and cultural influences. The challenge is that some of these mechanisms are either not well-known or not trusted outside the agencies concerned, which may also explain differences in participants' perceptions of the appropriateness and effectiveness of the regulatory regime.

The UK oversight regime differs from the Australian regime. In particular, under the current law, there are separate Commissioners and Tribunals that split the role played in Australia by organisations such as the Inspector-General of Intelligence and Security (IGIS). This regime will be changed under the *Investigatory Powers Bill*. However, as in Australia, the UK relies on both independent/external and internal oversight mechanisms.

All participants in Canada ,except one, believed that there was not sufficient transparency and oversight. Concerns were raised over whether increased transparency would be meaningful absent increased education and training to understand Big Data systems. Algorithmic transparency was regarded as a desirable outcome only if would be sufficiently understood by decision makers. Canadian participants also identified the problem of oversight silos and the need for better oversight appropriate for the new formation of sharing under the *Security of Canada Information Sharing Act 2015* with appropriate resources levels to ensure that oversight is robust. The lack of accountability mechanisms was not directly mentioned in the interviews though it is difficult to separate comments about oversight with those of accountability.

5.5.3 Appropriateness and Effectiveness

In Australia, research participants working in government were generally more positive in their evaluation of the appropriateness and effectiveness of laws, regulation and oversight than those in the private/research/NGO sectors. As noted above, some of this divergence may flow from differences in knowledge and understanding about the regulatory regime itself, inevitable in the case of internal oversight mechanisms. Some of the difference, in particular whether concerns relate to restrictiveness of the regulatory regime resulting in reduced capacity or the sufficiency of protections for citizens, likely follows from differences in values. Those who commented on internal auditing and procedures and the effectiveness of independent oversight mechanisms such as the Inspector-General of Intelligence and Security (IGIS) did so positively. Views on the appropriateness and effectiveness of privacy laws were more mixed.

Similar to the findings in Australia, UK research participants working in government were generally more positive about laws, regulation and oversight than those in the research/NGO sectors. There is a greater overlap in relevant laws identified between different categories of research participants in the UK compared to Australia. The explanation for differences in views in the UK thus likely rests heavily on differences in values (see section 5.6) and challenges of trying to perform particular functions with limited access to data. Opinions about the appropriateness and effectiveness of the *Investigatory Powers Bill* (older version) were mixed. The Bill seems to have resolved some (not all) participants' concerns about transparency, clarity, simplicity, comprehensiveness and currency of existing laws. However, those concerned that the current legal regime was too permissive retained the same concern about the Bill.

Unlike findings in Australia and the UK, there was not a clear division in Canada between those in the research/NGO sectors who were sometimes critical (particularly about oversight) and those in the government sector who were generally uncritical, or focussed on restrictiveness. In Australia there were 22 on the positive side with only 3 on the negative side. In Canada this distribution was more equal with 4 positive, and 5 negative. Research participants from all sectors and roles expressed strong concerns with appropriate oversight mechanisms.

5.5.4 Perceived shortcomings in law and regulation and proposals for reform

Research participants in Australia raised a variety of specific and general proposals for reform. Some of these may not be appropriate and others may be based on limited knowledge of the regulatory regime or the participant's limited viewpoint. There are, however, some suggestions that are worthy of more detailed consideration. Specific proposals in that category include:

- the possibility of reducing 'red tape' without reducing oversight,
- reducing complexity, enhancing consistency across agencies and jurisdictions,
- limiting duplication of oversight,
- enhancing alignment between the warrant regime, privacy law and how data can be used in the course of analysis, and
- holistic consideration of data deletion and retention requirements (particularly for data available online).

One participant suggestion worth considering is conducting research (or engaging in public consultation) on evolving public attitudes towards privacy in order to enhance the alignment of law with community values. This is particularly important given the divergence among views expressed by research participants. Seemingly neutral suggestions such as the need to 'update' laws were, when analysed, tied to recommendations for moving in one direction or the other (towards permissiveness or restrictiveness).

Another broad but useful suggestion was the idea of developing a common framework for regulation of data access, use and action based on evidence of the effectiveness of particular uses of data and the degree of risk involved in such uses. Such a framework could also examine the balance between restrictions on access, restrictions on use and restrictions on action that might be taken.

The following suggestions made by UK participants are of interest to the Australian law reform process: (1) suggestions for the conditions under which law reform decisions in this area ought to be made (based on evidence of privacy risks and security benefit, including proper justification for operational cases), subject to transparency issues discussed in 2.6.4 of the UK and Australian Reports; (2) ideas for improving oversight and accountability; (3)

the importance of a principles-based regime that is less likely to date quickly; and (4) the importance of clarity and comprehensiveness.

Research participants in Canada noted that laws around privacy and oversight required updating. There was an additional call for updated Guidelines and Directives for sharing data with foreign agencies in an easier to understand and transparent fashion that could be harmonised across agencies. Similar to the Australian study, participants called for reduction of the complexity and to enhance harmonisation of practices across agencies. Where research participants from the Australia Study expressed the possibility of reducing 'red tape' without reducing oversight, Canadians did not address 'red tape' issues. The majority of participants were concerned about inadequacy of the oversight framework.

5.5.5 Regulation by design

There is significant literature on the extent to which one can achieve regulation through technological design, either generally or in particular cases (such as Privacy by Design). Research participants in technical organisations in Australia confirmed that elements of regulation by design (privacy/compliance/security by design etc) were already incorporated in their software, particularly in the case of privacy and personal information security, data integrity, regulatory compliance and testing and evaluation. Compliance by design measures included sometimes fine-grained access restrictions, built-in audit tracking, cybersecurity measures such as encryption, de-identification of data, data deletion processes, cross-checking tools to enhance discover inconsistencies in data, provenance tracking, in-built processes that match regulatory requirements, testing and evaluation. In many cases, these are designed around the needs of particular customers and in consultation with users, oversight agencies and/or legal advisers.

The Australian interviews suggested, however, that more can be done to utilise design features to mitigate legal and policy risks. Few research participants, for example, addressed questions around comprehensibility of outputs to decision-makers. The re-identification risk was also largely ignored, partly because many systems do not deal in de-identified data. Only one research participant discussed how design could reduce the risk of discrimination. Research participants in technical organisations gave various responses to the question about agency inter-operability, including the fact that the challenges were not primarily technical.

Only three UK participants commented on regulation by design; they noted features similar to those discussed in the Australian study including access controls and audit checks. The positive reaction by the NGO shows that that particular NGO may have been unaware of the commonness of such measures. Greater publicity of existing measures would have many benefits, including increasing public confidence. There may also be benefits for agencies in sharing ideas for compliance by design with each other. Also of note is the comment by one research participant that '[o]fficers won't trust it if it is wrong once' and the resulting importance of evaluation prior to deployment.

Data integrity and cost were the only design features that were taken into account by each of the three research participants in Canada, all having worked in operational organisations. The question about privacy by design yielded an interesting result where one participant placed this responsibility with the data owner, another said that they didn't factor privacy, while the last research participant laid out extensive measures used to assess and minimise privacy concerns.

5.6. Values and Big Data

5.6.1 Protections where individual consents to use or sharing of their data

Research participants in the Policy grouping raised a range of issues regarding use of data obtained with consent. These included the need for consent to be meaningful, informed and freely given, and the continuing obligation on agencies to store data securely and use data for a proper purpose. There are also questions around the revocability and expiry of consent as well as consent by children and young people. Some research participants would move in a different direction, reducing consent requirements (such as advance statement of purpose) to facilitate better exploitation of data or removing consent requirements entirely.

Research participants in all three countries mentioned issues around the 'quality' of consent, continuing limits on its use (including proper purpose) and security requirements.

The issue of expiry or revocation was not raised in the UK study. One interesting issue explored by some UK research participants is how consent requirements fit with national security and law enforcement exceptions. The idea of 'societal consent' could be a useful term here.

The issue of expiry or revocation was raised in Canada. Two research participants expressed concerns over implied and opt-out standards calling for opt-in and express consent.

5.6.2 Attitudes to privacy

There was a wide spectrum of views among Australian research participants about the importance of privacy, particularly in the context of serious, imminent threats. These ranged from a sense that privacy is a 'complete myth' to the belief that privacy must give way or be balanced against other needs in some circumstances. No-one expressed the view that privacy should always be prioritised. In some cases, the differences among research participants can be linked to different perceptions about how important privacy is to the Australian public and segments thereof.

Research participants in all three countries had varied views on the importance of privacy, particularly in the context of serious, imminent threats.

As in Australia, no-one in the UK sample expressed the view that privacy should always be prioritised, although the view was expressed that security threats never justified untargeted intrusions on privacy. While the UK study revealed differences in the relative importance of privacy between different sectors (research/NGO compared to government/independent, the latter being more likely to say privacy should give way), research participants from both 'sides' emphasised the importance of following rules relating to oversight, necessity and proportionality. As observed by one of the participants, there are ways of improving both privacy and security in which neither is sacrificed.

5.6.3 Privacy versus security: A scenario

Participants in all three countries in the Policy group were presented with a scenario in order to analyse how they reacted to the tension between individual privacy and an urgent security threat (kidnapping, child sexual assault and terrorism).

Child kidnapping and child sexual assault were treated similarly by most research participants in Australia, while some research participants (still a minority) felt changing the context to terrorism would make a difference. The answers to particular suggestions for data-based tools were diverse, suggesting that the particular features of a scenario will

sometimes trump general value preferences. There are some threads through the responses, in particular references to the need for proportionality, the need to avoid inappropriate use of state power, the need to narrow the people affected (to avoid affecting 'many people who have nothing to do with the case'), and the need to satisfy legal requirements such as reasonable suspicion and warrants.

Most UK participants gave the same answers to the scenario whether the context was kidnapping, child sexual assault or terrorism. There were some important differences in the UK responses, including the emphasis on proportionality, the suggestion that data be deleted when it was no longer needed, the suggested need for evidence of reoffending to draw a link with 'known kidnappers', and the fact that many potential suspects would already be under surveillance. Also, there was some scepticism about the effectiveness of the hypothesised CCTV face recognition matching tool.

Three of the Canadian research participants gave the same answers to the scenario whether the context was kidnapping, child sexual assault or terrorism. They indicated that there are sufficient legal provisions and flexibility to allow law enforcement to move to more intrusive measures in order to curtail the threat. Only two participants indicated potential problems such as abuse or scope creep, and only one participant was uncomfortable with the use of Big Data techniques including the escalation of context.

5.6.4 What transparency is required

Transparency is a significant challenge for national security and law enforcement agencies. Transparency can ensure that errors and biases are addressed, is a deterrent to misuse of data, is an important public value, and is an important element of democratic accountability. However, operational secrecy is also crucial for operational effectiveness in many situations.

Overall responses of research participants in Australia differed between transparency of the *data* employed in analysis and transparency of the *analysis* itself. Participants generally agreed either that the types of data used should be transparent, or at least that there should be some information about the types of data used (for example, an envelope within which data used must fall). Even in the case of disclosure of data used, there are risks that '[i]f criminals know what is collected, they will avoid leaving a trail'. Concerns about disclosure of algorithms were greater, as this was seen as more closely aligned with 'capabilities' that are generally kept secret to preserve effectiveness. Full transparency was regarded as controversial even within government. Research participants recognised that while it is important for users to understand the data and algorithms underlying their decisions, there are limits to the technical comprehension of users and the operational capacities need to be protected from potential leaks.

In the UK, transparency also raises questions about competing priorities – operational effectiveness, trade secrets and democratic accountability. Although some research participants did not believe in transparency about the types of data collected, there was still more concern about disclosure of algorithms than disclosure of data types. Noteworthy points arising from the UK study include the discussion about oversight and trust and the inevitable reliance on co-operation between oversight and operational agencies. Fuller transparency (for example, direct access to computers) risks undermining that trust and the joint construction of oversight systems. The possibility of post-surveillance disclosure was also a new finding in the UK study.

Unlike in Australia, the four Canadian research participants who responded were not concerned about competing priorities in increasing transparency. In the Australian study there were differences between transparency of the data and of the analysis outputs. In Canada there was no differentiation. The Canadian responses instead focussed more on

utility, education, limits and the importance of trust and rules when sharing information between agencies.

5.6.5 How views align with others

Research participants in Australia were generally aware that their own views were located on a spectrum and that they were not shared by all stakeholders. It would seem there are four clusters of opinion-holders: rights-based NGOs and some community groups, victim-aligned NGOs, industry groups, and government agencies. Differences can be explained in part by the fact that different sectors have different levels of knowledge about how data is actually used and how this use is regulated. While some of this is inevitable, and some is tied to limitations on transparency, many research participants also expressed frustration with media reporting. However, our analysis reveals that different underlying attitudes to privacy may also explain differences of views between clusters.

Although the same differences in opinions existed in the UK as in Australia, the public process through which the law has been changed (including the three reports leading up to the *Investigatory Powers Bill*) seemed to have narrowed the gap to some extent, or at least clarified the areas of disagreement. However, there remained some distrust between parts of the government and agencies, and the NGO community.

The views reflected in the Canadian sample were different from those in the Australian sample. In Canada rights-based NGOs and community groups, or victim-aligned NGOs were not interviewed. In Australia, differences could be explained in part by the fact that different sectors had different levels of knowledge about how data is actually used and how this use is regulated. In Canada, however, this distinction wasn't as apparent. This could be due to the fact that three out of the five policy research participants had previous roles in intelligence and law enforcement such that their views would have been formed from having seen the issues develop from different perspectives.

5.6.6 Resolving conflicts in values

Any conflict in values is unlikely to be fully resolved, particularly as it relates to underlying differences in attitudes towards privacy. However, research participants in Australia offered constructive suggestions about how conflicts can be reduced, including reducing the information gap between government agencies and the public, through dialogue among stakeholders and interested groups, an attempt to find the 'middle ground' between polarised views (although challenges here were acknowledged), and enhancing public trust in and trustworthiness of government agencies. Ultimately, as one research participant stated, legitimate conflict in a democracy is dealt with through elections; not everyone will change to a common view.

UK participants offered constructive suggestions for resolving value conflicts, for example, further conversations and dialogue, including public workshops, an ethical council or collective problem solving. In some circumstances it may be possible to conduct empirical testing as to matters of fact on which there is disagreement (such as the effectiveness of particular techniques) to the extent this can be done without compromising operational secrecy.

5.6.7 Sources of views

Research participants in Australia reported that they had formed their views based on professional experience, personal experience, contact with people with such experience, media and blogs as well as evidence and academic papers. Scepticism about media reporting

in this area, and the reliance on it by some research participants, likely underlines some of the divergence in their views.

Research participants in the UK formed their views based on similar sources to Australian participants. The recent reports leading up to and following release of the *Investigatory Powers Bill* were also important in the UK.

Research participants in Canada also relied on similar sources, but appeared to rely more on sources of information external to their professional or personal experience.

6. LEGAL ANALYSIS

6.1. Is access for data mining enabled?

Does the legal framework, subject to appropriate controls discussed in 6.2, enable access to relevant datasets in a manner that allows data mining? This question focused on collection, use and disclosure of data in relation to four types of data holdings: government-held data (information collected, use and disclosed by all levels of government in data systems), 'open source' data,[62] privately held data, and data held by foreign governments.

6.1.1 Australia

Government-held data may be subject to secrecy or confidentiality provisions in governing legislation that restrict or prevent access to the data. Restrictions may also apply to the use and disclosure of information collected coercively under statute.[63]

The *Privacy Act* and the Australian Privacy Principles (APPs) apply to personal information contained in government-held data unless an exception or exemption applies. The APPs establish a framework for the responsible collection and handling of personal information by Australian Government agencies and sections of the private sector in Australia. The APPs enable government agencies to collect personal information if it is reasonably necessary for or directly related to an agency's functions or activities. Personal information can be used and disclosed for the primary purpose of collection and a number of permitted secondary purposes. If a proposed use or disclosure is unrelated to the purpose of collection, it is not permitted. Key national security and law enforcement agencies are however not subject to the *Privacy Act* and APPs but subject to specific statutory provisions and/or privacy guidelines or rules.

In addition, the collection, use and disclosure of specific government-held data may also be governed by agency- or data-specific legislation as well as statutory or delegated authorisations, including those detailed in public and confidential Memorandums of Understanding (MOUs),[64] and by other general mechanisms such as rules or guidelines issued by the Privacy Commissioner for particular scenarios.

---

[62] The term 'open source' (originally meaning explicit licensing of free access to non-personal software 'source code') is used here to refer to information accessible publicly, including unrestricted online social media. There are a confusing and fluid range of access controls on Facebook, such that there is no obvious bright or stable line between what is 'public' for the world to see and what is intended to be more private interpersonal communication; because of this the intended status of much material is potentially uncertain. This category would also include user-generated content, such as those from NGO partners engaged in identifying human rights violations and other forms of offending, and citizen journalism for the same purpose. For a recent international example, see C Ribeiro (International Criminal Court), 'Innovation through partnership', presentation for Pearls in Policing conference, Copenhagen, June 2015; <http://www.pearlsinpolicing.com/wp-content/uploads/2014/07/Pearls-in-Policing-2015.pdf>.

[63] *Johns v ASC* (1993) 178 CLR 408.

[64] The current framework of Memorandums of Understanding developed with the support of the Australian Law Reform Commission *Review of Australian Privacy Law*, DP 72 (2008), Proposal 11-4.

(cont.)

To address the complexity, police services created CrimTrac as the national information sharing service for Australia's police, law enforcement and national security agencies.[65] CrimTrac is responsible for developing and maintaining national information-sharing services between state, territory and federal law enforcement agencies.[66] It operates not as a primary collection agency but rather as an intermediary facilitating national data disclosure and access arrangements for Australian police agencies, collecting information indirectly from them. In the context of its cooperative structure, the police agencies collectively determine what data should be disclosed to CrimTrac, the minimum set of data they will provide, and who is authorised to access or receive the data.[67] Police agencies either input information directly into CrimTrac systems, or upload it via automated system uploads.

Access to CrimTrac systems is restricted to authorised officials, such as police officers, who may access them for authorised purposes. CrimTrac has information sharing agreements with agencies known as Approved External Agencies. These include the ACC, Australian Securities and Investments Commission, NSW Independent Commission against Corruption, and QLD Crime and Misconduct Commission.

The Australian Crime Commission (ACC), Australia's national criminal intelligence agency, is another important example of an agency that facilitates information-sharing.[68] Its key functions include to collect, correlate, analyse and disseminate criminal information and intelligence, and to maintain a national database of that information and intelligence. The ACC may disclose information in its possession to Commonwealth, State or Territory bodies, foreign law enforcement, intelligence or security bodies as well as to international law enforcement, intelligence or judicial bodies, if the ACC's CEO considers it appropriate to do so; the ACC's CEO considers that the information is relevant to a permissible purpose; and the disclosure would not be contrary to Commonwealth, State or Territory law.[69]

Since 2010, the ACC has led a National Criminal Intelligence Fusion Capability that embodies a whole-of-government response to serious and organised crime. This enables the ACC, national intelligence agencies and law enforcement agencies to share information within projects and cooperate against serious and organised crime.[70]

---

[65] CrimTrac *Annual Report 2013-2014* 12. In addition all Australian police commissioners signed a Partnership Approach MOU in 2006. The MOU establishes a common understanding of the relationship between CrimTrac and each State and Territory police agency. CrimTrac's Board of Management comprises Australia's police commissioners, the ACT Chief Police Officer and a Deputy Secretary of the Attorney-General's Department.

[66] CrimTrac's services and capabilities include: police reference and information services; national fingerprint matching capability; national DNA matching capability; national child sex offender register; firearms and ballistic services; a cybercrime reporting system; and national police checks. CrimTrac has been expanding with the addition of services such as a missing person and victim system, and an online cybercrime reporting network. CrimTrac, Annual Report 2013–2014 11.

[67] CrimTrac, Information Publication Scheme, CrimTrac web site <https://www.crimtrac.gov.au/information-publication-scheme>.

[68] S 7A(a) Australian Crime Commission Act 2002 (Cth) ('ACC Act').

[69] *Australian Crime Commission Act 2002* (Cth) s 59AA.

[70] The ATO described the Fusion Centre and its involvement as follows in ATO *Submission to the Parliamentary Joint Committee on Law Enforcement Inquiry into the Gathering and Use of Criminal Intelligence* (13 August 2012) 3: '… [Th]e Fusion Centre was established in July 2010 to maximise the effective use of Commonwealth and other data holdings, and to facilitate intelligence sharing in relation to serious and organised crime. It is led by the ACC, and the ATO pursued the process to have the Fusion Centre prescribed as a taskforce pursuant to the Taxation Administration Act 1953 (TAA 1953). This was achieved in December 2011. This prescription allows the ATO to disclose protected information to the Fusion Centre. We have worked closely with the ACC to develop appropriate

(cont.)

In November 2015, the Minister for Justice announced that an agreement that will give effect to a merger was reached between CrimTrac and the ACC.[71] ACC is also in the process of merging with the Australian Institute of Criminology.[72] A new combined agency, the Australian Criminal Intelligence Commission, will operate from 1 July 2016. Legislation to effect these mergers was adopted by Parliament in May 2016.[73] CrimTrac and the ACC have their own access rules and share data with their own sets of partner agencies. The merger will consolidate the crime intelligence picture as far as these agencies are concerned but the pattern of unique access arrangements will still continue in relation to other agencies such as the ATO and national intelligence agencies.[74]

6.1.2 United Kingdom

Compared to Australia, UK intelligence and law enforcement agencies seem to enjoy more extensive access to a wide range of government-held data. The UK's Police National Computer (PNC), for example, is a computer system for police forces in the United Kingdom, owned by the Association of Chief Police Officers (ACPO) and managed and controlled by the Home Office.[75] Police forces and other law enforcement agencies, approved organisations and government departments, such as intelligence agencies and the Home Office, can access the system for specific purposes.[76] It holds criminal justice statistics, vehicle details (vehicle descriptions, ownership and insurance details) and details of people on the National Firearms Certificate Holders register.[77] The PNC supports a number of applications, such as:

---

governance processes in accordance with the law to allow for the effective sharing of tax information. We have provided the ACC with information and training to ensure that they are aware of the legal obligations in relation to use and disclosure of the information… ACC intelligence products are provided to the ATO either by email or safe hand delivery, depending upon the security classification of the product and its size.'

