AUSTRALIA 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, 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

Australia Report

Authors

Chapter 1: The Australian Legal Context

1.1-1.4: Louis de Koker

1.5-1.6: Danuta Mendelson

Chapter 2: Using Big Data for National Security: Stakeholders' Perspectives

2.1-2.4: Janet Chan

2.5-2.6: Lyria Bennett Moses

Chapter 3: Big Data, Law Enforcement and National Security: The Legal Environment in Australia

3.1. Is access for data mining enabled? Louis de Koker; Observations Lyria Bennett Moses, Louis de Koker

3.2. Are legal controls comprehensive and proportional? Danuta Mendelson; 3.2.3 Danuta Mandelson, David Vaile; Table 3.1 David Vaile, Alana James; 3.2.9 David Vaile; Observations Lyria Bennett Moses, Louis de Koker; Concluding Observations Danuta Mendelson

3.3. Are legal rules clear, principle-based, consistent and instructive Louis de Koker; 3.3.1 Louis de Koker, David Vaile; Table 3.2 David Vaile; 3.3.2 Lyria Bennett Moses; Observations Lyria Bennett Moses, Louis de Koker

3.4. Is integrity of data and analysis supported? Louis de Koker; Observations Lyria Bennett Moses, Louis de Koker

3.5. Are data and systems protected? Louis de Koker; Observations Lyria Bennett Moses, Louis de Koker

3.6. Is accountability maintained? Louis de Koker; Observations Lyria Bennett Moses, Louis de Koker

3.7. Are principles and rules regularly reviewed? Louis de Koker; Observations Lyria Bennett Moses, Louis de Koker

3.8. Is there a sufficient measure of transparency? Louis de Koker; Observations Lyria Bennett Moses, Louis de Koker, David Vaile

Chapter 4: Conclusion

4.1: Lyria Bennett Moses, Janet Chan

4.2: Louis de Koker, Lyria Bennett Moses; 4.2.2 Danuta Mendelson

Interviews

Lyria Bennett Moses, Alana Maurushat, Janet Chan, Louis de Koker

Qualitative analysis

Lyria Bennett Moses, Janet Chan

Research assistance

Mr Daniel Cater

Technical editing

Mr David Vaile

Other Reports from this Project

Methodology Report

UK Report

Canada Report

Comparative Report

Select Bibliography

Technical References [for Australia Report]

Contents

List of tables

List of Figures

.

1. THE AUSTRALIAN LEGAL CONTEXT

This chapter introduces the broad contours of the discussion regarding Big Data and national security in Australia. It provides an overview of the key agencies and discusses the agency focus of this study.

1.1. Intelligence and national security – contours of the policy discussion

Australia's discussion of Big Data, national security and law enforcements is driven by concerns common to the members of the Five Eyes intelligence community: terrorism, radicalisation and organised crime.

While Australia has experienced various instances of politically-related violence during the course of the 20th century,[1] concerns became