[71] Minister for Justice, 'New Super Agency to Tackle Emerging Threats' (Media release, 5 November 2015).

[72] See Australian Crime Commission Amendment (Criminology Research) Bill 2015, which includes a provision that disclosure of information collected for criminological research purposes can occur for a range of purposes modelled on the Privacy Act APP6. It appears the AIC function will otherwise be exempt from Privacy Act protections.

[73] See Australian Crime Commission Amendment (National Policing Information) Bill 2015; Australian Crime Commission (National Policing Information Charges) Bill 2015; and Australian Crime Commission Amendment (Criminology Research) 2015. See also Minister for Justice, 'Australian Criminal Intelligence Commission to Combat Criminal and National Security Threats' (Media release, 7 May 2016).

[74] The Parliamentary Joint Committee on Law Enforcement captured it as follows in the 2013 report on the gathering on use of criminal intelligence: 'Intelligence sharing currently takes place through a range of Memoranda of Understanding (MOUs), sharing agreements or requests for information between agencies. As these are primarily individual arrangements, they can create silos of information. The PFA (Police Federation of Australia) commented that such arrangements create an 'ad hoc system of information sharing that lacks consistency' and can hamper the speed of intelligence sharing. CrimTrac also noted that while different rules will always apply in different jurisdictions, law enforcement and intelligence agencies have also taken different approaches in relation to data collection.' See Parliamentary Joint Committee on Law Enforcement, *Inquiry into the gathering and use of criminal intelligence* (2013) [4.10].

[75] Home Office 'Guidance – Police National Computer (PNC)' (2014) 11.

[76] http://www.inbrief.co.uk/police/police-national-computer.htm.

[77] http://hub.unlock.org.uk/knowledgebase/criminal-record-databases-2/; Home Office 'Guidance – Police National Computer (PNC)' (2014) 5, 7-8.

(cont.)

- **QUEST** (Querying Using Enhanced or Extended Search Techniques), which enables users to search the names database and to identify suspects on the basis of partial physical descriptions and personal features.
- **VODS** (Vehicle Online Descriptive Search), which enables users to search for specific vehicles using criteria as registration, colour and postcode.
- **ANPR** (Automatic Number Plate Recognition), which is linked to an extensive CCTV camera network and enables identification of vehicles of interest based on visual images of a number plate, combined with other PNC data; and
- **CRIMELINK**, which enables crime and intelligence analysts to identify patterns and links in crimes across the UK.[78]

In addition to the PNC, the UK also maintains the Police National Database (PND)[79] which holds more background information relevant to crimes, rather than hard criminal justice data.[80] It holds, for example, police intelligence such as details of criminal investigations that did not lead to a conviction.[81]

Access to data includes access to non-clinical patient data on the National Health Service (NHS) to assist with the tracing of individuals for the purposes of law enforcement.[82]

While the PNC and PND provide central access to key crime and justice-related data, research participants indicated that a number of relevant databases are still held separately and needed to be accessed and interrogated individually.

6.1.3 Canada

Of the three countries, Canada appears to provide particularly broad NSLE access to government data. In Canada, access to government datasets, open datasets and privately-held data is allowed in the absence of a particular prohibition. In addition, sharing is promoted by the *Security of Canada Information Sharing Act 2015* (SCISA), which creates a framework to encourage information sharing and shields participating government agencies from civil liability. In particular, SCISA provides legal clarity, the purpose of which is to break down silos, foster information sharing and facilitate more effective operations in the national security space. While it permits and encourages information sharing, SCISA does

[78] http://www.inbrief.co.uk/police/police-national-computer.htm.
[79] The PND was rolled out as a result of the recommendations of the Bichard inquiry into child protection procedures in the Humberside Police and Cambridgeshire Constabulary. See the Bichard Inquiry Report HC653 (22 June 2004).
[80] http://www.information-age.com/technology/data-centre-and-it-infrastructure/1632588/police-national-database-launched#sthash.T1EAuPd5.dpuf.
[81] Jacqueline Beard and Sally Lipscombe The retention and disclosure of criminal records Briefing Paper CPB6441 House of Common Library, 12 August 2015, 4.
[82] Health and Social Care Information Centre Registers of approved data releases: Guide to tabs, column descriptions, key terms and abbreviations (2015) 10: 'The NBO's (National Back Office's) primary task is to ensure that demographic information on the Personal Demographics Service is accurate so that the NHS can use it for providing care. The NBO also provides strictly circumscribed non-clinical information to assist with the tracing of individuals for the purposes of law enforcement where certain criteria are met, including where the exemption under section 29(3) of the Data Protection Act applies or where it is compelled to do so by a court order.'

(cont.)

not mandate information sharing, not even between Canadian Security Intelligence Service, Communications Security Establishment and the Royal Canadian Mounted Police. [83]

6.1.4 'Open source' data, privately-held data and foreign agency data in Australia, the UK and Canada

'Open source' data[84]

None of the three countries have specific legislation regulating access to 'open source' information by federal or state NSLE agencies.[85] In Australia the application of the *Privacy Act* and APPs to the collection of such data for inclusion in a record, depends on whether the data concerned is classified as a "generally available publication".[86] Generally available publication is excluded from the definition of "record" in the *Privacy Act*. Key national security and law enforcement agencies are however not subject to the *Privacy Act.*

In the absence of the application of such provisions it appears such 'open source' data can be accessed, collected and shared.[87] The UK, for example, maintains various capabilities to access and mine social media for NSLE purposes.[88]

The absence of explicit statutory rules regulating access does not, however, imply that agencies enjoy unrestricted or unlimited access. Access to the repository at system level, or

---

[83] *Security of Canada Information Sharing Act*, S.C. 2015, c. 20, s. 5(1). Section 3 of the Act states that 'the purpose of this Act is to encourage and facilitate the sharing of information…'. Information disclosure as such is allowed 'in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption.'

[84] See 6.1 above.

[85] There is also no reference to 'social media' or 'social messaging' as a source for intelligence or law enforcement purposes in any Australian legislation. The reference to 'social media' in the data retention legislation is only by way of example, without further explanation.

[86] "Generally available publication" is defined in s 6 of the *Privacy Act* as "a magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public: (a) whether or not it is published in print, electronically or in any other form; and (b) whether or not it is available on the payment of a fee."

[87] Victoria Police have done a trial collating Facebook content, and have previously used software on a trial basis for collection of social media posts. It apparently only operates on the basis of collecting information from 'public' Facebook profiles. See Commissioner for Law Enforcement Data Security, *Social Media and Law Enforcement*, Victorian Government, July 2013 <https://www.cpdp.vic.gov.au/images/content/pdf/cleds_special_reports/CLEDS-Social-Media-and-Law-Enforcement-11-11.pdf>. While some data from open source is 'personal information', this may be affected by exceptions to the *Australian Privacy Principles*. The exception would apply where there appears to be informed consent to make a particular item public, such as a public Twitter feed; or where the person would 'reasonably expect' data to be disclosed or used for a purpose related to the one for which it was collected, such as a Facebook post, uploaded by a user on the understanding it is to be made accessible to, for instance, either all Facebook users, or a large subsection such as 'Friends of Friends'). *Privacy Act 1988* (Cth) s 16 exemptions from the APP's traditional data protection models did not explicitly address the selective disclosure model available under social networking tools, or the capacity for permanent global publication by individuals of their own and others' personal information, but a focus on the rights of individuals to retain and exercise control remains central. . Objections to extraterritorial access to 'open source' information by National Security Agency (US) through Facebook Ireland was the trigger for the European Court of Justice case of *Schrems v Irish Data Protection Commissioner* (case C-362/14).

[88] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 3.64.

(cont.)

to the non-'public' parts, may be subject to other rules, or to access by agreement with and at the discretion of the data host. Technological barriers and jurisdictional barriers may also apply.[89] Further, once 'open source' data is obtained, standard rules as to data retention and deletion may apply.

Privately-held data

A significant source of data for government agencies is data held by private corporations. Data sets in this category include for example financial data (with legislation compelling banks and other regulated institutions to report financial intelligence to national financial intelligence units) and telecommunications data. In general privately-held data may be acquired covertly and overtly and may even be purchased from companies and vendors and obtained from foreign counterparts.[90]

Telecommunications data (both 'traffic' and 'content') has long been accessible for law enforcement and national security purposes. In Australia the *Telecommunications (Interception and Access) Act 1979* (Cth) and *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) provide agencies the ability to access telecommunications data. The TIAA scheme differentiates between 'the content or substance' of a communication or document in online systems, and 'metadata' or 'telecommunications data' about that information or document.[91] Warrants are required where access to content is sought,[92] whereas 'authorisations for access to existing or prospective information' and orders to produce or supply information allow access to telecommunications data for certain purposes related to the performance of functions of the receiving entity (ASIO), or specified purposes (law enforcement agencies).[93]

Encryption of privately-held data may pose a barrier to access to the content of communications. The *Crimes Act 1914* (Cth) allows a law enforcement officer to search and seize electronic data held in Australia. Section 3LA of the *Crime Act 1914* (Cth) allows a

---

[89] Facebook's offshore data stores provide a useful example. In some cases, Facebook will give certain information to any recognised police officer in the jurisdiction. In others, police have to make a formal application through the Mutual Legal Assistance Treaty (MLAT) with the US. See *Mutual Assistance in Criminal Matters Act 1987* (Cth) ('MACM Act') <https://www.comlaw.gov.au/Series/C2004A03494>; Mutual Assistance in Criminal Matters (United States of America) Regulation 1999; Andrew K Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, Global Network Initiative, January 2015 <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf>. See also SMH 2010 <http://www.smh.com.au/technology/technology-news/facebook-hindering-the-police-20100525-wb8u.html>. In second half of 2014, Australian law enforcement made 900 requests for user data and were allowed access to 68% of those requests. Facebook Ireland Ltd, 'Australia Requests for Data,' *Government Request Report*, 2015 <https://govtrequests.facebook.com/country/Australia>; 'Facebook, Information for Law Enforcement Authorities,' (undated) https://www.facebook.com/safety/groups/law/guidelines/. See also the comment of one research participant at 7.2.3 (first paragraph).

[90] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 1.52.

[91] *Telecommunications (Interception and Access) Act 1979* (Cth) Part 4-1, Div 3, 4 and 4A for authorisations for disclosure to ASIO, 'criminal law enforcement agencies' and 'foreign law enforcement' respectively, and Div 5 permitting a use of such data by the disclosing person.

[92] *Telecommunications (Interception and Access) Act 1979* (Cth) Parts 2-2 and 2-5. Under section 6C of the TIAA for example there has to be 'a warrant issued on an application by an agency or an officer of an agency, or on an application by an eligible authority of a State.'

[93] *Telecommunications (Interception and Access) Act 1979* (Cth) Parts 4-1, ss 175 and 176 for ASIO, ss 178–180 for law enforcement agencies.

(cont.)

police officer to obtain a court order to compel a person to provide assistance to access data that is evidential material. Such assistance could extend to revealing encryption keys to enable police to obtain crucial evidence.

In the UK the *Intelligence Services Act 1994* and the *Security Service Act 1989* provide the legal basis for the acquisition of privately-held data. Specific provisions apply in relation to telecommunications information. The *Regulation of Investigatory Powers Act 2000* (**RIPA**) - to be amended by the *Investigatory Powers Bill 2016* - currently provides the legal basis for the lawful interception of communications, access to communications data, surveillance, the use of undercover agents and informers, and access to protected data. This Act responds to the privacy protection under the *Human Rights Act 1998* by setting out the grounds for justification for such intercepts. These grounds include national security interests, including safeguarding the economic well-being of the UK in circumstances relating to national security, and the prevention or detection of serious crime.[94]

RIPA distinguishes between communications data (metadata) and content. Officials within the organisation seeking access to communications data may authorise such access and may do so only for certain purposes.[95] A warrant issued by a Secretary of State is generally required to access content and the approval decision must be based on proportionality and necessity considerations.[96] RIPA also distinguishes between 'internal communications' (that are both sent and received in the UK) and 'external communications' (in which either the sender and/or recipient are outside the UK). Communications that are internal may only be intercepted under a warrant issued in terms of section 8(1) of RIPA. The warrants must name or describe the subject of the interception, as well as identifying factors that will be used to identify the communications to be intercepted.[97] External communications can be accessed by a warrant granted under section 8(4) of RIPA. Such a warrant does not need to name the subject of interception and does not need to impose a limit on the number of external communications which may be intercepted.

While section 8(1) warrants are primarily investigative tools, section 8(4) warrants are used for intelligence purposes to collect bulk data.[98] Section 8(1) has, however, also been interpreted in a manner that lends it to broader application.[99] It has been used to issue thematic warrants covering a group or network of persons.[100] The application of section 94 of the *Telecommunications Act* (directions in the interests of national security) to access bulk communications data has also been controversial. This section allows the Secretary of State, after consultation with a person to whom the section applies, 'to give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory

---

[94] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 4.17.
[95] RUSI par 4.23.
[96] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 4.18, 4.21.
[97] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 4.19.
[98] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 4.20.
[99] http://cyberleagle.blogspot.com.au/2015/08/the-coming-surveillance-debate-targeted.html.
[100] Intelligence and Security Committee of Parliament (ISC), Privacy and Security: A modern and transparent legal framework (2015) par 42-45. See also David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) par 14.63.

(cont.)

outside the United Kingdom.' Confidential directions were apparently issued that enabled agencies to access bulk data.[101]

The *Investigatory Powers Bill* does not dramatically increase access to data compared to current powers and practices. It modernises definitions and adds 'Internet Connection Records'[102] (a new record-keeping obligation), clarifies the range of available powers and subjects their exercise to a range of control measures, including a double-lock system of official approval and judicial review based on tests of necessity and proportionality.

Access to information by, and from, foreign governments

Australian law enforcement agencies can obtain access to data held by foreign agencies, and disclose to them, subject to control or supervision by the host government under mutual assistance provisions such as the 1999 *Mutual Legal Assistance Treaty*[103] (MLAT) between the United States and Australia. MLATs are a key measure enabling agencies like AFP to disclose information to and receive it from foreign counterparts. Agreements between governments sometimes treat data effectively as a form of currency. State and Territory police services also exchange information with foreign counterparts. One of the statutory functions of the AFP is to provide 'police services' and 'police support services' for the purposes of assisting, or cooperating with, an Australian or foreign law enforcement, intelligence, security or government regulatory agency.[104] These services have been interpreted as including information exchange.[105] State and Territory police services and the AFP are able to exchange domestically available information with foreign counterparts through the AFP's International Liaison Officer Network. This network has more than a 100 positions in 29 countries.[106]

The *Privacy Act* provides that an act or practice of an organisation done outside Australia does not breach the *Privacy Act* if it is required by an 'applicable law of a foreign country'.[107]

---

[101] In its 2014 report, the Interception of Communications Commissioner disclosed that he accepted a request from the prime minister to oversee section 94 directions. May, Report of the Interception of Communications Commissioner (March 2015) par 10.2. In the wake of litigation brought by Privacy International regarding the use of section 94 powers, it has gained access to redacted versions of formerly classified documents. These were released in early 2016 for purposes of the litigation and were published by Privacy International. See https://www.privacyinternational.org/node/854.

[102] Cl 54 of the Investigatory Powers Bill 2016 defines 'internet connection record' as communications data which (a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and (b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).' The new obligation has been criticised as potentially highly intrusive, costly and doomed to be unsuccessful, especially given that users may use a range of tools (Virtual Private Networks, The Onion Router etc) to evade logging meaningful records. House of Lords House of Commons Joint Committee on the Draft Investigatory Powers Bill Draft Investigatory Powers Bill Report HL 93 HC 651 (2016) par 89-156.

[103] This is in the Schedule of Mutual Assistance in Criminal Matters (United States of America) Regulations 1999. See also *Mutual Assistance in Criminal Matters Act 1987* <https://www.comlaw.gov.au/Series/C2004A03494>

[104] S 8(1)(bf) of the Australian Federal Police Act 1979.

[105] FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia – Mutual Evaluation Report* (2015) 191.

[106] See <http://www.afp.gov.au/policing/international-liaison/international-network>.

[107] *Privacy Act* 1988 (Cth) s 6A and 6B. Note that other broad exemptions will often also apply to law enforcement and security agencies.

(cont.)

In the absence of a law of a foreign country authorising the act or practice, there are protections in the *Privacy Act* for individuals whose information is disclosed overseas. APP 8 and section 16C of the *Privacy Act* create a framework for the cross-border disclosure of personal information. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and make the APP entity accountable if the overseas recipient mishandles the information. Similar to APP 6, there are exceptions contained in APP 8.2 that support the disclosure of information for enforcement-related activities. The *Privacy Act* however does not apply to key national security and law enforcement agencies.

Australia is also a party to the UKUSA Agreement (also known as the 'Five Eyes' agreement, after the intelligence alliance), pursuant to which the ASD is reported to be able to share data it collects about those who are not 'Australian persons' with its peer agencies in the United States, United Kingdom, Canada, and New Zealand.[108] That allows ASD and perhaps other agencies to disclose data to and receive data from partners. Intelligence agencies, for example, are empowered by provisions such as section 13 of the *Intelligence Services Act* to cooperate, subject to any arrangements made or directions given by the responsible Minister, with authorities of other countries approved by the Minister as being capable of assisting the agency in the performance of its functions. The ACC and Australian Federal Police jointly represent Australia in the Five Eyes Law Enforcement Group.[109]

Australia, however, lacks a clear, consistent and transparent legal framework regulating such information exchanges. The UK, which actively exchanges information with counterparts, similarly lacks such a framework. The Royal United Services Institute (**RUSI**) report stated that currently 'there is insufficient clarity over the powers and safeguards governing the exchange of data and intelligence between international partners.'[110] The report also noted that, as far as cross-border law enforcement is concerned, 'current legal-assistance processes are burdensome and, crucially, slow in comparison to the pace at which online threats can develop.'[111] The ISC report also expressed concerns regarding the lack of statutory underpinning for exchanges with foreign agencies.[112] The Investigatory Powers Bill 2016 aims to improve aspects of the current UK exchange regime, but the reforms are not fundamental.[113]

---

[108] A historical version of the UKUSA Agreement was released in 2010: National Archives, *Newly released GCHQ files: UKUSA Agreement*, June 2010 <http://www.nationalarchives.gov.uk/ukusa/>. See also Norton-Taylor, Richard, 'Not so secret: deal at the heart of UK-US intelligence', *The Guardian* (online), 25 June 2010 <http://www.guardian.co.uk/world/2010/jun/25/intelligence-deal-uk-us-released> and Privacy International, *Eyes Wide Open*, 26 November 2013 <https://www.privacyinternational.org/sites/default/files/Eyes Wide Open v1.pdf>.

[109] ACC <https://www.crimecommission.gov.au/5-capability-and-development> (now https://www.acic.gov.au/sites/g/files/net1491/f/2016/06/acc-ar-2014-15-chapter-5-capability-development_0.pdf?v=1467011889).

[110] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 5.75.

[111] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 5.77.

[112] Intelligence and Security Committee of Parliament (ISC), Privacy and Security: A modern and transparent legal framework (2015) par 241-242.

[113] See for examples cll 7 and 47 of *the Investigatory Powers Bill 2016*.

(cont.)

6.1.5 Observations

Australia has a complex framework of data collection, use and disclosure rules. In principle, law enforcement and intelligence agencies are able to access relevant open source data, unless jurisdictional or technical barriers apply. Different rules apply in relation to different types of privately-held data. In general, such data, for example telecommunications data, can be accessed under existing laws, when the applicable legal conditions are met. Specified financial data, on the other hand, must be disclosed to the government. The picture regarding access to government-held data is complex. This complexity stems from the federal structure of Australia, the nature of privacy protection in Australia, the incremental and fragmented development of legislative power; controls and exceptions to general principles, and technical factors relating to the format and design of different systems and databases.[114]

6.2. Are legal controls comprehensive and proportionate?

Having introduced some of the parameters around access to data for data mining and other Big Data purposes, the next section considers the key legal mechanisms that control access and other dealings with Big Data systems.

6.2.1 Australia

In Australia jurisdictional boundaries are particularly relevant in relation to laws on access and management of data sets, where the powers of Federal Parliament are subject to explicit or implied constitutional guarantees, and the common law principle of legality.

For instance, in the case of privacy, which is not a constitutionally recognised right in Australia, the *Privacy Act 1988* grants individuals certain protections against interference with their personal information. However as a general rule, the *Privacy Act* does not cover the acts and practices, records that originate with, or disclosures of personal information to the national intelligence agencies. These agencies will increasingly be major users of Big Data systems. To this end, they have developed their own regulatory codes for retention and communication of intelligence information. *Guidelines to Protect the Privacy of Australian Persons* (*Privacy Guidelines*) were adopted by the DIO and ONA and *Privacy Rules* were issued in accordance with s 15 of the *Intelligence Services Act* for ASIS, ASD and AGO. The *Privacy Guidelines* are broadly consistent with the *Privacy Rules*,[115] slightly adapted to the specific functions of each agency.

Furthermore, at the Commonwealth level, by virtue of *Human Rights (Parliamentary Scrutiny) Act 2011,*[116] regulations governing federal agencies that access, collect, use, store or disclose personal information obtained from third party data sets must be assessed for compatability with the rights and freedoms recognised in seven core international human rights treaties which Australia ratified, the *International Covenant on Civil and Political Rights* [ICCPR]. Article 17 of the ICCPR provides that 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, correspondence, nor to unlawful attacks on his honour and reputation.' Federal legislation that affects this right should thus

[114] See 5.2 earlier.

[115] S 15 of the *Intelligence Services Act 2001*.

[116] *Human Rights (Parliamentary Scrutiny) Act 2011*, s 3.

(cont.)

be both reasonably necessary and proportionate.[117] However, of itself, assessment of incompatibility with rights and freedoms by the Parliamentary Joint Committee on Human Rights[118] will not invalidate the relevant Bill or disallow the legislative instrument.

To further complicate the regulatory landscape governing distribution of information, foreign law enforcement agencies can obtain access to data hosted in Australia by the Federal agencies such as the Australian Federal Police, and vice versa, subject to control or supervision by the host government under mutual assistance provisions, and, where it applies, also the *Privacy Act*.[119] As noted above, Australia is also a party to the UKUSA Agreement (also known as the 'Five Eyes' agreement, after the intelligence alliance), pursuant to which the Australian Signals Directorate agency is reported to be able to share data it collects about those who are not 'Australian persons' with its peer agencies in the United States, United Kingdom, Canada, and New Zealand. An act or practice of an organisation done outside Australia does not breach the *Privacy Act 1988* (Cth) if it is required by an 'applicable law of a foreign country'.[120]

Proportionality to protect privacy

A range of proportionality factors are employed to protect privacy.[121] These factors feature in a range of different forms and formulations in relevant legislation, reflecting the different contexts in which privacy and other potentially relevant factors arise. The most common factor considered relevant is privacy, but other factors include the following:

---

[117] *Maloney v The Queen* [2013] HCA 28; *Betfair Pty Ltd v Western Australia* [2008] HCA 11; (2008) 234 CLR 418; *Thomas v Mowbray* [2007] HCA 33; (2007) 233 CLR 307. The Parliamentary Joint Committee on Human Rights and the High Court of Australia adopted the criteria of reasonable necessity (in the circumstance of the case) and proportionality as the test for determining whether interference with someone's privacy is 'unlawful' or 'arbitrary'. The proportionality test is also relevant to a range of constitutional controls and rules about data apart from privacy. For, the valid exercise of these constitutional powers is predicated on compliance with the common law principle of legality, the major rule of constitutional statutory construction. The principle of legality 'protects, within constitutional limits, commonly accepted 'rights' and 'freedoms', and its principal criterion is the test of proportionality. See *Saeed v Minister for Immigration and Citizenship* (2010) 241 CLR 252, 258–259 [11]–[15].

[118] See for example, the opinion of the Parliamentary Joint Committee on Human Rights as cited in the National Security Legislation Amendment Bill (no. 1) 2014, Explanatory Memorandum, [30]: 'Article 17 of the ICCPR provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence …The United Nations Human Rights Committee interpreted 'reasonableness' to imply that any limitation must be proportionate and necessary in the circumstances'.

[119] For example the 1999 *Mutual Legal Assistance Treaty* (Schedule of Mutual Assistance in Criminal Matters, United States of America, Regulations 1999; *Mutual Assistance in Criminal Matters Act 1987* (Cth)) between the United States and Australia. The Council of Europe *Convention on Cybercrime* (CETS No. 185) was ratified by Australia in 2012. Arts 23 and 25 of the Convention include expedited search, seizure and real-time interception of content. The terms of Convention also facilitate, or in some cases, require disclosure.

[120] S 6A and 6B of the *Privacy Act 1988* (Cth).

[121] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report No 108, 2008) 142 defined 'information privacy' [data protection] as consisting of 'rules governing the collection and handling of personal data such as credit information, and medical and government records', while 'privacy of communications … covers the security and privacy of mail, telephones, e-mail and other forms of communication'.

(cont.)

- The activity is 'necessary, and not beyond what is necessary, for the performance of a function of the agency'[122]
- The 'nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out'[123]
- '[T]he gravity of the conduct constituting the serious contravention'[124]

Proportionality factors also feature extensively in ASIO's *Attorney-General's Guidelines*.[125] Acknowledging that inherent in the performance of its functions is the risk of encroachment on personal freedoms and liberties, ASIO's *Attorney-General's Guidelines*[126] are more comprehensive than the *DIO Guidelines*, and, like the *ASIO Act 1979*, seek to achieve a 'balance between individual rights and the public's collective right to security'.[127] Elements of the proportionality test are woven into several control mechanisms, which are imposed at different levels of decision-making. The ASIO Director-General is, for example, responsible for determining who should be investigated by ASIO, and the investigative methods to be used. [128] The decision has to be made in accordance with considerations that include 'the immediacy and severity of the threat to security; the reliability of the sources of the relevant information; [and] … the investigative techniques that are likely to be most effective'.[129] In this instance, proportionality is employed at a high level of abstraction.

At the operational level, 'information is to be obtained by ASIO in a lawful, timely and efficient way,' and in accordance with the criterion of proportionality as condition for decision-making: 'any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence'.[130] Furthermore, once the decision to obtain the information is made, the proportionality test focuses on respect for the subject person's fundamental rights freedoms, albeit limited by consideration of national interest in security and safety of the public. Inquiries and investigations into individuals and groups should be undertaken:

> (i) using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions; and
>
> (ii) with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest;[131]

At the technical access level, the intrusive investigative techniques may include interception, non-consensual access to third party electronic data, data-mining and comparing data sets

---

[122] *Intelligence Services Act 2001* s 9(1)(a) and (b).
[123] *Intelligence Services Act 2001* s 9(1)(c).
[124] *Telecommunications (Interception and Access) Act 1979* s 116(2)(b). The variation in proportionality tests in the *Telecommunications (Interception and Access) Act 1979* (Cth) and other relevant legislation range from operational considerations when considering the privacy of a select few individuals to the potential intrusion of privacy at a higher level of consideration, such as determinations by the Attorney General for ensuring interception capabilities.
[125] *Attorney-General's Guidelines in relation to the performance by the ASIO of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence*, ASIO web site, undated <https://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf>.
[126] ASIO *Attorney-General's Guidelines* [6.2].
[127] See <http://www.asio.gov.au/About-ASIO/Legislation.html>.
[128] ASIO *Attorney-General's Guidelines* [7.1]; [9.1].
[129] ASIO *Attorney-General's Guidelines* [9.1].
[130] ASIO *Attorney-General's Guidelines* [10.4].
[131] ASIO *Attorney-General's Guidelines* [10.4].

(cont.)

about individuals.[132] The test is again conceptualised in terms of proportionality controls, however, it includes more detailed criteria than at the higher levels of decision-making. The focus is on assessment of concrete situations:

(a) the more intrusive the investigative technique, the higher the level of officer that should be required to approve its use;
(b) wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and
(c) where a threat is assessed as likely to develop quickly, a greater degree of intrusion may be justified.[133]

The ASIO guidelines therefore incorporate the control test of proportionality that is multi-layered and includes countervailing considerations, which focus on limiting the intrusion into personal information privacy, and respect for religious beliefs, and cultural values and 'sensitivities of individuals of particular cultural or racial backgrounds'.

However, the Guidelines are not legislative instruments. This weakens their legal standing and provides for amendments without the direct Parliamentary oversight. While these guidelines are balanced in relation to the rights of non-Australians, that is not the case in relation to the Privacy Guidelines applicable to other national intelligence agencies.[134] In addition it must be noted that guidelines containing privacy and proportionality test for analysts who examine data-sets for law enforcement and national security departments and agencies are not publically available. Yet, the decisions of analysts regarding examination of data may have profound legal, reputational and commercial implications for subjects of the assessment.

6.2.2 United Kingdom

The current legal regime regarding access to and retention, examination, exchange and deletion of private communications data is out-dated and lacking in public trust.

Under the current regime, metadata can be accessed on the strength of an authorisation issued by senior officials within the requesting agency while access to content data requires a warrant issued by a minister. Authorisation and warrants may only be issued if tests of lawfulness, necessity and proportionality are met, and processes may be inspected independent oversight bodies to ensure that appropriate tests were applied. While access controls are set to change under the *Investigatory Powers Bill* regime, the authorisation process will remain for less intrusive data access powers.

Warrants must comply with the *Human Rights Act 1998* (UK) and article 8 of the European Convention on Human Rights. Article enshrines the right of privacy. Article 8(2) provides:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the

---

[132] ASIO is not one of the Agencies involved in the data-matching under *Data-Matching Program (Assistance and Tax) Act 1990*, see below.
[133] ASIO *Attorney-General's Guidelines* [10.4].
[134] See for example, Defence Department, *Guidelines to Protect the Privacy of Australian Persons* <http://www.defence.gov.au/dio/privacy-rules.shtml> Approved by the Minister for Defence on 16 December 2012 after consultation with the Inspector-General of Intelligence and Security (IGIS) and the Attorney-General.

(cont.)

country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In relation to the present regime, the ISC described the relevant test as a 'triple test', essentially combining legality,[135] necessity[136] and proportionality.[137]

Little public information is generally available about the operational controls that apply to the *analysis* of data for purposes of national security and law enforcement. However, in March 2016, Privacy International[138] gained access to redacted versions of formerly classified documents.[139] Extracts of GCHQ's *Compliance Guide*, in force from June 2014 onwards, reflect training and guidance on the relevance of proportionality and necessity for purposes of analysis.[140]

The *Investigatory Powers Bill 2016* will improve control measures by increasing the clarity and consistency of control measures. Provisions of the *Investigatory Powers Bill* include statutory controls on and oversight over access to and gathering of communications and bulk/large sets of data, its use and management by nine law enforcement and national security and intelligence agencies. The Bill consolidates and streamlines safeguards previously contained in several statutes including *Regulation of Investigatory Powers Act*

---

[135] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) par 5.19-20: 'The first element of that test is that the interference must be '*in accordance with the law*'. In other words: (a) the interference must have some basis in domestic law; (b) the law must be sufficiently accessible: the rules must be reasonably easy to obtain and understand; and (c) the manner in which the law will operate or be applied must be sufficiently foreseeable. These requirements have not always proved easy to reconcile with the secret nature of electronic surveillance. A balance must be found between retaining the secrecy of operational tools and methods on the one hand, and, on the other, having a law that is '*sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities*' will access their communications.'

[136] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) par 5.20-5.22 described the challenges applying these tests to meet the interpretation of the European Court of Human Rights. See par 5.22: 'The second element of the test involves the identification of a *legitimate aim* whose pursuit is necessary. Article 8(2) … provides a broad list of interests that are capable of justifying interference. The courts are almost always willing to find that a legitimate aim is being pursued, for example, national security or the prevention of crime. '*Necessary*' means less than '*indispensable*', but more than merely '*admissible*' or '*useful*'. To be necessary, an interference must correspond to a '*pressing social need.*'

[137] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) par 5.22: 'To satisfy the third element of the test, the interference must be proportionate to the aim pursued. That is determined via a balancing exercise, which may for example require *'the interest of the … state in protecting its national security*' to be balanced against *'the seriousness of the interference with the applicant's right to respect for his private life*'. These elements, for example, encountered in section 7 of the Intelligence Services Act 1994 in relation to ministerial authorisation.

[138] The matter is before the Investigatory Powers Tribunal and focuses on the use by MI5, MI6 and GCHQ of s 94 powers. See https://www.privacyinternational.org/node/854.

[139] These were released for purposes of the litigation and were published by Privacy International. See https://privacyinternational.org/node/842.

[140] For example: 'The individuals whose communications you examine have a right to privacy, so your work must conform to the standards of HRA. Your queries and analysis must be necessary for an intelligence requirement and proportionate. You usually have to demonstrate this through a HRA justification that is logged for audit. If you are examining the content of individuals' communications, the standard of your HRA justification must be higher than if you are examining events data. No additional authorisation is needed for querying and examining events data.' See Extracts from GCHQ's Compliance Guide, in force from June 2014 onwards (March 2016) 1.

(cont.)

2000 (UK), *Police Act 1997* (UK), *Justice and Security Act 2013* (UK), *Counter-Terrorism and Security Act 2015* (UK), and *Data Retention and Investigatory Powers Act 2014* (UK). It also expands and re-shapes them. In particular, it deals with rules for data including large data-sets as templates to be adhered to by all agencies based not on the nature of the agency that has generated, gathered and manages them, but in accordance with the characteristics of the data-set in question (bulk, interference with equipment, etc.), and the nature of usage (access, sharing, retention, etc.)

At the heart of the proposed control system lies a new Investigatory Powers Commissioner and other Judicial Commissioners to be appointed under cl 194. For purposes of this discussion it suffices to note that appointees must hold a judicial position of at least senior or a High Court judge.[141] The Investigatory Powers Commissioner will replace the Interception of Communications Commissioner, the Chief Surveillance Commissioner and the Intelligence Services Commissioner.[142]

In future, the warrantry regime, the key control mechanism for the exercise of the most intrusive powers will operate on a double-lock system. This means that warrants must be authorised by the Secretary of State and approved by a Judicial Commissioner, who will in essence review the decision of the Secretary, among others by considering proportionality.[143] While targeted equipment interference warrants for intelligence agencies and Defence will be subject to the double-lock system described below; warrants for law enforcement will be issued by a Chief Constable and a Judicial Commissioner.[144]

Less intrusive access powers will only require authorisations rather than warrants. The *Investigatory Powers Bill* allows designated senior officer of a relevant public authority to issue a targeted authorisation empowering officers of authority to access communication data if it is considered necessary and proportionate.[145] The targeted access to communications data include 'filtering arrangements' established, controlled and maintained by the Secretary of State.

Controls are not limited to the double-lock system. Although the provisions of the *Investigatory Powers Bill* are intended for Agency personnel at the very high level of decision-making,[146] some analysts would also be covered by other control measures

---

[141] Appointments of Judicial Commissioners will be made by the Prime Minister after consultation with the Lord Chief Justice of England and Wales, the Lord President of Scotland, the Lord Chief Justice of Northern Ireland, the Scottish Ministers, and the First Minister and deputy First Minister in Northern Ireland.

[142] See also 6.6.2 below.

[143] See for example cl 18 and 21 of the *Investigatory Powers Bill 2016.*.

[144] Cl 96 of the Investigatory Powers Bill 2016.

[145] Cl 53 of the Investigatory Powers Bill 2016.

[146] Clause 16 'Persons who may apply for issue of a warrant

(1) Each of the following is an 'intercepting authority' for the purposes of this Part—
- (a) a person who is the head of an intelligence service;
- (b) the Director General of the National Crime Agency; (c) the Commissioner of Police of the Metropolis;
- (d) the Chief Constable of the Police Service of Northern Ireland;
- (e) the chief constable of the Police Service of Scotland;
- (f) the Commissioners for Her Majesty's Revenue and Customs;
- (g) the Chief of Defence Intelligence;
- (h) a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.'

(cont.)

including those in the form of safeguards relating to retention and disclosure that attach to the interception of communication data,[147] equipment interference warrants. In these cases,[148] the 'the issuing authority' must ensure, in relation to each targeted interception warrant, mutual assistance warrant, or targeted equipment interference warrant that:

> arrangements are in force for securing … in relation to the material obtained under a warrant ... [that] each of the following is limited to the minimum that is necessary for the authorised purposes: (a) the number of persons to whom any of the material is disclosed or otherwise made available; (b) the extent to which any of the material is disclosed or otherwise made available; (c) the extent to which any of the material is copied; (d) the number of copies that are made.

Essentially the same controls apply to bulk interception warrants,[149] bulk acquisition warrants,[150] bulk equipment interference warrants,[151] and bulk personal dataset warrants;[152] however, in these cases, the Secretary of State is under duty to ensure that appropriate arrangements are in place. As a general rule, every copy made of any of the material acquired under warrant must be destroyed 'as soon as there are no longer any relevant grounds for retaining it'.[153]

Supplementary controls provide safeguards for examination of the intercepted content and secondary data obtained under bulk interception warrants,[154] bulk acquisition warrants,[155] bulk equipment interference warrants[156] and bulk personal dataset warrants[157] by mandating that:

(a) any selection of data, the intercepted content, secondary data, bulk personal datasets, for examination by humans is carried out only for the specified purposes;
(b) the selection of any of the data for examination is necessary and proportionate in all the circumstances, and

---

[147] Cl 46 and 47 of the Investigatory Powers Bill 2016 provide safeguards relating to disclosure of material overseas.
[148] Cl 112 and 113 of the Investigatory Powers Bill 2016 provide safeguards relating to disclosure of material or data overseas.
[149] Cl 132 and 133 of the Investigatory Powers Bill 2016 provide safeguards relating to disclosure of material overseas.
[150] Cl 150 and 151 of the Investigatory Powers Bill 2016 provide safeguards relating to disclosure of material overseas.
[151] Cl 168 and 169 of the Investigatory Powers Bill 2016 provide safeguards relating to disclosure of material overseas.
[152] Cl 191 and 192 of the Investigatory Powers Bill 2016 provide safeguards relating to disclosure of material overseas.
[153] In the case of bulk interception warrants, 'intercepted content or secondary data'.
[154] Cl 134 of the Investigatory Powers Bill 2016.
[155] Cl 151 of the Investigatory Powers Bill 2016.
[156] Cl 170 of the Investigatory Powers Bill 2016.
[157] Cl 191 of the Investigatory Powers Bill 2016: '(1) The Secretary of State must ensure, in relation to every class BPD warrant or specific BPD warrant which authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, that—(a) any selection of data contained in the datasets (or dataset) for examination is carried out only for the specified purposes, and (b) the selection of any such data for examination is necessary and proportionate in all the circumstances. (2) The selection of data contained in bulk personal datasets for examination is carried out only for the specified purposes if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 183.'

(cont.)

(c) the selection of any of the intercepted content for examination meets any of the [statutory] selection conditions.

Another form of control involves duty not to make unauthorised disclosures. This duty is imposed in relation to interception,[158] equipment interference warrants,[159] bulk interception warrants,[160] and bulk equipment interference warrants.[161]

The Bill furthermore enhances oversight and transparency to improve public trust in the operation of the system.

While there is broad political support for the Bill debates and pressure to compel the government to strengthen privacy protections in the Bill and to revisit bulk data collection provisions, continued when this Report was concluded.[162]

6.2.3 Canada

A range of constitutional controls and rules about data arise from Canada's Constitutional framework, most notably in the form of case law based on the Canadian *Charter of Human Rights and Freedoms*. In contrast to Australia and the United Kingdom, there is a lack of articulated legislative control measures in Canada for Federal agencies' use of data with the exception of information sharing between agencies involved with security threats[163]. Key control measures are generally in the form of agency internal guidelines and by Memoranda of Understanding.[164]

---

[158] Cl 49 of the Investigatory Powers Bill 2016 imposes a duty not to make unauthorised disclosures on '(a) any person who is an intercepting authority (see section 16); (b) any person holding office under the Crown; (c) any person employed by, or for the purposes of, a police force; (d) any postal operator or telecommunications operator; (e) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator; (f) any person to whom any of the matters within subsection (4) have been disclosed in relation to a warrant.'

[159] Cl 114 of the Investigatory Powers Bill 2016 imposes a duty not to make unauthorised disclosures on ' (a) any person who may apply for a warrant…; (b) any person holding office under the Crown; (c) any person employed by, or for the purposes of, a police force; (d) any telecommunications operator; (e) any person employed or engaged for the purposes of any business of a telecommunications operator; (f) any person to whom any of the matters within subsection (4) have been disclosed in relation to [equipment interference] warrant'.

[160] Cl 136(2) of the Investigatory Powers Bill 2016: 'Sections 49 to 51 (duty not to make unauthorised disclosures) apply in relation to bulk interception warrants as they apply in relation to targeted interception warrants, but as if the reference in section 50(2)(c) to a requirement for disclosure imposed by virtue of section 34(5) were a reference to such a requirement imposed by virtue of section 131(4)'

[161] Cl 172 of the Investigatory Powers Bill 2016: 'Sections 114 to 116 (duty not to make unauthorised disclosures) apply in relation to bulk equipment interference warrants as they apply in relation to targeted equipment interference warrants, but as if the reference in section 115(2)(c) to a requirement for disclosure imposed by virtue of section 109(4) were a reference to such a requirement imposed by virtue of section 167(4)'.

[162] House of Lords and the House of Commons Joint Committee on Human Rights *Report on the Legislative Scrutiny: Investigatory Powers Bill* (2016) http://www.publications.parliament.uk/pa/jt201617/jtselect/jtrights/104/10403.htm#_idTextAnchor000; Letter by Andy Burnham to Theresa May on the Investigatory Powers Bill, 26 May 2016.

[163] *Security of Canada Information Sharing Act* (S.C. 2015, c. 20, s. 2)

[164] These guidelines and memoranda of understanding are not publically available documents, and although the question was asked in the interviews to review any memoranda of understanding or internal guidelines, these were not provided.

(cont.)

The controls for law enforcement (but not intelligence agencies) are found in the case law of *Wakeling*[165], *Jarvis*[166] and *Spencer*[167]. The only control specified in these decisions is, however, that a warrant is required to access, use and disclose information if done in the course of an investigation leading to charges. This does not mean, however, that agencies are over-sharing data or abusing privileges; it simply means that legislative controls are minimal.

Law enforcement agencies also require a warrant to (1) access or intercept the content of private communications such as emails and texts which is explored below, and (2) to access stored communications such as those found in the cloud or on a device. The definition of 'private communication' is of interest. A private communication, as defined in Part VI, s. 183 of the *Criminal Code*, states:

> *private communication* means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it …

In Canada, the location of the intended recipient plays a role, but this is not defined strictly as someone or a device being physically located in Canada. 'Stored communications' as such is not a term that is used in the Canadian framework, and is not defined in the Criminal Code.

Interception warrants are granted by judges of a superior court (called a s. 96 court in Canada as they refer to section 96 of the Canadian Constitution allowing judges to be appointed to the provinces and federal courts) in confidential hearings. Similar to Australia, interception warrants require the applicant to outline a number of items including the facts giving rise to suspicion, the type of communication to be intercepted, names, number of instances, and so forth.[168] One item of difference involves notification that a suspect has been made the target of an interception. Section 196(1) of the *Criminal Code* requires that the target(s) of surveillance must be notified within 90 days once the warrant or authorisation has expired unless it is in the 'interests of justice' not to disclose the surveillance. In the latter circumstance (notably in cases of terrorism) the confidentiality element may be extended for up to three years under section 196(2).

The Canadian system differentiates between accessing communications stored on a device and accessing communications stored on a third party server such as an Internet Service Provider or cloud space. An interception warrant is required to access communications stored on a third party server, while an information search warrant is required pursuant to section 487 of the *Criminal Code* to access communications stored on a device.[169] This distinction, of course, makes little sense when communications are stored on a device and on a server but is, nonetheless, Canadian law at present. Search warrants and production orders (to preserve data) pursuant to section 487.02 do not refer to communications but to

---

[165] *Wakeling v. United States of America* [2014] 3 SCR.

[166] *R. v. Jarvis*, [2002] 3 SCR 757.

[167] *R. v. Spencer*, [2014] 2 SCR 212.

[168] *Criminal Code*, R.S.C. 1985, c. C-46, s. 184(3).

[169] The type of required warrant for the RCMP to use was contested in the Supreme Court in *R v Telus* (2013) SCC 16.

data. This differentiation is confusing in that it does not distinguish between mere data (computer data, transmission data, tracking data) and the content of private communications.

Intelligence agencies are not bound by the same controls for data collection, use and interception.

The courts have taken a consistent approach to the use, access and control of data when used in the course of an investigation [170]. Absent a warrant or appropriate judicial authority, data accessed, used, sharing and disclosed would be seen to be a violation of sections 7 and 8 of the *Charter*. The section 1 Charter test (Oake's test [171]) requires that all restraints on rights and freedom be justified in a democratic society. This in turn requires that measures be reasonable, proportionate and necessary.

The notion of reasonable, proportionate and necessary is generally expressed in some legislation[172], as well as Memorandums of Understanding, Guidelines and Directives. Other legislation directly refers to the Charter. There are no guidelines or directives, however, that discuss the meaning of 'reasonable and proportionate' in the context of Big Data.

6.2.4 Observations

Controls on communication of intelligence information about persons, and collecting, accessing or disclosing information for intelligence purposes are necessarily complex, given Australia's federal structure. These controls create a matrix of overlapping requirements that apply to different organisations in different ways.

A number of provisions contained in national security and law enforcement legislation and guidelines require the decision-maker to consider whether the measures or actions to be adopted for access, collection, and dealings with third party data are *proportionate* in the sense of being 'reasonably necessary' for the stated statutory purpose. In relation to privacy, ASIO's *Attorney-General's Guidelines*, for example, contain a range of proportionality controls. There are however inconsistencies in both the presence and content of proportionality provisions for controls on access, use and other functions. In some cases there is no explicit requirement to apply any proportionality test and, where a proportionality test is present, the factors required to be considered may vary, or not be explicit. Similar concerns arise in relation to the regulatory codes for retention and communication of intelligence information developed by several intelligence Agencies.

Some of the variation observed in the proportionality tests in the relevant laws may be related to the unavoidable reality of legislative adaptation to varying ends, or the difference between high level determinations and the more operational authorisations and warrants. Nevertheless, the inconsistency and uncertainty increase the complexity of the law and decrease confidence that correct decisions are taken and that all available powers are exercised when required.

The Australian control measures largely resemble the current UK framework. The improvement of the clarity and consistency of the UK control measures and processes envisaged in the *Investigatory Powers Bill 2016* is likely to simplify the framework and

---

[170] See *Wakeling v. United States of America* [2014] 3 SCR; *R. v. Jarvis*, [2002] 3 SCR 757; *R. v. Spencer*, [2014] 2 SCR 212.

[171] *R v David Edwin Oakes* [1986] 1 S.C.R. 103.

[172] Reasonable and proportionate is a dominant principle as espoused in section 1 of the *Charter of Human Rights and Freedoms 1982*. These terms are also mentioned in the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23, s 12.1(2).

strengthen public support for the data powers of NSLE agencies. This approach to control measures may provide a useful model for Australia. The Canadian model on the other hand would appear less relevant to Australian policymakers. In contrast to Australia and the United Kingdom, Canada does not regulate the use of data by Federal agencies closely. It relies in essence on a range of constitutional controls and principles about data that arise from Canada's Constitutional framework and Bill of Rights, especially from case law based on the Canadian *Charter of Human Rights and Freedoms*.

6.3. Are legal rules clear, principle-based, consistent and instructive?

The Australian access and control framework as described in 6.1 and 6.2 is complex. This study was unable to ascertain whether the laws and regulations are sufficiently clear to provide officials with appropriate guidance. In particular, much of the guidance on the application of laws is contained in confidential internal policies and manuals that the researchers could not review.

Compliance audits done by the Inspector-General of Intelligence and Security (IGIS) and other independent oversight bodies provide a measure of comfort that compliance levels are high.[173] By implication it would be reasonable to assume that the internal policies and operational rules are sufficiently clear and instructive to prevent non-compliance. It is less clear whether they are sufficiently clear to enable officials to act confidently within the full scope of what the law allows. A number of research participants raised concerns regarding different interpretations of the law, especially where it impacts on access to and sharing of data.[174] Differing interpretations indicate that some aspects of the legal rules could be expressed more clearly. Some research participants also called for rules to be based on consistent principles or policy.

A general obstacle to clarity and consistency is the inconsistent use of terminology. In particular,[175] there are diverse meanings ascribed to concepts such as 'data', 'information', 'communication/electronic communication', 'document', and 'record' in various Australian Acts.

In the UK, legal clarity was rated as very important by all three 2015 reports (by the ISC, RUSI, and Anderson) and its absence noted in relation to the current, that it the pre-*Investigatory Powers Bill* regime.[176] Statutory terminology was also identified as problematic. In relation to RIPA for example it was observed that important concepts such as 'content' were not defined[177] and the definitions of terms such as 'communications' (especially 'external communications', and internal communications'),[178] and 'subscriber data' were anachronistic and counter-intuitive.[179]

---

[173] See section 3.6 below.
[174] See 7.2.
[175] Danuta Mendelson et al, 'The Absence of Clarity', forthcoming.
[176] ISC, Privacy and Security: A Modern and Transparent Legal Framework (March 2015) par xvi; RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 5.24; David Anderson, A Question of Trust: Report of the Investigatory Powers Review (2015) par 12.19-20.
[177] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) par 12.20.
[178] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) par 12.25.
[179] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) par 12.20.

(cont.)

Confusion is compounded by the fact that many rules in the legislation and accompanying Codes of Practice are insufficiently detailed.[180] Internal legal interpretations of the *Regulation of Investigatory Powers Act 2000* also play an important role. The fact that agencies interpreted section 8 of this Act to allow for the issuing of thematic warrants was, for example, not publicly known until this interpretation was first avowed in the Intelligence and Security Committee's *Privacy and Security* report in March 2015.[181] What the public had believed was the clear meaning of section 8 was thus less clear than supposed.

The *Investigatory Powers Bill* was drafted with the objective to clarify the law. The drafters aimed to improved terminology and to promote consistency of rules and procedures.[182]

Canada illustrates why clarity and consistency should not be viewed in isolation in this context. The principles elaborated in the *Privacy Act 1985,* for example, are clear and principle-based but are so out of date as to render them of limited value when applied to Big Data and any technology developed post-1983, including the Internet. Treasury Board documents in the form of guidelines and directives relevant to the space are equally clear, principle-based and are additionally quite flexible. Government agencies are free to adopt principles as best suits their organisation. Unfortunately, however, 'clear and principle-based' does not necessarily equal 'adequate'. The flexibility in these Guidelines and Directives often means that best practices are not necessarily pursued. Principles-based drafting also assumes that agencies will be able to keep on top of emerging issues, and alter their practices in accordance with the principles.

6.3.1 Observations

While perfect clarity, consistency or longevity of rules is not possible, there are improvements that can be made. Legislation, rules and guidelines should ideally use consistent and terminology, particularly as to basic terms such as 'data', 'information', 'communication', 'electronic communication', 'document', and 'record'. Consistency and clarity of control measures and processes (see 6.2.4) will also be of value. In general, a focus on principles (as in privacy) and standards (as in information security) would be helpful to support greater consistency while maintaining flexibility across contexts.

That said, the subject matter is complex, requiring sophisticated rules. Challenges to simplify rules are increased by the pace of technological developments and by institutional and agency needs for compliance clarity. Where rules are overly complicated, however, public understanding and trust is difficult to secure and agencies may not be able to use the full scope of law that the drafters actually intended.

---

[180] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) par 12.20. RUSI commented that the lack of clarity extends to the powers and safeguards governing the exchange of data and intelligence between international partners. See RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 5.75.

[181] ISC, Privacy and Security: A Modern and Transparent Legal Framework (March 2015) par 42-45; David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) par 6.42. See also Anderson par 7.69: 'The use by the security and intelligence agencies of bulk personal datasets was publicly avowed only on 12 March 2015 when the ISC published its report. I had already been extensively briefed on their use at all three agencies, and was also aware that the ISCommr has, for several years, been reviewing the use of bulk personal datasets as part of his duties.'

[182] Draft Investigatory Powers Bill CM 9152 (November 2015) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf.

(cont.)

6.4. Is integrity of data and systems supported?

Data integrity and measures to ensure integrity are important factors impacting on user confidence in the system and the quality of products, as well as on public trust.

Integrity and security are closely related but separate matters. This discussion focuses on the integrity of data while the data security aspects are considered in 6.5.[183]

6.4.1 Australia

In Australia government entities are compelled by a range of laws and policies to ensure data integrity.

- **General management laws** such as the *Public Governance, Performance and Accountability Act 2013* and general management principles require agencies to ensure that the data they collect and retain are correct. Incorrect and incomplete data poses risks to their effective and efficient management and administration of their functions.
- **Privacy laws** such as the *Privacy Act 1988* include concrete formulations of principles governing data integrity many of which are well-entrenched globally.[184]
- **Agency or function-specific laws**, such as the *Intelligence Services Act 2001* (Cth) may also contain provisions relevant to data integrity.[185]
- **Government policy** and standards, such as the *Australian Government Big Data Strategy* also address data integrity.[186]

While various legal rules and principles address data integrity, analysis of legal rules is not closely regulated. Australian intelligence analysts use the Admiralty code to support the integrity of their intelligence analysis.[187] Depending on the analysis required, structured

---

[183] Integrity of government data can be compromised in different ways. For instance, see Australian National Audit Office, *2005–2006 Audit Report No.29: Integrity of Electronic Customer Records* (2006) <http://www.anao.gov.au/Publications/Audit-Reports/2005-2006/Integrity-of-Electronic-Customer-Records>; or Australian National Audit Office, *Integrity of Medicare Customer Data: Department of Human Services* (2014) <http://www.anao.gov.au/Publications/Audit-Reports/2013-2014/Integrity-of-Medicare-Customer-Data>.

[184] Inspector-General of Intelligence and Security (Dr Vivienne Thom), Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority and related matters, December 2011, 4. Australian Privacy Principle 10 (Quality of Personal Information), for example, addresses data integrity as follows: '10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.'

[185] S 3 of the *Intelligence Services Act 2001* (Cth) defines 'operational security of ASIS' as meaning the protection of the integrity of operations undertaken by ASIS from (a) interference by a foreign person or entity; or (b) reliance on inaccurate or false information.

[186] Principle 3 (data integrity and the transparency of processes) embeds the notion of integrity as a feature of the project, its governance and of the data *per se.* See *Big Data Strategy - Improved Understanding through Enhanced Data-Analytics Capability* (2013) 21 <http://www.finance.gov.au/big-data>.

[187] The Code is an intelligence assessment tool that reflects the source of the information (on a scale of A-F, with A assigned when it is completely reliable) and the accuracy of the information (on a scale of 1-6 with 1 assigned where the report was confirmed.) See John Joseph and Jeff Corkill Information evaluation: how one group of intelligence analysts go about the task Proceedings of the 4th Australian

(cont.)

analytic techniques such as key assumptions checks, structured brainstorming, assessment of cause and effect, timeline and chronology analysis, and link network analysis may also be employed.[188] The researchers, however, could not locate public evidence of specific rules in Australia relating to integrity assurance and the employment of, or reliance on, automated data mining algorithms.[189]

6.4.2 United Kingdom

The UK's has a range of rules focused on data accuracy. The *Data Protection Act 1998*, for example, sets out eight principles of 'good information handling', the fourth of which addresses data accuracy: 'Personal data shall be accurate and, where necessary, kept up to date.'[190] This accuracy principle finds application in different ways, including for example in the *Code of Practice on the Management of Police Information*,[191] issued under the *Police Act 1996.*[192] All police staff members are furthermore required to apply data quality principles to all police information,[193] ensuring that it is accurate, adequate, relevant and timely.

The *Investigatory Powers Bill* contains provisions and processes regulating the examination of datasets. Clause 151 (Safeguards relating to examination of data) for example requires the selection of communications data obtained under a warrant to be carried out only for the operational purposes specified in the warrant at the time of the selection. The selection of any of the data for examination must furthermore be necessary and proportionate in all the circumstances. The definition of examination in clause 225(7) of *Investigatory Powers Bill* restricts the concept to human examination of the data.[194]

Submissions to the Joint Parliamentary Committee on the draft *Investigatory Powers Bill*[195] pointed to the need to mitigate risks that may accompany automated analysis.[196] The Bill

---

Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 5th–7th December <2011 http://ro.ecu.edu.au/asi/20>.

[188] Parliamentary Joint Committee on Law Enforcement. '*Examination on the Australian Crime Commission Annual Report 2011–12*', 15 March 2013 <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Annual_Reports/2013/ACC/hearings/~/media/Committees/Senate/committee/le_ctte/annual/2013/ACC/hearings/ACC_AR_2011-12_Qon_1-21.ashx>.

[189] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (2015) 14.43.

[190] Data Protection Act 1998, Schedule 1, Part 1.

[191] Home Office, Code of Practice on the Management of Police Information (2005).

[192] See for example Home Office, Code of Practice on the Management of Police Information (2005): '4.3.2 Where appropriate and in accordance with guidance to be issued under this Code, the source of the information, the nature of the source, any assessment of the reliability of the source, and any necessary restrictions on the use to be made of the information should be recorded to permit later review, reassessment and audit'; '4.3.3 Information should be assessed for reliability in accordance with guidance to be issued under this Code.'

[193] College of Policing, *Common process for managing police information* (2013) [Internet]. https://www.app.college.police.uk/app-content/information-management/management-of-police-information/common-process/ [Accessed 17 February 2016]. Information must be accurate, adequate, relevant and timely.

[194] Cl 225(7) of *Investigatory Powers Bill 2016*: 'References in this Act to the examination of material obtained under a warrant are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.'

[195] House of Lords House of Commons Joint Committee on the Draft Investigatory Powers Bill Draft Investigatory Powers Bill Report HL 93 HC 651 (2016).

[196] Paul Bernal, for example, argued that the automated processing required to facilitate such big data analysis comes with additional risks: 'Further vulnerabilities arise at the automated analysis stage:

(cont.)

however does not regulate the automated analysis of the relevant data explicitly[197] and it will fall to the new Investigatory Powers Commissioner to 'scrutinise the automated analysis of bulk datasets conducted by the security and intelligence agencies to ensure that they are conducted appropriately and proportionately and with regard to privacy and data protection requirements.'[198]

The approach to automated analysis can be contrasted to the protection afforded to customers of private companies where a decision affecting that individual if is informed by automated analysis. Section 12 of the Data Protection Act 1998 for example requires a data controller which bases a decision which significantly affects an individual solely on such processing, to notify the individual that the decision was taken on that basis. An individual may also file a notice on a data controller to prevent that controller from taking a decision affecting that individual if is informed by automated analysis. It is also at odds with the approach to automated decisions in the 2016 *Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences (also known as the 'EU-US Umbrella Agreement'*). *Article 15* requires that decisions producing significant adverse actions concerning the relevant interests of an individual may not be *based solely on the automated processing of personal information without human involvement, unless authorised by domestic law, and appropriate safeguards apply, including the possibility to obtain human intervention.*

6.4.3 Canada

While data integrity is the subject of a range of policies, laws and principles, it is not comprehensively regulated in Canada. The Canadian *Privacy Act*, unlike its Australian and UK counterparts, does not set a general data accuracy or integrity standard. The Treasury Board does, however, have several Guidelines and Directives relevant to data integrity and decision-making. There are many specific standards for types of data including metadata.

Principle 6 of the *Personal Information Protection and Electronic Documents Act 2000,* applying to the private sector, requires that personal information 'shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is used.' This Act does not bind law enforcement and intelligence agencies but it does extend to private organisations such as Canada Post.[199] Enabling legislation such as the *National Defence Act*

---

decisions are made by the algorithms, particular in regard to filtering based on automated profiling. In the business context, services are tailored to individuals automatically based on this kind of filtering —Google, for example, has been providing automatically and personally tailored search results to all individuals since 2009, without the involvement of humans at any stage. Whether security and intelligence services or law enforcement use this kind of a method is not clear, but it would be rational for them to do so: this does mean, however, that more risks are involved and that more controls and oversight are needed at this level as well as at the point that human examination takes place.' House of Lords House of Commons Joint Committee on the Draft Investigatory Powers Bill Draft Investigatory Powers Bill Report HL 93 HC 651 (2016) par 338.

[197] Appropriate analysis is not a matter addressed by the draft Codes of Practice either. Where relevant, Codes rather focus on limiting access for purposes of examination to preserve privacy. See for example Security and Intelligence Agencies' retention and use of bulk personal Datasets Draft Code of Practice [Spring] 2016 par 7.5.

[198] House of Lords House of Commons Joint Committee on the Draft Investigatory Powers Bill Draft Investigatory Powers Bill Report HL 93 HC 651 (2016) par 703. Also see Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny Cm 9219 p 75-76.

[199] See *Personal Information Privacy and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1.

and the *Royal Canadian Mounted Police Act*, however, do not refer to reliability, accuracy, authenticity, integrity or security of data.

6.4.4 Observations

While a range of policies, laws and principles are relevant to data integrity and accuracy, it is not comprehensively regulated in Australia, the UK or Canada. As a lack of integrity undermines the usefulness of the data, this is often an aspect that would be addressed by operational measures and the lack of comprehensive regulation is therefore not surprising. Such regulation and a clear concept of 'data integrity' can however result in greater consistency in the application of methods to improve integrity and may support greater sharing of data among agencies.

The UK's proposed improvements to the examination of datasets increases transparency and consistency of the relevant rules. The restriction of the measures to human examination of data limits the value of the approach for Big Data systems. Appropriate safeguards to ensure the integrity of automated processing of data and automated decision-taking, such as those envisaged in the *EU-US Umbrella Agreement,* require closer attention.

6.5. Are data and systems protected?

How do current rules support the integrity of data collected, retained and accessed by government for law enforcement and national security purposes?

6.5.1 Australia

A range of statutory provisions govern security of data in Australia.[200] Some provisions promote data security. Law enforcement and national security agencies are, for example required by statute to keep secure data pertaining to Australians, and unauthorised access to their information is prohibited.[201]

[200] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report No 108, 2008) 142; ALRC, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123), 3 September 2014 <https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>. Individuals may not generally have an enforceable remedy in circumstances where there is unlawful or inappropriate access or use of that individual's data as a result of inadequate security. Determinations on *Privacy Act* 1988 complaints by the federal Privacy Commissioner are very rare, cannot be compelled to be made, and are not enforceable without separate action. Many actions by law enforcement or national security agencies would in any case fall outside the core jurisdiction, as discussed above. The basis of any such complaint would lie in a breach of APP 11 on personal information security; see Schedule 1.

[201] *ASIO Act* s 18 creates offences for 'communication of intelligence' without authority. *Intelligence Services Act 2001* (Cth) Part 6 Division 1 creates similar offence on a per agency basis. *Australian Federal Police Act 1979* (Cth) s 60A(2) creates a related offence.

(cont.)

- Secrecy provisions apply to individuals dealing with information held in a data system, for instance *Crimes Act 1914* (Cth) Part VII,[202] and particularly s 79 and s 91.1 of the *Criminal Code* covering espionage and similar activities.[203]
- A range of offences at Federal as well as State and Territory levels criminalise unauthorised access to computer data. At the Federal level the *Criminal Code,* for example, creates a number of such offences, the most serious of which is knowing, unauthorised access to data held in a computer with intent to use this access to facilitate a serious offence.[204] There are also relevant State and Territory equivalents of offences related to unauthorised access to computer data.[205] These offences target access to data, not the use of the accessed data.

Privacy Principles also support data security, for example Australian Privacy Principle 11 (Security of Personal Information).[206] Although the privacy rules issued by some national intelligence agencies are not as comprehensive as the *Australian Privacy Principles* model, they do require security to be addressed.[207] These requirements are however not prescriptive, and offer no benchmarks, standards or methods of confirmation of adequacy.

Key government strategies, policies and guidance such as the *Australian Cyber Security Strategy*[208] and the Australian Government's *Protective Security Policy Framework* also

---

[202] *Crimes Act 1914* (Cth) ('CA') <https://www.comlaw.gov.au/Series/C1914A00012>. S 79 Official Secrets creates a range of offences in subsections (2)–(6) relating to 'prescribed' items such as a 'sketch, plan, photograph, model, cipher, note, document, or article' and 'prescribed information.' The different offences are particularised by specifying the nature of the item or information, the circumstances of its creation or handling, expectations or authorisations about it, or the knowledge or intentions of the defendant. For items, offences cover actions such as communicating or permitting access, receiving, retaining, failing to comply with a direction about retention or disposal, or failing to take reasonable care or endangering the safety of the item. For 'prescribed information' which a person has it in his or her possession or control, s 79(1), the actions covered are communicating or permitting access, receiving, failing to take reasonable care or endangering its safety; but not retaining, or failing to comply with a direction about retention or disposal.

[203] *Criminal Code Act 1995* (Cth) ('CCA') <https://www.comlaw.gov.au/Series/C2004A04868>.

[204] CCA cl 477.1. The requirement for an association with a serious offence means this would not cover most unauthorised access.

[205] As noted, Commonwealth offences in this area apply on to protection of Commonwealth computers and computer systems [which potentially covers many relevant Big Data systems], and the commission of crimes by means of a telecommunications service [as access to data goes into 'the cloud', this is also increasingly broad in its effect on Big Data use for law enforcement and national security: AGD, Supplementary Submission 44.2, 10, House Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime,* 104, 21 June 2010. NSW computer offences covering other scenarios are found in *Crimes Act 1900* (NSW), particularly s 308C Unauthorised access, modification or impairment with intent to commit serious indictable offence. In Victoria, s 247B *Crimes Act 1957* (Vic) covers similar ground.

[206] *Privacy Act 1988* (Cth) Schedule 1: '11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss; and from unauthorised access, modification or disclosure.'

[207] See for example: '2.2 Where ASIS does retain intelligence information concerning an Australian person, ASIS is to ensure that: a. the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; …'. ASIS, *Privacy Rules,* 2012 <https://www.asis.gov.au/Privacy-rules.html>; see Technical Reference 4.

[208] See <http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx>.

(cont.)

strengthen data security[209] The *Framework* is complemented by the Australian Government *Information Security Manual* which, sets security standards for government ICT systems. Published by the Australian Signals Directorate, it aims to assist Australian government agencies in applying a risk-based approach to protecting their information and ICT systems that is specific to their unique environments, circumstances and risk appetites.[210] A series Cyber Security Operations Centre (CSOC) *Protect Notices* issued by the Australian Signals Directorate set out security considerations[211] for agencies seeking to use cloud based resources, the most recent from the perspective of 'tenants' and cloud service providers.[212]

There are also relevant provisions at the State and Territory level in Australian. Binding data security and integrity standards were, for example, issued to Victoria Police in 2007 under the *Commissioner for Law Enforcement Data Security Act 2005* (Vic) (CLEDS Act). The *CLEDS Standards* impose security and data integrity obligations on Victoria Police in relation to law enforcement data. This system was reformed by the *Privacy and Data Protection Act 2014 (Vic*), which compels the Victorian Commissioner for Privacy and Data Protection to develop the Victorian protective data security framework for monitoring and assuring the security of public sector data.[213]

6.5.2 United Kingdom

The UK's statutory data security framework resembles the Australian framework. It has a range of laws that criminalise data-related offences, complemented by sound data security principles.[214]

---

[209] The *Framework* addresses appropriate governance, personnel security, physical security and also information security. A 2014 *Directive on the Security of Government Business* directs agency heads to apply the *Protective Security Policy Framework* (PSPF) and to promote protective security as part of their agency's culture. See <https://www.protectivesecurity.gov.au/ExecutiveGuidance/Pages/Directive-on-the-security-of-Government-business.aspx>. Agencies are required to appropriately safeguard all official information to protect its confidentiality, integrity, and availability. In particular, they must ensure that only authorised people access information through approved processes; that information is only used for its official purpose, retains its content integrity and is available to satisfy operational requirements; and that information is classified and labelled as required. *Australian Government Securing Government Business - Protective security guidance for executives* (2014 as amended in April 2015) [2.3].

[210] The ISM, in turn, references other standards, such as risk management standards and information security standards issued by Standards Australia and the International Organisation for Standardization (e.g. Australian Standards HB 167: 2006 *Security risk management* and HB 327:2010 *Communicating and consulting about risk* and ISO/IEC 27000:2009, *Information technology—Security techniques— Information security management systems—Overview and vocabulary* and the related ISO/IEC 27000 standards mentioned below.) See *Information Security Manual* <http://www.asd.gov.au/infosec/ism/>.

[211] Department of Defence, Australian Signals Directorate, CSOC Protect Notice, *Cloud Computing Security Considerations*, September 2012.

[212] Department of Defence, Australian Signals Directorate, *Cloud Computing Security for Tenants*, April 2015 <http://www.asd.gov.au/publications/protect/cloud-security-tenants.htm>; DoD, ASD, *Cloud Computing Security for Cloud Service Providers*, April 2015 <http://www.asd.gov.au/publications/protect/cloud-security-providers.htm>.

[213] *Privacy and Data Protection Act 2014 (Vic)* s 85(1).

[214] For example the *Computer Misuse Act 1990* criminalises unauthorised access to computer material (s 1), unauthorised access with intent to commit or facilitate commission of further offences (s 2); and unauthorised modification of computer material (s 3). The *Communications Act 2003* also creates

(cont.)

The UK's good information handling principles set out in the *Data Protection Act 1998*, for example, includes Principle 7 which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.[215] Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate:

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected.[216]

As far as government data is concerned, data security is also protected by the UK Government Security Classification system that came into effect in 2014.[217] The new system simplifies the previous categories (top secret, secret, confidential, restricted, protect and unclassified) by providing for three classifications (top secret, secret and official).[218] The classification system applies to all information that the UK government collects, stores, processes, generates or that it shares to deliver services and conduct its business.[219] The classifications also impact on choices regarding the cloud services.[220] Off-shoring of information that relates to or supports national security is, however, prohibited.

The Communications-Electronics Security Group (CESG) – a part of GCHQ – is the National Technical Authority for Information Assurance within the UK. It provides advice on Information Assurance Architecture and cyber security to UK government agencies, critical national infrastructure, the wider public sector and suppliers to UK government.[221]

While certain organisations, such as telecommunications service providers, are required to notify the Commissioner of Information, and in some cases individuals themselves, of

---

relevant offences such as dishonestly obtaining communications services (s 125); possession or supply of apparatus etc. for contravening s 125 of the *Communications Act 2003* (s 126) and improper use of public electronic communications network (s 127).[214] The *Wireless Telegraphy Act 2006* criminalises the use of wireless telegraphy apparatus with intent to obtain or disclose information as to the contents of a message without authorization (s 48). (Note that cl 221 of the Investigatory Powers Bill 2016 envisages amendments to s 48 and related sections of the Wireless Telegraphy Act 2006. The general fraud offence under the *Fraud Act 2006* can be used to prosecute phishing. The *Regulation of Investigatory Powers Act 2000* criminalises the failure by a decryption key holder to comply with a demand to hand over the key to the police, intelligence services or customs and excise (ss 49-51). (See s 200(4) and Schedule 10 Part 3 of the Investigatory Powers Bill 2016 for amendments to these provisions.)

[215] *Data Protection Act 1998*, Schedule 1, Part 1.

[216] *Data Protection Act 1998*, Schedule 1, Part 2.

[217] <https://www.gov.uk/government/publications/government-security-classifications>.

[218] <https://www.gov.uk/government/publications/government-security-classifications>.

[219] Cabinet Office, Government Security Classifications (2013) 3: 'Each attracts a baseline set of security controls providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.'

[220] Cabinet Office, Government Security Classifications (2013) par 52.

[221] <https://www.cesg.gov.uk/articles/cesg-information-security-arm-gchq>.

(cont.)

personal data security breaches,[222] this requirement does not extend to government agencies in the UK. The Information Commissioner's 2014/14 annual report noted that of the 1677 reports filed voluntarily, 31 involved police and criminal records and 23 central government.[223]Various provisions of the *Investigatory Powers Bill* scheme address data security and deletion obligations. For example, in relation to data accessed through lawful interception,[224] clause 46 provides for measures such as:

- Limiting to the minimum necessary for authorised purposes:[225]
    - the number of persons to whom any of the material is disclosed or otherwise made available;
    - the extent to which any of the material is disclosed or otherwise made available;
    - the extent to which any of the material is copied (note however that 'copy' has a restricted meaning);[226]
    - the number of copies that are made.
- Ensuring that every copy made of any of the material is stored, for so long as it is retained, in a secure manner.[227]
- Ensuring that material obtained under a warrant, if not destroyed earlier, is destroyed as soon as there are no longer any relevant grounds for retaining it.

The integrity and security of retained by telecommunications operators in terms of the Bill are also protected. Clauses 81 and 82 require operators retaining communications data under the Act to:

(a) secure that the data is of the same integrity, and subject to at least the same security and protection, as the data on any system from which it is derived,
(b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and
(c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure.

---

[222] Information Commissioner's Office, Guidance on Data Security Breach Management: Data Protection Act, version 2.1, 4. See also <https://ico.org.uk/for-organisations/guide-to-pecr/security-of-services>.
[223] Information Commissioner, Annual Report and Financial Statements 2014/15, 26.
[224] For similar provisions on the Investigatory Powers Bill relating to other warrants and data, see cl 112 (Safeguards relating to retention and disclosure of material; cl 113 (Safeguards relating to disclosure of material or data overseas); cl 132 (Safeguards relating to retention and disclosure of material); cl 133 (Safeguards relating to disclosure of material overseas); cl 150 (Safeguards relating to the retention and disclosure of data); cl 152 (Offence of making unauthorised disclosure); cl 168 (Safeguards relating to retention and disclosure of material; cl 169 (Safeguards relating to disclosure of material or data overseas); and cl170 (Safeguards relating to examination of material etc.)
[225] Cl 46(2) of the Investigatory Powers Bill 2016.
[226] Cl 46(10) of the Investigatory Powers Bill 2016: 'In this section—
'copy', in relation to material obtained under a warrant, means any of the following (whether or not in documentary form)—
(a) any copy, extract or summary of the material which identifies the material as having been obtained under the warrant, and
(b) any record which—
(i) refers to any interception or to the obtaining of any material, and
(ii) is a record of the identities of the persons to or by whom the material was sent, or to whom the material relates, and 'copied' is to be read accordingly.
[227] Cl 46(4) of the Investigatory Powers Bill 2016.

(cont.)

Codes of Practice under the *Investigatory Powers Bill* regime must also regulate security and retention of communications data held by public authorities under Part 3 of the Bill (communications data obtained by authorisation).[228]

Submissions to the Joint Parliamentary Committee on the draft *Investigatory Powers Bill*[229] raised a range of security concerns relating to the retention of large datasets.[230] Particular concern was raised in relation to the security of increased data to be retained by telecommunications and postal operators.[231] To address cost barriers, clause 213 of the *Investigatory Powers Bill 2016* compels the Secretary of State to ensure that arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of such of their relevant costs as the Secretary considers appropriate.

6.5.3 Canada

Canada has an extensive range of legal provisions and standards relating to data security, reflecting a high level of government concern about data and cyber security. This includes relevant criminal provisions to deal with unauthorised access, use, modification or interference with data and data systems. [232]

The *Digital Privacy Act 2015* was passed on June 18, 2015 which amended aspects of the *Personal Information Protection and Electronic Documents Act* and entered into force also on 18 June 2015. One of the amendments was to introduce new data breach notification provisions, which will come into effect on a later date. It will require private organisations to report security breaches involving personal information to the Privacy Commissioner.

A number of the current data security policies – notably the Management of Information Technology Security Standard, a Treasury Board Standard - are general and do not address Big Data issues explicitly, or else they may not cover criminal intelligence and national security concerns in depth. The current data security standards framework does not reflect dynamic mechanisms that seek to address risks as they arise in a coherent manner either.

The Government Security Policy issued by the Treasury Board outlines an accountability framework for matters of government security. The Policy, however, is focused more around security clearances and matters of security breaches from personnel. While protecting data and information is part of the Policy, it is not at the forefront of addressing data security risks. This may be contrasted with the *Personal Information Protection and Electronic Documents Act 2000* which does have dynamic mechanisms for dealing with security risks and poses an appropriate level of data security on private organisations including data breach notification.

---

[228] Investigatory Powers Bill 2016 Schedule 7 cl 3. These must, in particular, include provision about why, how and where the data is held, who may access the data on behalf of the authority, to whom, and under what conditions, the data may be disclosed, the processing of the data for purposes otherwise than in connection with the purposes for which it was obtained or retained, the processing of the data together with other data, and the processes for determining how long the data should be held and for the destruction of the data.

[229] House of Lords House of Commons Joint Committee on the Draft Investigatory Powers Bill Draft Investigatory Powers Bill Report HL 93 HC 651 (2016).

[230] House of Lords House of Commons Joint Committee on the Draft Investigatory Powers Bill Draft Investigatory Powers Bill Report HL 93 HC 651 (2016) par 164.

[231] House of Lords House of Commons Joint Committee on the Draft Investigatory Powers Bill Draft Investigatory Powers Bill Report HL 93 HC 651 (2016) par 174-175.

[232] See s 432 and 430 of the Canadian Criminal Code.

6.5.4 Observations

Australia has a range of data security-related offences, strategies, policies and standards relating to data security, reflecting a high level of government concern about data and cyber security. Increased data sharing in a Big Data environment will however increase the need for consistency in data security measures and practices. The data security measures of the UK can provide useful guidance; in particular measures contained in the *Investigatory Powers Bill*, would augment current Australian measures. For example, (1) the emphasis on limiting to the minimum necessary for authorised purposes the persons who can examine data obtained under the *Investigatory Powers Bill*; (2) the extent to which relevant material is copied and disclosed; and (3) the requirement that material obtained under the Bill should be destroyed as soon as there are no longer any relevant grounds for retaining it, appear particularly helpful to balance NSLE objectives and data security.

6.6. Is accountability maintained?

This section probes aspects of the legal and policy framework of each country to determine whether data access and usage decisions are subject to appropriate internal governance as well as independent oversight and accountability. Appropriate governance and accountability measures are vital to ensure the public trust and acceptance of invasive national security measures.

6.6.1 Australia

Oversight and accountability measures differ from agency to agency and generally include executive oversight, a measure of independent oversight and ultimately Parliamentary oversight.

6.6.1.1 Independent oversight bodies

Inspector-General of Intelligence and Security (IGIS)

IGIS is an independent statutory office is established by *the Inspector-General of Intelligence and Security Act 1986 (Cth)* and located in the Prime Minister's portfolio. IGIS has oversight of ASIO, ASIS, ONA, DIO, DIGO and ASD. The Prime Minister may also request the Inspector-General to inquire into an intelligence or security matter relating to any other Commonwealth agency.[233]

In addition to its compliance and general proprietary and effectiveness reviews IGIS may also inquire into acts or practices of the agencies that are or may be inconsistent with or contrary to any human right, constitute or may constitute discrimination, or may be unlawful under the *Age Discrimination Act 2004*, the *Disability Discrimination Act 1992*, the *Racial Discrimination Act 1975* or the *Sex Discrimination Act 1984*. Under s 11(3) of the *Australian Human Rights Commission Act 1986* the Australian Human Rights Commission is required to refer such complaints to IGIS where it relates to an act or practice of an intelligence agency.

IGIS is able to perform important oversight functions in relation to Big Data usage, albeit limited to the national intelligence agencies and within the scope of its capacity. It is not

[233] S 9(3) of the *Inspector-General of Intelligence and Security Act 1986.* This happened for example when IGIS undertook an inquiry in 2011 into data practices at the Defence Security Authority. See IGIS Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority (2011) <https://www.igis.gov.au/publications-reports/public-reports>.

(cont.)

clear from IGIS's reports whether it consistently and deeply reviews intelligence data and analysis by the relevant agencies or the design and functioning of the technical analytical or data systems. Those inquiries that have been undertaken, however, were highly relevant.[234]

Commonwealth Ombudsman

The office of the Commonwealth Ombudsman was established by the Ombudsman Act 1976 to investigate government administrative actions through investigation and record inspection powers.[235]

The Commonwealth Ombudsman focuses on action of federal government departments within the meaning of the *Public Service Act 1999* as well as actions of prescribed authorities.[236] ASIO and IGIS are excluded from the scope of the *Ombudsman Act 1976*[237] but the other national intelligence agencies (ASIS, the ONA, ASD, DIO and DIGO) are covered by the Act. IGIS and the Ombudsman collaborate in relation to the oversight of these bodies. Other agencies relevant to this study, for example, the Australian Federal Police, AUSTRAC, the Australian Crime Commission and CrimTrac are also covered by the Commonwealth Ombudsman.[238]

The Ombudsman inspects the records of agencies such as the Australian Federal Police and the Australian Crime Commission to ensure compliance with legislative requirements applying to selected law enforcement and regulatory activities. This inspection role is detailed in laws such as the *Telecommunications (Interception and Access) Act 1979.* The Ombudsman administers the Public Interest Disclosure Scheme under the *Public Interest Disclosure Act 2013*. IGIS shares these responsibilities in relation to the national intelligence agencies. [239] The Ombudsman was given an additional and extensive oversight function in terms of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)*.[240]

Certain restrictions apply to the jurisdiction of the Ombudsman. For example, in addition to having ASIO and IGIS outside its scope, the Ombudsman is not authorized to investigate action taken by a Minister.[241] Under section 9(3) of the *Ombudsman Act 1976,* the Attorney-General can prevent the Ombudsman from accessing information if he or she certifies that

---

[234] For example, in 2013 it reported on an inquiry into the analytic independence of ASIO, DIO and ONA. The inquiry noted that ASIO and DIO did not conduct formal reviews of key judgements to see whether there were any lessons that could be learnt and did not have written policies relating to the management of dissent. See Inspector-General of Intelligence and Security, *Annual Report 2012–13* (2013) 9. It reported on subsequent improvements in Inspector-General of Intelligence and Security, *Annual Report 2014–15* (2015) 29.

[235] Overview of the Commonwealth System of Administrative Review <http://www.arc.ag.gov.au/Aboutus/Pages/OverviewoftheCommonwealthSystemofAdminReview.aspx#28>.

[236] S 3 read with s 5(1) of the *Ombudsman Act 1976.*

[237] *Ombudsman Regulations 1977* (Cth) Regs 4 and 6, read with Schedule 3.

[238] The Commonwealth Ombudsman cooperates with the Inspector-General of Taxation in relation to the ATO. The Ombudsman deal with complaints concerning Freedom of Information and Public Interest Disclosures matters relating to the ATO while the Inspector-General of Taxation addresses tax administration matters. See <http://www.ombudsman.gov.au/pages/tax/>.

[239] In addition, it also acts as the Ombudsman in relation to a number of specific schemes, for example in relation to the Defence Force, Law Enforcement and the Postal Industry.

[240] Parliamentary Library, *Budget Review 2015–16*, 2015 <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201516/Telco>.

[241] S 5(2)(a) of the *Ombudsman Act 1976.*

(cont.)

disclosure of that information would be contrary to the public interest because it would prejudice the security, defence or international relations of the Commonwealth. The Ombudsman's capacity is also an important restrictive factor.

There are few indications that the Ombudsman actively probes issues relating to data analysis. The main focus, especially under the *Telecommunications Act*, is to review records to check compliance with data access and retention requirements. It has no particular obligations in relation to data analysis and usage.

Australian National Audit Office

The Auditor-General,[242] an independent officer of the Parliament[243] established under the *Auditor General Act 1997*[244] is assisted by the Australian National Audit Office (ANAO) to provide an independent view of the performance and financial management of public sector entities. While the auditing of financial statements provides some means to consider efficient data management practices, the ANAO's performance audits are the most important means to investigate the data management practices of agencies.[245]

Privacy and Information Commissioners

The Office of the Australian Information Commissioner (OAIC), which operates at a federal level, was established in 2010 under *the Australian Information Commissioner Act 2010* to house the Privacy Commissioner, the Australian Information Commissioner and the Freedom of Information Commissioner. Currently the appointed Privacy Commissioner also functions as the Information and the Freedom of Information Commissioner.

The OAIC is an Australian government agency whose Act gives it responsibility to oversee government information policy functions. The Information Commissioner reports to the Attorney-General on matters relating to Australian Government information management policy and practice. Importantly for this study, the OAIC also has responsibility for freedom of information (FOI) and for privacy.[246]

Its FOI functions include oversight of the operation of the *Freedom of Information Act 1982* (Cth) and review of decisions made by agencies and ministers under that Act. If a person is dissatisfied with the result of an FOI request, they may seek review by the OAIC. There are limits on the application of the FOI regime to law enforcement and national security intelligence functions.

The OAIC is responsible for privacy functions conferred by the *Privacy Act 1988* and other laws. The OAIC is responsible for privacy functions conferred by the *Privacy Act 1988* and other laws. The *Privacy Act* entitles persons to lay complaint with the Information

---

[242] Functioning under the *Auditor-General Act 1997*.
[243] *Auditor General Act 1997* (Cth) s 8.
[244] *Auditor General Act 1997* (Cth) s 7.
[245] See for example ANAO, *Managing Data Privacy in Centrelink* Audit Report No.8 1999–2000; ANAO, *The Australian Taxation Office's Use of Data Matching and Analytics in Tax Administration*, Audit Report No.30 2007–08; ANAO, *Cyber Attacks: Securing Agencies' ICT Systems*, Audit Report No. 50 2013–14; ANAO, *AUSTRAC's Administration of its Financial Intelligence Function*, Audit Report No.47 2012–13.
[246] See <http://www.oaic.gov.au/about-us/what-we-do/what-we-do>. There are also rights akin to FOI embedded in the *Privacy Act 1988* APPs 12 and 13. There is therefore some overlap with Privacy Commissioner functions and the OAIC's FIO functions, although this is lessened by a number of limitations in the application of APP 12 and 13, in particular their exclusive focus on personal information.

(cont.)

Commissioner regarding the handling of their personal information by Australian, ACT and Norfolk Island government agencies as well as private sector organisations covered by the *Privacy Act*. The OAIC may also launch investigations at its own initiative into acts or practices that might breach the *Privacy Act*. The OAIC has a wide range of powers in relation to privacy matter, including the power to conduct assessments to determine whether practices are in accordance with the *Privacy Act* and APPs. It may also direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function. The OAIC can also, under s 52 of the *Privacy Act 1988*, make determinations on privacy complaints where conciliation has not resolved the matter or in relation to Commissioner initiated investigations.[247]

The OAIC also has a range of responsibilities under other laws, including relating to data matching, eHealth, spent convictions and tax file numbers.

In the May Budget in 2016 the Government announced a decision not to proceed with proposals from 2014 to change arrangements for privacy and Freedom of Information (FOI) regulation. The OAIC would have been disbanded and its functions distributed (under a Bill which passed the House of Representatives but which did not proceed in the Senate), but early in 2016 it was announced that the OAIC will continue and that it retains ongoing responsibility for its three areas of responsibility (FOI, privacy and information policy).[248]

Privacy commissioners exist in most states and territories. They play roles in general compliance, and dealing with complaints, particularly in relation to state agencies and organisations.

Other independent oversight mechanisms

The Australian Human Rights Commission operates under the *Australian Human Rights Commission Act 1986* (Cth) as well as federal laws[249] that seek to ensure freedom from discrimination on the basis of attributes such as age, disability, race, sex, sexuality and gender identity. The Commission also has specific responsibilities under the *Native Title Act 1993* (Cth) and the *Fair Work Act 2009* (Cth). The Commission's footprint in relation to national intelligence agencies is limited. Its functions do not include inquiring into an act or practice of a national intelligence agency. Where a complaint is made to the Commission alleging that an act or practice of such an agency is inconsistent with or contrary to any human right, constitutes discrimination, or is unlawful under the *Racial Discrimination Act 1975*, the *Sex Discrimination Act 1984* , the *Disability Discrimination Act 1992*, or the *Age Discrimination Act 2004* , the Commission must refer the complaint to IGIS.[250]

---

[247] An important recent example is *Ben Grubb and Telstra Corporation Limited* [2015] AICmr 35 (1 May 2015) <http://www.austlii.edu.au/au/cases/cth/AICmr/2015/35.html>, where the Privacy Commissioner held that the complainant's telecommunications metadata held by the telecommunications company is personal data and that the complainant is entitled to access that data.

[248] See Attorney General's Department 'Portfolio Budget Statement', May 3 2016, 261 <https://www.ag.gov.au/Publications/Budgets/Budget2016-17/Pages/Portfolio-Budget-Statements-2016-17.aspx>

[249] The *Age Discrimination Act 2004*, *Disability Discrimination Act 1992*, *Racial Discrimination Act 1975*, *Sex Discrimination Act 1984* are mentioned by name in s 11(1) *Australian Human Rights Commission Act 1986*.

[250] S 11(3) Australian Human Rights Commission Act 1986 (Cth).

(cont.)

The Australian Commission for Law Enforcement Integrity and the Integrity Commissioner[251] have important functions to ensure that data management is not subverted through 'corruption', including an abuse of office, perversion of the course of justice and extending to fraud, bribery, extortion or misuse of information or resources.[252] The Commission's jurisdiction does not extend to the national security agencies.[253]

Parliamentary oversight

Parliament is the ultimate oversight body, holding relevant Ministers accountable for the agencies under their control.[254] Annual reports that are produced by agencies and departments assist Parliament to exercise this function. ASIO is however the only national intelligence agency that is required to file such a report. Budget processes, especially the Senate Estimates processes, provide a range of parliamentary committees with the opportunity to engage agencies regarding their proposed spending. Important oversight functions are clustered in the Parliamentary Joint Committee on Intelligence and Security.

Section 28 of the *Intelligence Services Act 2001* (Cth) provides that a committee to be known as the Parliamentary Joint Committee on Intelligence and Security must be established after the commencement of the first session of each Parliament. The Committee's functions include the review of the administration, expenditure and annual financial statements of ASIO, ASIS, AGO, DIO, ASD and ONA. It also reviews any matter in relation to these agencies referred to it by the responsible Minister or by a resolution of either House of the Parliament. The Committee furthermore monitors and reviews the performance by the Australian Federal Police of its functions under Part 5.3 (Terrorism) of the *Criminal Code.*[255]

However, a range of matters fall outside the Committee's scope. The functions of the Committee for example do not include reviewing the intelligence gathering and assessment priorities of the national intelligence agencies; reviewing their sources of information or other operational assistance or operational methods available to them; reviewing an aspect of their activities that does not affect an Australian person; or reviewing the coordination and evaluation activities undertaken by ONA.[256] The Committee furthermore does not have the power to decide to review any matter without it being referred to the Committee.[257]

Australian oversight bodies and Big Data

The current oversight bodies are able to perform and do perform important functions in respect of the current data regime.[258]

---

[251] Currently Mr Michael Griffith AM. See <http://www.aclei.gov.au/Pages/Integrity-Commissioner.aspx>.

[252] According to s 6(1) of the *Law Enforcement Integrity Commissioner Act 2006* (Cth) a staff member of a law enforcement agency engages in corrupt conduct if he or she, while a staff member of the agency, engages in conduct involving an abuse of office as a staff member of the agency; or conduct that perverts, or that is engaged in for the purpose of perverting, the course of justice; or conduct that involves corruption of any other kind. See for examples ss 6(3) and 8 of the *Law Enforcement Integrity Commissioner Act 2006*.

[253] See <https://www.comlaw.gov.au/Series/C2006A00085>.

[254] *Church of Scientology v Woodward* (1982) 43 ALR 587.

[255] S 29(1) *Intelligence Services Act 2001* (Cth).

[256] S 29(2) *Intelligence Services Act 2001* (Cth).

[257] This power was envisaged in Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015. The Bill lapsed on 17 April 2016.

[258] Interviewees highlighted their role to inform agency policy ('[IGIS] also critiques the benchmark' and encourage compliance (see 7.5.2A-C, 7.5.3A-D). On the negative side, there may be some duplication (see 7.5.4 'Duplication of oversight').

From a Big Data perspective it is noticeable that no single body has oversight of the whole data universe that is relevant to Big Data and national security in Australia. There is, for example, an important divide between IGIS and the other oversight bodies: IGIS does not have oversight over non-intelligence agencies supplying data to intelligence agencies. The other oversight bodies, however, do not have coverage of the use by intelligence agencies of that data.

It is not clear that the existing bodies jointly have effective and holistic oversight over the data universe either. Oversight bodies appear very conscious of the need to cooperate, especially where powers and scope may overlap. The bodies therefore conclude memoranda of understanding to facilitate their cooperation and prevent overlap. It does not however appear from public documents, including their annual reports, that they cooperate and exchange information to ensure seamless oversight over data flowing from one agency to another.

Little in the public realm indicates that technical issues regarding data analysis receives much attention from oversight bodies. Attention is given to compliance with data accessing and collection rules, but data analysis itself does not appear to be subject to an equivalent measure of independent monitoring.

Recording and record-keeping

The quality and effectiveness of oversight is dependent on the availability of information and records evidencing decisions and decision-making processes. A range of laws regulate aspects of retention management and disclosure of government records.[259] General obligations to keep records of decisions and activities of public functions stems from general management legislation such as the *Public Governance, Performance and Accountability Act 2013*, information security standards and general management imperatives. There are, however, no explicit, system-wide rules applying throughout the national intelligence and law enforcement system that require data access and usage to be tracked and sufficiently recorded to enable the review of the grounds for the access and usage decisions.[260]

Where records are made, the *Archives Act 1983* (Cth) is particularly significant for this study. This Act regulates the retention and destruction of a wide range of documents relevant to data as well as the disclosure of documents after a sufficient time elapsed to render them historical.[261] While the *Archives Act* requires a significant number of records to be retained its scheme allows many records relevant to the assessment of data access and mining

---

[259] See for example also the *Freedom of Information Act 1982 (Cth)*; *Australian Information Commissioner Act 2010* (Cth); *Privacy Act 1988* (Cth); *Electronic Transactions Act 1999* (Cth); *Financial Management and Accountability Act 1997* (Cth); and *Crimes Act 1914* (Cth). See in general <http://naa.gov.au/records-management/strategic-information/standards/records-and-legislation/index.aspx>.

[260] For an example where such rules introduced, see AUSTRAC *Annual Report* 2012–2013 (2013) 63. AUSTRAC advised that it implemented a Reason for Access (RFA) function, enabling partner agency users to record the grounds for conducting searches.

[261] The National Archives issues 'records authorities' set out detailed requirements for keeping, destroying or transferring records of business common to many Commonwealth agencies. The Administrative Functions Disposal Authority (AFDA) and AFDA Express provide for a range of common administrative functions. See <http://www.naa.gov.au/records-management/publications/afda.aspx>.

(cont.)

systems to be destroyed.[262] Retention requirements of records regarding the design, technology and telecommunications functions are too limited to support public scrutiny of Big Data systems. Disclosure of retained records will also be too late to support appropriate scrutiny.

Complaint mechanisms as sources of information and review

A range of complaints handling entities (including IGIS, [263] the Commonwealth Ombudsman - also acting among others as the Defence Force Ombudsman, the Immigration Ombudsman and the Law Enforcement[264] - the Privacy Commissioner and the Inspector-General of Taxation) may receive a complaint from a person who feels aggrieved by an act or decision of a federal government department or agency, provided it falls within their statutory scope.[265] The chances of a breach coming to the attention of an affected person are, however limited. Most of the decisions regarding data access and data analysis take place beyond the reach and knowledge of affected persons. This is illustrated by the experiences of IGIS. In its 2013-2014 *Annual Report*, IGIS noted that it received 504 complaints of which 487 related to visa-related security assessment.[266] Security assessments are undertaken as part of the visa application processing and a negative finding would result in the refusal of a visa, thereby potentially triggering a complaint.[267] Such disclosure is uncommon in relation to the use and analysis of data outside formal law enforcement processes.

The *Public Interest Disclosure Act 2013 (Cth)* was adopted to channel formal, serious disclosures by staff members. This Act facilitates disclosure and investigation of wrongdoing and maladministration in the Commonwealth public sector. The Act allows for intelligence and law enforcement officials to make a formal disclosure to the relevant agency, the Commonwealth Ombudsman or, where relevant, IGIS. As the scheme is still relatively new it is not possible to assess its impact. By 30 June 2014, for example, IGIS had received only 1 disclosure but reported that it did receive a number of enquiries regarding the scheme.[268]

6.6.2 United Kingdom

The *Investigatory Powers Bill 2016* envisages significant changes to the UK's oversight regime. The current system of oversight for NSLE agencies' use of investigatory powers is grounded in different Acts, for example in RIPA, the *Police Act 1997*, and the *Justice and Security Act 2013*. These Acts provides for oversight by a number of different bodies.[269] The Parliamentary oversight function is currently entrusted to the cross-party Intelligence and Security Committee of Parliament[270] while independent non-Parliamentary oversight is carried out by a number of commissioners:

---

[262] The extensive Technology and Telecommunications chapter of the AFDA, Chapter 19, stipulates for example allows records documenting testing activities where unexpected results are found to be destroyed when problem has been rectified. See National Archives of Australia, *AFDA*, 322.
[263] IGIS, 'Making a Complaint', IGIS web page <https://www.igis.gov.au/making-complaint>.
[264] <http://www.ombudsman.gov.au/pages/our-legislation/australian-federal-police/>.
[265] See for example <http://www.ombudsman.gov.au/pages/related-sites/other-complaint-handling-review-agencies.php>.
[266] *IGIS Annual Report 2013–2014* (2014) 15.
[267] *Plaintiff M47-2012 v Director General of Security* [2012] HCA 46.
[268] *IGIS Annual Report 2013–2014* (2014) 14.
[269] Draft Investigatory Powers Bill Cm 9152 (November 2015) par 5.
[270] *Justice and Security Act 2013* ss 1-4.

(cont.)

- The Interception of Communications Commissioner oversees the exercise by public authorities of their interception and communications data powers under RIPA and the powers under section 94 of the *Telecommunications Act* (directions in the interests of national security).[271]
- The Chief Surveillance Commissioner oversees how law enforcement agencies use covert surveillance powers and covert human intelligence sources under RIPA and the *Police Act 1997*.
- The Intelligence Services Commissioner oversees how the intelligence agencies use the powers available to them under RIPA Part II (covert surveillance and covert human intelligence sources) and the *Intelligence Services Act 1994*.
- The Information Commissioner has responsibility for promoting and enforcing the *Data Protection Act 1998* and the *Freedom of Information Act 2000*, as well as associated legislation such as the Privacy and Electronic Communications (EC Directive) Regulations 2003.
- The Surveillance Camera Commissioner, introduced under the *Protection of Freedoms Act 2012*, is primarily focused on raising awareness of, and generating debate on, the use of CCTV in public spaces and other related issues. The Commissioner's functions include encouraging compliance with the Surveillance Camera Code of Practice.

In addition, the Investigatory Powers Tribunal investigates and determines complaints of unlawful use of covert techniques by public authorities that infringing the right to privacy and claims against intelligence or law enforcement agency conduct which breaches a wider range of human rights.[272]

The complexity of the oversight framework was criticised in RUSI report.[273] They also noted a lack of public trust in the oversight framework:

> The ISC is the body responsible for holding the SIAs to account. Critics argue that the Committee has 'consistently, and sometimes very publicly, failed in its duty to challenge these agencies'. These criticisms over its membership, outputs and degree of independent scrutiny have contributed to the deficit in public confidence …'[274]

The *Public Interest Disclosure Act 1998* provides protection against employer victimisation when an employee blows the whistle in the public interest. While civil servants are in general included in the ambit of this Act, police officers and employees of national intelligence agencies are excluded.[275] The *Official Secrets Act 1989* does not provide a public

---

[271] *Telecommunications Act 1984* s 94. See 3.1.3.

[272] <http://www.ipt-uk.com>.

[273] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 4.47. See Information Commissioner's Office (ICO) et al., Surveillance Road Map: A Shared Approach to the Regulation of Surveillance in the United Kingdom, Version 3.5, (2015).

[274] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) par 2.37. See also par 2.39: 'A second layer of oversight, provided for in legislation, comes in the form of the commissioners – comprising a number of retired senior judges – who, among other functions, retrospectively assess the necessity and proportionality of samples of warrants granting authorisation to intercept citizens' communications. However, they have also come under criticism, particularly, it is said, because they are ''only part-time, inspect a small proportion of intercept warrants, have not publicly found a warrant to be disproportionate, have refused to provide adequate statistics and are under-resourced'. Evidence to the ISR Panel suggests that the commissioners and their work is not well known among the general public, and the role of the expert inspectors who support them is equally underappreciated by their critics.'

[275] Ss 10, 11 and 13 of the Public Interest Disclosure Act 1998.

(cont.)

interest disclosure defence for unauthorised disclosures[276] and is particularly onerous in relation to officials of intelligence and security services.[277] Since 2013, witnesses giving evidence to the parliamentary Intelligence and Security Committee do however enjoy protection against incrimination.[278]

Improvement of the oversight mechanism was one of the main objectives of the *Investigatory Powers Bill*. It will replace three existing commissioners (Interception of Communications Commissioner, Intelligence Services Commissioner, and Chief Surveillance Commissioner) and provide new powers and resources to an independent Investigatory Powers Commissioner (IPC). The Commissioner will hold, or have held, high judicial office and will oversee the use of the powers in the Bill by public authorities.

6.6.3 Canada

Canadian oversight bodies are able to perform and do perform important functions, often with limited resources. No single body, however, has oversight of the data exchanged between agencies identified under Bill C-51.[279] The various oversight bodies have a mandate to table a report to Parliament, but the organisations themselves do not have to make any changes to their practices based on the report. These are recommendations only. In theory the courts provide some oversight to CSIS and CSE but as seen in various leaked information to the media, and in an overt statement by a judge of the secret court, these agencies have deliberately misguided the oversight bodies, have not always been forthright, and are not bound to follow decisions issued by the court. [280] This is not true with law enforcement agencies which must comply with court rulings, and in particular to the many court decisions rendered using the Charter.

There is also little indication of a consistent investigation of memoranda of understanding or of monitoring of compliance with such memoranda that regulate access to and exchange of data. Unlike Australia, the media, academics, NGOs and former members of oversight bodies have had an active voice in stating the inadequacies in accountability, transparency and oversight of intelligence agencies.

---

[276] *R v Shayler* [2002] UKHL 11 par 20.

[277] Lucinda Maer and Oonagh Gay Official Secrecy SN/PC/02023 30 December 2008 House of Commons Library 7. *R v Shayler* [2002] UKHL 11 par 18: 'Section 1(1)(a) of the OSA 1989 imposes criminal liability on a member or former member of the security and intelligence services if, without lawful authority (as defined in section 7), he discloses any information or document relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services. The only defence expressly provided is, under subsection (5), that at the time of the disclosure he did not know and had no reasonable cause to believe that the information or documents in question related to security or intelligence. As already demonstrated, a member or former member of the security and intelligence services is treated differently under the Act from other persons, and information and documents relating to security and intelligence are treated differently from information and documents relating to other matters. Importantly, the section does not require the prosecution to prove that any disclosure made by a member or former member of the security and intelligence services was damaging to the interests of that service or the public service generally.'

[278] Cl 7 of Schedule 1 of the Justice and Security Act 2013.

[279] Security of Canada Information Sharing Act (S.C. 2015, c. 20, s. 2)

[280] See *X (Re)* (2013) FC 1275.

6.6.4 Observations about oversight mechanisms

The existing oversight bodies are able to perform and do perform important functions in Australia, the UK and Canada. Australia and the UK have oversight frameworks that are more fragmented than the Canadian framework but in general Australian and UK bodies appear to have more power to ensure that NLSE agencies improve their practices.

The fragmented nature of the oversight framework in Australia and the UK will be challenged by an environment where NSLE agencies collaborate more closely in a Big Data framework. No single body has oversight of the whole data universe that is relevant to Big Data and national security in Australia and the UK. While the bodies do seem to strive for close collaboration the number of bodies involved appear to complicate such arrangements. The UK is therefore envisaging a simplification of their regime by replacing three existing commissioners with a new and powerful independent Investigatory Powers Commissioner. The Commissioner will hold, or have held, high judicial office, thereby consolidating the enhanced judicial oversight of data-related powers under the *Investigatory Powers Bill*. The enhanced role of judicial officers in this regard in the UK stand in contrast to the role of Courts in Canada that appear in practice to be in a much weaker position.

Little in the public realm indicates that technical issues regarding data analysis receives much attention from existing oversight bodies. Attention is given to compliance with data accessing and collection rules, but data analysis itself does not appear to be subject to an equivalent measure of independent monitoring. The new Investigatory Powers Commissioner in the UK will have a brief to oversee practices relating to automated data analysis.

6.7. Are principles and rules regularly reviewed?

This section considers whether the legal framework supports the regular, transparent review of principles and rules to ensure that the system delivers intended results efficiently and reliably, proportional to impacts on civil liberties, other legal rights and individual and commercial interests.

6.7.1 Australia

Australia has a range of statutory review mechanisms. These include sunset clauses in new legislation that provides Parliament with a choice to pass new legislation, renewing or amending those provisions, or to allow their termination;[281] mandatory statutory review mechanisms that can be inserted into an Act;[282] and voluntary reviews, such as the 2012 Council of Australian Governments' review of counter-terrorism legislation,[283] the Australian Law Reform Commission inquiries into areas of law at the request of the Attorney-General

[281] Nicola McGarrity, Rishi Gulati and George Williams 'Sunset clauses in Australian Anti-Terror Laws' 2012 33 *Adelaide Law Review* 307.

[282] S 251 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* for example required a review of the operation of the Act to commence before 13 December 2013

[283] <http://www.ag.gov.au/Consultations/Pages/COAGReviewofCounter-TerrorismLegislation.aspx>. This resulted from a 2005 decision by COAG to review these laws formally after five years but the review processes only commenced in 2012. The INSLM pointed out in its *2013–2014 Annual Report* that the government has not yet heeded the recommendations of the review. See Independent National Security Legislation Monitor *Annual Report 2013–2104* (2014) 3.

(cont.)

of Australia,[284] and Commissions of Inquiry. The latter has been a particular significant mechanisms for the review and development of national security laws.[285] Important inquiries include the Royal Commission on Intelligence and Security (1974–77, Justice Robert Hope);[286] the Royal Commission on Australia's Security and Intelligence Agencies (1983–84, Justice Robert Hope); the Inquiry into Australian Intelligence Agencies (2004, Philip Flood)[287] and the Independent Review of the Intelligence Community (2011, Robert Cornall and Rufus Black).[288] The scope and depth of such reviews depend on the terms of reference and the resources allocated to the inquiry. The independent oversight bodies discussed in 6.6 also perform important review functions.

In addition to these ad hoc review mechanisms, Australia appointed the Independent National Security Legislation Monitor to review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation on an ongoing basis. The Monitor, acting in terms of the *Independent National Security Legislation Monitor Act 2010* (Cth) considers, for example, whether the laws contain appropriate safeguards for protecting the rights of individuals, remain proportionate to any threat of terrorism or threat to national security or both, and remain necessary. The government signalled its intent to repeal the *Independent National Security Legislation Monitor Act 2010* (Cth) by introducing a Bill to this effect.[289] The government may not be proceeding with changes. No formal announcement was made to that effect but the repeal Bill was discharged from the Notice Paper in July 2014.[290] After acting in the position for some months the current INSML was appointed for a period of two years in August 2015.

These mechanisms need to be real with tools and processes that are employed to support the drafting of appropriate laws and their review, such as regulatory impact assessments and privacy impact assessments. The Australian government adopted a regulatory assessment regime that includes Regulation Impact Statements or a Post-Implementation Reviews in appropriate cases.[291]

The Australian framework provides a range of mechanisms that support the review of laws, regulations and practices. They are however not embedded as consistent, systemic and mandatory requirements. The mechanisms are generally ad hoc in nature and where it is more systemic, such as the regulatory assessment processes, they rarely extend to considerations of civil liberties.

---

[284] The Commission is an independent federal agency operating under the *Australian Law Reform Commission Act 1996 (Cth)*.

[285] Royal Commissions of Inquiry function under the *Royal Commissions Act 1902* (Cth). The Governor-General on advice of the Prime Minister initiates a Royal Commission.

[286] <http://www.naa.gov.au/collection/explore/security/royal-commisson>.

[287] <https://fas.org/irp/world/australia/flood.pdf>.

[288] <http://www.dpmc.gov.au/pmc/publication/2011-independent-review-intelligence-community>.

[289] Independent National Security Legislation Monitor Repeal Bill 2014 (Cth) <https://www.comlaw.gov.au/Details/C2014B00041>.

[290]<http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5189>.

[291] The Office of Best Practice Regulation in the Department of the Prime Minister and Cabinet administers the Government's and the Council of Australian Government's regulatory impact analysis requirements.

(cont.)

6.7.2 United Kingdom

The review mechanism in the UK resemble those applied in Australia. Where laws are particularly controversial, the UK parliament sometimes uses mechanisms that require parliamentary re-consideration of statutory provisions, for example the use of renewal by affirmative resolution mechanisms,[292] and the use of sunset or review clauses.[293] The *Investigatory Powers Bill* will for example be subject to parliamentary review five years after its implementation.[294]

The independent oversight bodies discussed in 6.6.3 also perform important ongoing review functions. Independent Reviewer of Terrorism Legislation is another important example of independent and ongoing review mechanism relevant to this study. The Reviewer is appointed by the Secretary of State in terms of section 36 of the *Terrorism Act 2006* to review the provisions of the *Terrorism Act 2000* (a broad instrument addressing among others proscribed organisations, terrorist property, investigations and counter-terrorist powers) and of Part 1 of the *Terrorism Act 2006* (terrorism offences and penalties). [295] Reviews are carried out annually and reports are laid before Parliament.[296]

As part of the political agreement that secured cross-party support for the *Data Retention and Investigatory Powers Act 2014* section 7 was inserted into that Act requiring the Secretary of State to appoint the Reviewer to review the operation and regulation of the relevant investigatory powers.[297] The report that resulted from this review was one of the trio of 2015 reports on data and investigation (see 4) and its recommendations informed the drafting of the *Investigatory Powers Bill*.[298] The Reviewer played an active role to inform public debate regarding the Bil[299] This role became even more central in mid-2016, when the Reviewer was requested by UK government to review the operational case for bulk data collection powers envisaged in the Bill and to deliver his report in time for the detailed debate of these powers at the committee stage in the House of Lords.

---

[292] Ss 1-9 of the Prevention of Terrorism Act 2005 (repealed) were subject to annual renewal by affirmative resolution of both Houses of Parliament. See s 13 of the Prevention of Terrorism Act 2005 (repealed). See in general See Anderson 'The Independent Review of Terrorism Law' 2014 *Public Law* 403 404-406 for an overview of the history of annual reviews of terrorism laws.

[293] For example, s 8(3) of Data Retention and Investigatory Powers Act 2014: 'Sections 1 to 7 (and the provisions inserted into the Regulation of Investigatory Powers Act 2000 by sections 3 to 6) are repealed on 31 December 2016.'

[294] Clause 222 of the *Investigatory Powers Bill 2016*.

[295] Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006 (2015) par 1.2: 'The function of the Independent Reviewer, as it was explained when reviews were first placed on an annual basis, is to 'look at the use made of the statutory powers relating to terrorism', and 'consider whether, for example, any change in the pattern of their use needed to be drawn to the attention of Parliament'. For more than 35 years, successive Independent Reviewers have used their reports to ask whether special powers continue to be necessary for fighting terrorism, and to make recommendations for reform.'. Also see David Anderson, 'The independent review of terrorism laws' 2014 *Public Law* 403-421 for the origins and history of independent review of UK anti-terrorism laws.

[296] S 36 of the Terrorism Act 2006.

[297] S 7(1) of the Data Retention and Investigatory Powers Act 2014.

[298] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (2015).

[299] See for example the papers and materials on the Reviewer's website at <https://terrorismlegislationreviewer.independent.gov.uk/>.

(cont.)

The Reviewer considers government policy and statistics and interacts with agencies and community groups.[300] The Reviewer does not only rely on formal reviews and reports to engage the government and the public. The Reviewer increasingly engages the public actively through posts on its official website, through participation in conferences and other public events and through use of social media. According to the Reviewer these additional communication channels enables him to react much faster to developments and often enables him to engage with experts and academics that he would not normally meet in person.[301]

Over the years various ad hoc commission of inquiry have investigated national security legislation and made recommendations regarding law reform and improvement in processes and procedures.[302] In addition to the Monitor's 2015 report referred to above, two other UK enquiries have played a major role to inform the drafting of the *Investigatory Powers Bill 2016*. The first of these was a parliamentary inquiry launched in 2013 by the Intelligence and Security Committee of Parliament. It resulted in a March 2015 report entitled 'Privacy and Security: A modern and transparent legal framework'.[303] The second report was an independent review of surveillance practices in the UK, announced by the UK government in March 2014.[304] The government appointed the Royal United Services Institute, with a broad-based review panel representing senior government, industry, civil society and

---

[300] Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006 (2015) par 10.16. The Reviewer was concerned that the Supreme Court placed too high a value on his Review when it stated in *DPP v Beghal* [2015] UKSC 49 at par 43(x) that: 'the continuous supervision of the Independent Reviewer is of the first importance; it very clearly amounts to an informed, realistic and effective monitoring of the exercise of the powers and it results in highly influential recommendations for both practice and rule change where needed.' The review process is however not an in-depth inspection function. The Reviewer explained it as follows in Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006 (2015) (emphasis in original): 'There is a difference between the function of *review*, as practised by successive Independent Reviewers working alone on a part-time basis, and the *inspecting* and *auditing* functions undertaken by other independent figures such as the Chief Inspector of Borders and Immigration or the Interception of Communications Commissioner, in each case with the help of trained inspectors and other staff. While I have devoted considerable time over the past four years to questioning ports officers and ports users, many of my contacts have been at a very senior level; I witness examinations only occasionally; there are still many ports I have never visited; and my efforts could be said to have amounted to '*continuous supervision*' or to '*monitoring*' only in a fairly general sense of those words. There are other functions in respect of which the Independent Reviewer is more thinly stretched still; further responsibilities have been or are to be added; and it is desirable to keep some slack in the system for one-off tasks or '*snapshot*' reports.'

[301] Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006 (2015) par 1.4.

[302] See for example *Report of the Commission to consider legal procedures to deal with terrorism in Northern Ireland*, December 1972, Cmnd.5185; *Report of a Committee to consider, in the context of civil liberties and human rights, measures to deal with terrorism in Northern Ireland*, January 1975, Cmnd.5847; Lord Shackleton *Review of the operation of the Prevention of Terrorism (Temporary Provisions) Acts 1974 and 1976,* August 1978, Cmnd.7324; *Report of the Committee of Inquiry into Police Interrogation Procedures in Northern Ireland* March 1979, Cmnd.7497; *The Jellicoe Report on The Prevention of Terrorism (Temporary Provisions) Act 1976* (1983), Cmnd.8803; Lord Lloyd of Berwick *Inquiry into legislation against terrorism* October 1996, Cm.3420. See Anderson 'The Independent Review of Terrorism Law' 2014 *Public Law* 403 for an overview of the history.

[303] Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework (2015).

[304] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 0.1.

(cont.)

Parliamentary expertise, to consider broader questions regarding surveillance.[305] The Independent Surveillance Report entitled 'A Democratic Licence to Operate' was published by in July 2015.[306]

Regulatory impact statements and assessments and privacy impact assessments are important review tools and processes. The UK government supports the submission of all new policies, programmes and projects, whether revenue, capital or regulatory to comprehensive but proportionate assessment to ensure that the public interest is best promoted.[307] Assessments include appraisals of proposed measures and retrospective evaluation of projects, programs and policies.[308]

It is UK government policy that government departments and agencies exercising statutory powers and making rules that could affect businesses, charities or the voluntary sector must produce a Regulatory Impact Assessment to assess the costs, benefits and risks of proposed regulation.[309] Assessments should also be produced for proposed European legislation that will have an effect on businesses, the public sector, charities or the voluntary sector in the UK.[310]

UK government departments and agencies as well as the private sector also undertake Privacy Impact Assessments. These generally follow the guidance issued by the Information Commissioner's Office.[311]

6.7.3 Canada

Canadian agencies may be audited around many of their practices such as data handling processes, information security protocols, use of technologies (capabilities), and disclosure of personal information to third parties (other agencies). The Treasury Board and the Auditor General have a mandate to order and/or perform an audit.

The Treasury Board of Canada may request that an agency perform a risk assessments and/or internal audit of an agencies practices. For example, Part II of the Operational Security: Management of Information Technology Security Standard requires risk management on a continual basis (no period of time specified) which is inclusive of internal audits, training on an ongoing basis, security awareness, vulnerability assessment, written agreements where information or infrastructure is shared between departments or with other organisations, and similar IT security aspects.[312] These audits, however, are done by the agency themselves.

For other guidelines and directives the Treasury Board may order an audit, perform an audit, and make recommendations. For example, the Treasury Board Secretariat according to

---

[305] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 0.2.
[306] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015).
[307] HM Treasury The Green Book: Appraisal and Evaluation in Central Government (2011) par 1.1.
[308] HM Treasury The Green Book: Appraisal and Evaluation in Central Government (2011) par 1.8.
[309] HM Treasury The Green Book: Appraisal and Evaluation in Central Government (2011) par 2.22.
[310] HM Treasury The Green Book: Appraisal and Evaluation in Central Government (2011) par 2.22. The UK government also maintains a better regulation framework applies to measures that regulate or deregulate business or concern the regulation of business. It does not apply to measures that only regulates or deregulates the public sector or individual citizens. See *Better Regulation Framework Manual: Practical Guidance for UK Government Officials* (March 2015).
[311] <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/>.
[312] Management of Information Technology Security Standard s 12.

(cont.)

section 7 of the Government Security Policy may require an audit, and make remedial recommendations and take corrective action.

The Auditor General has the power and duty under sections 5 and 6 of the *Auditor General Act 1985* to audit the accounts and financial statements of the government of Canada (inclusive of all Federal agencies). The Auditor General often makes reports not specifically targeting one agency but, rather, auditing spending in a specific area such as national security or protecting critical infrastructure.[313]

6.7.4 Observations

Big Data technology is in a state of rapid evolution and development. Risks and opportunities are not all evident or fully appreciated. Any rules that are designed may not be as enabling and balanced as hoped. An appropriate Big Data framework will therefore enable consistent, timely and holistic reviews of all relevant aspects of the framework to ensure that it delivers intended results efficiently and reliably, proportional to impacts on civil liberties, other legal rights and individual and commercial interests. There will also need to be more robust and comprehensive reviews to address the overall objectives of the system to ensure that the objectives are still valid and that they are achieved effectively, efficiently and proportionally in a manner that appropriately balances the interests of all stakeholders fairly.

The Australian, UK and Canadian framework provides a range of mechanisms that support the review of laws, regulations and practices. They are however not embedded as consistent, systemic and mandatory requirements. The mechanisms are generally ad hoc in nature and focused on specific elements. The assessment methodology also differs from mechanism to mechanism. Not all reviews engage the impact on civil liberties and on commercial interests. In addition, the government has not been consistently responsive to the results of these reviews.

While it would be relatively easy to improve technical review frameworks, it is important to retain sight of the relevance of public trust in both the framework and the review processes. The three enquiries leading to the reports that informed the Investigatory Powers Bill, involved varying levels of civil society participation. That, combined with the civil society engagement by Independent Reviewer of Terrorism Legislation, appear to have assisted in ensuring a broad level of public and political support for the Bill and, where support lacked, in increasing the clarity around policy questions and options.

6.8. Is there a sufficient measure of transparency?

Big Data tools, by adoption of algorithmic and machine learning methods, correlation and massive data sets to derive outputs, are difficult to make transparent to those affected by them. The concern for secrecy and protection of capability in this area, and the challenge of protecting the privacy of the other subjects covered by large data sets (and minimising 'honey pot' effects where knowledge of the content of such a set may provoke wider criminal interest in accessing it) pose additional challenges to transparency frameworks. These challenges informed the position taken by many research participants on transparency. Does the legal framework of the countries ensure, to the extent consistent with the need for operational secrecy, that the nature of data accessed, the analytic

[313]See Auditor General of Canada,' National Security in Canada' (March 2006); Auditor General of Canada, 'Protecting Canadian Critical Infrastructure Against Cyber Threats' (2012 Fall Report).

processes employed, and the right to access the data are as transparent as feasible for those potentially affected by decisions, and for those with an interest in policy- and rule-making?

6.8.1 Australia

In general, Australians are able to gain access to specific government data, subject of course to national security and operational confidentiality principles. The *Freedom of Information Act 1982 (Cth)* provides the statutory framework for open government in Australia and covers federal government ministers and most agencies. Under section 11 of the Act every person has a legally enforceable right to obtain access in accordance with the Act to a document of an agency or an official document of a Minister. This right is however subject to exemptions and exclusion under the Act and secrecy provisions in other laws and these limit the value of the *Freedom of Information Act* for purposes of transparency regarding Big Data and national security.[314]

The *Privacy Act 1988* has similar rights embedded in its *Australian Privacy Principles*.[315] These apply to 'personal information' rather than general information. However, the effect of these are limited, in a similar fashion, by the exemption or exclusion of many agencies from the oversight of the Principles and the *Privacy Act*, as discussed in section 6.2 above.

There are a significant number of sources of information available on data access and general management of data by government agencies for the purposes, as reflected in this paper. The above information is however generic rather than personal. If personal information is leaked in a government data breach, or otherwise mishandled, data subjects will not necessarily be informed and empowered to protect their rights[316] or act to mitigate impact on their interests. In case of data breach involving personal information, there is no mandatory obligation to provide information or notify persons affected, including breach of data of interest in this report.[317] A draft of data breach notification law was circulated for comment on 4 March 2016.[318] The exposure contains a number of restrictions that may render this regime of lesser relevance of the subject matter of this report, for example by

---

[314] See S 7 of the *FOI Act*, especially read with Schedule 2 to the Act. Also see section 2A that exempts an agency from the FOI Act in relation to a document that hat has originated with, or has been received from, any of the national intelligence agencies, DIO or IGIS. The exemption extends to a document that contains a summary of, or an extract or information from, such a document, to the extent that it contains such a summary, extract or information.

[315] See *Australian Privacy Principles* 1, 5, 10, 12 and 13.cSee the Schedule with APPs at <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html>.

[316] See eg, *SZSSJ v Minister for Immigration and Border Protection* [2015] FCAFC 125 (2 September 2015) <http://www.austlii.edu.au/au/cases/cth/FCAFC/2015/125.html>.

[317] See Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) 299. Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, 192. See Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) 295–296.

[318] Rohan Pearce, 'Draft data breach notification bill to be revealed soon,' *Computerworld* (online), 4 November 2015 <http://www.computerworld.com.au/article/588188/draft-data-breach-notification-bill-revealed-soon/>. See discussion of Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 <https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx>.

(cont.)

exempting entities already exempt from the *Privacy Act*, such as intelligence agencies, from the reporting requirements.[319]

6.8.2 United Kingdom

The importance of public transparency and the dual challenge of enhancing transparency while maintaining operational secrecy was recognised in all three 2015 reports that informed the *Investigatory Powers Bill*. The Intelligence and Security Committee of Parliament, for example, stated:

> … there is also a legitimate public expectation of openness and transparency in today's society and, while the Agencies require secrecy in order to conduct much of their work, the Government must make every effort to ensure that as much information as possible is placed in the public domain. This is essential to improve public understanding and retain confidence in the work of the intelligence and security Agencies.[320]

While tension between transparency and operational secrecy were highlighted, ways to align them in relation to national security was also identified. The Royal United Services Institute, for example, recognised that transparency and necessary secrecy are not incompatible, but rather that cultures of secrecy needed to be confined to operational activities where such secrecy is necessary and in the public interest and not extend to accountability and oversight mechanisms, ethical framework and policy documents, or as means to avoid accountability or hide mistakes.[321] This is consistent with Anderson's recommendation that *the operation* of covert powers remain secret while *intrusive capabilities and powers*, including their interpretation and justification, be made public.[322]

Increased transparency in relation to intrusive powers and capabilities is one of the features of the 2015 draft *Investigatory Powers Bill*.[323] The increased transparency was generally welcomed by the 2016 parliamentary reports, with the Intelligence and Security Committee

---

[319] A law enforcement body will also need to notify the Information Commissioner but will not have to notify affected individuals if it believes on reasonable grounds that such notification would be likely to prejudice enforcement-related activities conducted by, or on behalf of, the enforcement body. See eg, discussion of new ss 26WC(5) and 26WD(6) in Explanatory Memorandum for Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, AGD, undated, [12], [99] et seq, [120] et seq <https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Consultation-Draft-Exp-Memorandum-Privacy-Amendment-Notification-of-Serious-Data-Breaches-Bill-2015.pdf>.

[320] Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework (12 March 2015) Key Finding xix. See also RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 2.1, 5.29 and David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) ch 12.

[321] RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) paras 5.20, 5.21, 5.61, 5.62

[322] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) 8.

[323] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny Cm 9219 page 7.

(cont.)

a notable dissenter, expressing disappointment that the draft Bill did not go far enough.[324] In response, aspects of the draft Bill were clarified when the 2016 Bill was published.[325]

The *Investigatory Powers Bill 2016* increases transparency in one particularly significant respect: It requires the Investigatory Powers Commissioner to inform a person of any relevant error relating to that person of which the Commissioner is aware if the Commissioner considers that (a) the error is a serious error, and (b) it is in the public interest for the person to be informed of the error.[326]

In making a decision whether to notify a person, the Investigatory Powers Commissioner must, in particular, consider the seriousness of the error and its effect on the person concerned, and the extent to which disclosing the error would be contrary to the public interest or prejudicial to —

- national security,
- the prevention or detection of serious crime,
- the economic well-being of the United Kingdom, or
- the continued discharge of the functions of any of the intelligence services.[327]

Before coming to a decision, the Commissioner must ask the public authority which has made the error to make submissions to the Commissioner about the matters concerned.[328]

The Commissioner's annual report must disclose information regarding the number of relevant errors the Commissioner identified; the number that the Commissioner decided was serious errors and the number of persons notified that during that year.[329] Notified persons will be able to apply to the Investigatory Powers Tribunal for relief.[330]

6.8.3 Canada

The *Access to Information Act 1985* allows Canadians to make a request to access government data subject to secrecy and confidentiality principles (for example, where there is an ongoing investigation). Section 4 gives a right of access to data while section 6 governs requests for information that are under control of a government institution provided that the information requested is reasonably identifiable.

---

[324] Intelligence and Security Committee of Parliament Report on the draft Investigatory Powers Bill HC 795 (2016) 1: 'The draft Bill makes some attempt to improve transparency; however, the Committee is disappointed to note that it does not cover all the Agencies' intrusive capabilities. This failure to address the Committee's key recommendation means that various powers and authorisations remain scattered throughout different pieces of legislation. As a result, the draft Bill is handicapped from the outset in terms of the extent to which it can provide a clear and comprehensive legal framework to govern the use and oversight of investigatory powers. This is – in our view – a significant missed opportunity.' See also their comments at 10.

[325] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny Cm 9219 page 84.

[326] Cl 198(1) of the Investigatory Powers Bill 2016. For notification purposes a 'relevant error' means an error by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and of a description identified for this purpose in a code of practice under Schedule 7 of the Act. See cl 198(9) of the Investigatory Powers Bill 2016. The Investigatory Powers Commissioner is required to keep the definition of 'relevant error' under review.

[327] Cl 198(4) of the Investigatory Powers Bill 2016.

[328] Cl 198(5) of the Investigatory Powers Bill 2016.

[329] Investigatory Powers Bill 2016 cl 198(8).

[330] Investigatory Powers Bill 2016 cl 198(6).

(cont.)

The *Privacy Act 1985* allows an individual to make a request to ascertain what personal information a government institution is holding about them.[331] This is subject to a list of exemptions in sections 18 through 28 such as the prevention, detection or investigation of a crime and national security threats.[332]

There is no requirement for government organisations to notify an individual where their personal information is breached (eg accidental, deliberate or third party leak).

6.8.4 Observations

Information regarding the powers of NSLE agencies to access, share and analyse data, to the extent that it is available, is not easily accessible but must parsed from a large range of documents. Even then, it remains partial and general. The challenge is of course to ensure sufficiently operational secrecy while ensuring that sufficient transparency to ensure public trust and adequate protection of the rights of individuals.

The UK's move to greater transparency is an important development for Australian policymakers to follow. The recognition that transparency and necessary secrecy are not incompatible (as per the RUSI report), that secrecy should be confined to operational activities where such secrecy is necessary and in the public interest and that intrusive powers and capabilities, including their justification and interpretation (as per the Anderson); accountability and oversight mechanisms, ethical framework and policy documents should be public, would go a long to building public trust in the exercise of intrusive powers. As part of a more transparent framework it is also important to protect the rights of an individual that may have been harmed by a serious error.

[331] *Privacy Act 1985* s 12.

[332] *Privacy Act 1985* s 22.

7. CONCLUSION AND DRAFT RECOMMENDATIONS

Data technology holds great promise, also to support NSLE objectives. Increased collection, handling and analysis of data also hold risks, many of which may not yet have been identified, especially privacy and data security risks. Public confidence in the sensitivity with which NSLE objectives and concerns about the safety or individuals are aligned with concerns regarding other individual rights, will provide a policy environment supportive more extensive government collection and use of data. Such public confidence hinges on an appropriate policy, ethical, legal, and governance framework. This should include mechanisms to account for opportunities and risks in the evolving technological landscape, engage meaningfully with stakeholders and society, thereby enhance transparency and public accountability for policy decisions.

The Canadian empirical analysis showed that the absence of an appropriate regulatory framework can, in some circumstances, impede creative uses of data analytics. Despite few legal barriers to data sharing in Canada, technical barriers, a lack of institutional support, appropriate levels of trust and confidence in technology among users operate as barriers to the use of some technologies. It is thus important to recognise that regulation can enhance confidence in a data access regime and thus increase, as well as channel, appropriate data sharing.

In order to form the basis for further discussions as to the recommendations arising from this study, we have prepared a list of *draft* recommendations. This will be further refined following consultation, in particular with the Attorney General's Department.

In order to organise the recommendations, we have separated them under ten headings, focussing on the need to:

1. Engender public confidence in government use of data and analytic tools
2. Develop principles for data governance in NSLE agencies
3. Employ clear and consistent principles in developing legal frameworks
4. Improve processes to enhance effective use of data within NSLE agencies
5. Ensure the continued effectiveness of the oversight regime as technologies and NSLE agency practices evolve
6. Disentangle elements of technological change associated with 'Big Data'
7. Maintain data integrity and security in a high volume environment
8. Ensure fair and appropriate use of data analytics
9. Use appropriate systems for data matching, data integration or federated access that takes account of benefits and risks
10. Ensure efficient, appropriate and regulated sharing of specific data for NSLE purposes

There is, of course, overlap between these categories and it may be that, on further consultation, the categorisation of recommendations will evolve. However, we hope that this provides a useful conceptual starting-point.

In order to assist the Attorney-General's Department, we have used flags to indicate whether each recommendation:

- can be commenced or implemented relatively quickly (C)
- are part of a law reform exercise, that would need some additional planning and also findings from the first category of recommendations (LR)
- are ongoing, in the sense that they need to take place continuously, and should already be occurring (O)

The table below captures the timings of the recommendations that follow:

Timing of recommendation	Recommendation number
Can be commenced or implemented relatively quickly (C)	7.1(a), (c), 7.4, 7.5(c), 7.6, 7.7(b), (c), (d), 7.8 (c), (d), 7.9(b), (c)
Part of law reform exercise (LR)	7.2, 7.3, 7.5(b), 7.8(a), 7.10
Ongoing	7.1(b), (d), (e), 7.5(a), (d), 7.7(a), 7.8(b), (e), (f), 7.9(a)

7.1. Engender public confidence in government use of data and analytic tools

To support public confidence in government use of data and analytic tools, the following are advisable:

(a) The government should **provide opportunities for public debate and engagement around agency powers**, particularly in relation to 'bulk' access to personal data. The benefits of this are evident in the UK process leading up to the *Investigatory Powers Bill*. While not everyone agrees with the current Bill, and many NGOs remain opposed to aspects of the Bill, there is greater clarity as to the areas of disagreement, in relation to which there has been political compromise and ongoing discussion. **Public and stakeholder engagement should (C)**:

i. **Allow for airing of concerns around risks**. The Australian empirical study revealed differences in perceptions of risk among those working in different sectors.

ii. **Facilitate collaboration around the formulation of principles to underlie regulatory and ethical frameworks and their application**. Our draft principles are set out in the document entitled "High level policy principles on the use of Big Data analytics by national security and law enforcement agencies" but these should be subject to further discussion and debate.

iii. **Provide a platform for informing the public** on matters such as:
- the risks and opportunities of government use of data and analytics;
- the risks to privacy and data security from commercial exploitation of consumer data; and
- the protective mechanisms already embedded in legislation and agency procedures, including independent oversight, complaints mechanisms, audit trails, mandated action in the event of mistakes, training, assessment and compliance by design.

Improved information will help ameliorate any concerns that the media presents a distorted view of the risks of government data practices.

iv. **Faciliate discussion of government's data practices in support of NSLE**. This should be conducted in a way that provides an opportunity for individuals or organisations to articulate alternative viewpoints and propose practical solutions. It should also encourage the debate to move from a simplistic opposition of 'security' and 'privacy' to identifying ways in which both can be enhanced through innovative, collaborative thinking. Smaller, focussed engagement should be combined with larger scale platforms (such as on-line fora) and methodologically valid ways of assessing broader public opinion

(such as using specific and contextualised questions in representative sample surveys).

(b) **Big Data legal and technical frameworks should be regularly or continually reviewed**, with sufficient stakeholder and public engagement as described above, to ensure that benefits of and public trust in the operators and the operation of the system can be maximised while risks, including risks to data subjects, are comprehensively identified, subjected to evidence-based assessment where possible, and adequately mitigated. Where differences between stakeholders hinge on different assumed empirically provable facts (such as the effectiveness of particular techniques or the state of public opinion), these should where possible be investigated through independent research, at least where this can be done without compromising operational secrecy. Privacy Impact Assessments should also be conducted as relevant in relation to particular use-cases. (O)

(c) Public trust in the system should be supported through **transparency of intrusive powers and capabilities as well as control measures and accountability and oversight mechanisms, and confining secrecy to those aspects of operational activities where secrecy is necessary and in the public interest**. While the appropriate level of transparency will remain a subject of public debate, recent policy developments in the UK illustrate the benefits of increased transparency around agency powers concerning data access, although there is still some demand there for greater transparency as to the effectiveness of those powers for achieving NSLE objectives. The transparency and clarity of controls over arrangements to access data held by foreign governments and sharing of government-held data with foreign agencies should also be improved. (C)

(d) **Algorithmic transparency, at least to agency management and oversight bodies, is significant in facilitating accountability in decision-making and should be pursued despite practical difficulties**. These difficulties include the fact that software is often commercial-in-confidence, decision-makers lack sufficient training to understand the 'black box' algorithms embedded in software and machine learning can have emergent properties that are difficult to predict. These factors should be considered in selecting software products for particular uses and developing training programs for agency officers. Algorithmic transparency goes beyond Privacy Policies required of agencies bound by the *Privacy Act 1988* (Cth) in APP 1.4. (O)

(e) **Independent evaluation** of software (both outcomes and impacts) is crucial for maintaining public confidence in agency processes. This goes beyond technical evaluation, to incorporate evaluation against legal and ethical principles discussed in 7.2 below. In particular, where appropriate algorithmic transparency remains unattainable, independent evaluation of software is one way to preserve accountability of decision-making. Sufficiently resourced (see 7.5), oversight bodies would be the appropriate institutions to fulfil this role. (O)

7.2. Develop principles for Big Data governance in NSLE agencies (LR)

(a) **Legal, policy and technology experts need to work together, incorporating insights from public engagement, to develop and articulate principles**:

i. **to guide the regulation, implementation, governance and oversight of data-based decision-support technologies to facilitate the achievement of NSLE**

objectives. This should consider issues at all stages of the data cycle. For example, some risks may be better managed by restricting how data can be used, what actions can be taken, or how long it can be retained, rather than limiting data disclosure *ex ante*, while in other cases, risks may be better managed by limiting initial data collection or disclosure.

ii. **to inform an ethical code for data collection, access, sharing, use, retention and deletion (elements of the 'data cycle') by NSLE agencies and their employees**.

iii. **to guide design of technological systems and tools**, especially reflecting the use of technology to mitigate risks and increase trust. This should ensure appropriate deployment of compliance/privacy/security-by-design principles. Particular mechanisms include comprehensive logging, auditing and record-keeping (see also 7.9, 7.10 below).

(b) Draft high level principles are set out in a separate document entitled "Draft high level policy principles on the use of Big Data analytics by national security and law enforcement agencies". As noted in recommendation 1(a)(ii), these are preliminary and should be subject to further public and stakeholder engagement.

7.3. Employ clear and consistent principles in developing legal frameworks (after 7.2 Principles are finalised) (LR)

As described in the Australian and Comparative Reports, the current legal framework in Australia is fragmented along several lines, including by agency and dataset. While some differences are justified, these should be based on clear principles that differentiate only according to risk level and other relevant factors. This is particularly important given differences among Australian research participants as to the extent to which perceived legal barriers were based on overly cautious interpretations of current legislation.[333] A clear set of principles that apply as consistently as possible across agencies would help clarify legal obligations and ensure a common understanding as to the circumstances in which data can be shared. In addition to recommending the development of such principles (7.2), we also make specific recommendations concerning clarity and consistency:

(a) **Data-related terminology used in legislation should be both consistent and minimalistic**. For example, distinctions currently made between 'data' and 'information' are increasingly impractical and definitions offered (where they are offered) are diverse with overlapping meanings. Consistent terminology, capturing only relevant distinctions, should be applied across all policy, legislation, rules and guidelines.

(b) As suggested by the OAIC,[334] **agencies collecting and using data should develop and implement policies to clarify the application of relevant secrecy laws to their information holdings.**

(c) There needs to **be greater clarity around what individual 'consent', where required, entails in the context of data collection**. Research participants used a range of terms to describe what would constitute appropriate consent (in situations where consent is required) including that consent be meaningful,

[333] A similar point was made by OAIC in its submission on the Productivity Commission's Issues Paper regarding the National Education Evidence Base in June 2016.
[334] Ibid.

informed, freely given and revocable. Such clarity is in addition to the need to consider the matters raised in 7.2(b)(vi). For those agencies bound by the *Privacy Act 1988* (Cth), consent is particularly relevant for APPs 3.3, 3.4(d) (collection of sensitive information), APP 3.6 (collection of personal information), APP 6.1 (use or disclosure for secondary purposes)

7.4. Improve processes to enhance effective use of data within NSLE agencies (C)

(a) **Enhance agency co-operation by addressing cultural barriers to sharing data, while recognising the continued importance of legal and operational restrictions.** There is no easy solution to overcoming cultural reluctance to co-operate with other agencies with diverse missions in terms of access to data. However, providing opportunities for cooperation for example through structures such as combined operations and fusion centres, a clearer legal framework (discussed below), legislative encouragement for data sharing (as in Canada), training and education around the applicable legal rules, support and resources for relevant officers, and smoother technical processes, may assist.

(b) **Provide training to relevant agencies to explain and reduce the problem of 'over-classification'** in the context of effective inter-agency communication about threats. This should recognise both the risk of information leaks and the concern that intelligence silos may limit threat assessment capacity in relevant agencies.

7.5. Ensure the continued effectiveness of the governance and oversight regime as technologies and NSLE agency practices evolve

(a) Ensure that **managers in NSLE agencies understand the opportunities and risks of new systems and tools** and are able to exercise appropriate managerial control. This may involve leadership by a particular officer within the agency.[335] (O)

(b) Ensure **appropriate, seamless independent oversight** of the whole data universe that is relevant to Big Data usage by NSLE agencies, including automated data analysis. While many research participants were positive about current oversight mechanisms, some referred to multiple overlapping processes and the possibility of better streamlining to avoid 'red tape' and unnecessary duplication without reducing oversight. This requires consideration of both technological design and legal frameworks. (LR)

(c) As NSLE agencies acquire new systems and tools, as well as enhance their analytic capacities, **oversight agencies will also require resources, particularly technical and technically trained human resources**, to increase their ability to monitor new, more complex, uses of data and data analytics within NSLE agencies. Oversight agencies will need to understand systems being sued within NSLE agencies in order to ensure that safeguards are sufficient, particularly where systems are interlinked or data availability is increased. (C)

(d) **The judiciary also plays an important role in regulating the collection and use of data by NSLE agencies**, in particular through issuing warrants, admitting evidence and determining the lawfulness of particular practices in cases brought to court. As the current political debate in the UK makes clear, the role of judges in assessing the

[335] See also OAIC, Guide to big data and the Australian Privacy Principles: Consultation draft (May 2016) p 7.

necessity and proportionality of surveillance and other intrusive powers for NSLE purposes (as part of the process of procuring certain categories of warrant) can engender public trust that such powers will be used appropriately. (O)

7.6. Disentangle elements of technological change associated with 'Big Data' (C)

This project began with the task of exploring perceptions regarding Big Data and appropriate frameworks for the use of 'Big Data' for NSLE. However, a literature review combined with interviews in Australia soon revealed that the term 'Big Data' captures a range of relevant technological developments, each of which raises distinct technical, legal and policy issues. In particular:

(a) **Increasing data volume:** In building technical infrastructure to ingest and handle increasing volumes of data, it is important to build in design elements, regulations, and agency processes to ensure data security and data integrity. See 7.7.

(b) **Analytic capacity:** New data science techniques offer new ways of knowing and predicting based on analysis of sufficiently large data sets. However, decision-making based on inferences drawn from large data sets needs to bear in mind that, generally speaking, what is revealed is based on correlation rather than causation. In light of this, it is important to ensure that those affected negatively by decisions based on such analysis are treated fairly. In addition, it is important for user agencies to be involved in determining the balance between false positives (requiring resources and impacting individuals) and false negatives (unknown threats). See 7.8.

(c) **Data matching, data integration and platforms for interrogating federated data:** The possibility of integrating disparately held datasets was an important aspect of 'Big Data', particularly for those working in operational organisations. There are diverse technological means for enabling NSLE agencies to analyse data currently held in separate agencies or systems. These are associated with different levels of risk in terms of data integrity (including integrity in 'matching' data) and data security. Whether by accident or design, data 'silos' provide protections for data privacy and data security at the same time that they can compromise efficient intelligence-gathering and impede investigations. See 7.9.

(d) **Efficient mechanisms for data sharing between agencies:** Our empirical research revealed that the mechanisms for disclosing data between agencies are currently *ad hoc*, sometimes depending on trust built up between individual officers and often involving slow, manual and analogue processes. While in some instances the solutions discussed above in (c) are appropriate, data sharing will often continue to be conducted on a case-by-case basis. This will apply for example to situations where specific authorisations or warrants are required as well as in the context of sharing with international partners. Nevertheless, technology platforms could make the process of sharing specific data, and recording relevant authorisations, more efficient. This will require legal frameworks and technological design to work in combination to ensure that data is only shared where it is appropriate to do so. See 7.10.

While this project explored the category of 'Big Data' broadly, some legal and policy issues associated with different aspects of 'Big Data' practices ought to be considered separately. Legislation, in particular, will require more precise terminology. For example, in the UK, terminology such as 'bulk personal dataset' is defined and used in the *Investigatory Powers Bill 2016* primarily in the context of establishing a legislative framework for (d) above.

7.7. Maintain data integrity and security in a high volume environment

As more data is captured, held within and shared with and by NSLE agencies, questions of data integrity and data security become increasingly important. As described earlier in this report, Australia already has a range of data integrity and security measures in place. For example, agencies bound by the *Privacy Act 1988* (Cth) must comply with APPs 10, 11 and 13. However, more can be done to support and enhance data accuracy and protect individuals whose personal data is held (which in many cases includes 'everyone'):

(a) **Carefully evaluate the need for collecting and holding large volumes of data**, taking account of both the NSLE and other benefits (in particular the potential of data as an evidence base for strategic decision-making) as well as the potential negative impact on privacy, data integrity, data security and agency resources. While data analytics increases the usefulness of data, data should not be collected or retained where it serves no useful purpose. In particular, data deletion is an important component of the data cycle that should be properly captured in 7.2. Agencies bound by the *Privacy Act 1988* (Cth) will already be bound by APP 3 and 4 in relation to collection of personal information. (O)

(b) Develop a **clear concept of 'data integrity' and effective and well-understood data integrity measures**. While these should apply across all government-held data, particular care is required when designing systems for data matching, data integration or federated data access (see 7.9 below). (C)

(c) **Augment existing data security standards** with clear data collection, usage and retention minimisation principles that can be applied in a Big Data environment. Measures adopted in the UK may be a useful benchmark against with Australian standards can be compared. (C)

(d) Consider the **circumstances in which 'open source' data, particularly if imported in bulk, should be retained for statutory limits** when no longer required by the agency concerned for a specified purpose, particularly where personal data is captured. Some concern was expressed in the Australian empirical study that the rules around this are currently unclear, particularly in the context of agencies' increasing use of high volume, high velocity social media data. (C)

7.8. Ensure fair and appropriate use of data analytics

Data analytics opens up new possibilities for drawing inferences about individual preferences and propensities and group dynamics from large volumes of data. This can have a positive impact on decision-making, both within the context of NSLE, but also across government more generally. However, without a complete understanding of the assumptions underlying data-supported inferences, and the choices and preferences embedded within the 'black box' algorithms, decisions may be less fair or less appropriate than they would otherwise. The use of sophisticated analytic tools to enrich decision-making (whether at the level of a particular investigation or at the level of strategic decision-making) is enhanced and associated risks reduced if the following recommendations are adopted:

(a) **Develop appropriate safeguards** to ensure the integrity of automated processing of data, automated decision-taking and data-based decision-support tools. In the context of decisions with potential significant negative impact, it may be crucial to retain a human-in-the-loop rather than fully automating the implementation of a decision. In other contexts (such as speeding cameras), it may be sufficient to provide appropriate mechanisms to challenge an automated decision. (LR)

(b) Ensure that there is a **common understanding between technology users and designers** as to how tools will be used, and the ways in which they may impact on operational priorities and strategies. This goes beyond questions of technical function, to include agency approaches – for example, whether the tool will facilitate a more pro-active or trend-based approach to achieving the agency's mission. (O)

(c) Explore ways in which de-identified or trend data can be used within agencies for **evidence-based strategic decision-making and program evaluation**, without compromising the privacy of identifiable personal information.[336] *De-identified aggregated* data (subjected to initial and subsequent testing for re-identification potential, recognising that risk of re-identification increases over time) may be able to be released to the public for research or advocacy purposes, as is done in the UK. However, this requires a realistic, and evolving, understanding of re-identification risk. (C)

(d) **Ensure appropriate alert management in the deployment of alert-generating systems**. Technical and human resources should be deployed in a way that avoids 'overload' that can compromise an agency's ability to achieve core objectives. In particular, tools for generating alerts should limit outputs to those that can be managed by an agency or prioritise alerts (based on criteria determined in consultation with users) so that agencies can focus on high priority threats. NSLE agencies, as well as the agencies and officers that oversee them, will need appropriate technical and human resources to carry out new activities and respond to threats identified by automated and semi-automated systems. (C)

(e) Those making decisions on the basis of inferences drawn from data analytics should receive **sufficient training** in order to understand, broadly, the assumptions underlying those inferences and the limitations of the data analytic technique employed. This includes ensuring decision-makers understand the limitations of relying on historical correlation in formulating proposed actions and interventions. Further, decision-makers should be made aware of the extent to which data collected and stored *may* be incomplete or biased. For example, crime data *may* show more offences within communities with an existing higher police presence. Where relevant, any such limits and assumptions should be taken into account in formulating both strategic and investigatory responses. Such training should also cover ethical principles developed in 7.2(a)(ii). (O)

(f) The **balance between false positives and false negatives** needs to be set with a close eye to organisational, individual and social harms caused by each. For rare, high-impact events (such as terrorism), most approaches generate high, often unworkable, rates of false positives. False positives can stretch agency resources and, in many circumstances, negatively impact on individuals. These may hold negative consequences for an individual (for example, inclusion on a 'no fly' list). Careful thought must be given to a mechanism that would appropriately protect the rights of individuals affected by errors, where possible by informing such individuals and giving them an opportunity to respond. Any such mechanism should, of course, also allow for a weighing of individual rights against operational considerations and the broader public interest. False negatives can also have significant broader consequences, as where a threat is not identified before it materialises. (O)

---

[336] See also OAIC, Guide to big data and the Australian Privacy Principles: Consultation draft (May 2016) pp 4-6

7.9. Use appropriate systems for data matching, data integration or federated access that takes account of benefits and risks

As discussed in 7.6(c) above, in some circumstances it will be appropriate to bring data together 'in bulk'. There are a variety of different tools and systems through which this can be achieved from a technical standpoint. These are associated with different operational advantages, technical challenges and risks, particularly to privacy and security of personal data. We therefore suggest:

(a) A decision to combine data, or enable federated access to separately held data, should be informed by an assessment of the operational impacts and risks of each of these, as against the alternative of maintaining fully separated storage and access facilities. For example, a federated system of access (appropriately designed to prevent bulk access) may reduce security risks associated with storing high volumes of valuable data while promoting efficiencies. Decisions as to the appropriate tool or system, as well as the legal and regulatory framework around it, should take account of the principles developed in 7.2. In some cases, there will be advantages to full or partial siloing of data, and the term should not be given an overly negative connotation. A preferential term may be 'purpose-specific record systems' which are supported by the OECD and Australian Privacy Principles. (O)

(b) New technical solutions need to be able to **manage legacy issues**, including challenges of locating and extracting data from historic databases and accessing historical data in older formats. (C)

(c) **Where separate purpose-specific record systems are maintained, enhance technical consistency and inter-operability** through government technical standard-setting processes. (C)

7.10 Ensure efficient, appropriate and regulated sharing of specific data for NSLE purposes (LR)

As discussed in 7.6(d) above, much data sharing is highly curated, requiring warrants, specific authorisations or careful consideration. While the kinds of technologies discussed in 7.6(c) and 7.9 above are not appropriate here, there are tools and systems that can improve efficiency, ensure and track compliance, log activities, provide an audit trail, protect data integrity and security and detect breaches and misuse. Appropriate technology, combined with a clear, appropriate and principles-based legal framework, can ensure efficient data sharing while providing important protections and maintaining public confidence. Many of these issues are addressed above. In addition, there is much Australia can learn from the recent UK debates around particular legal protections (in particular, debates around and evolution of the 'double lock' mechanism) in formulating its own legal framework.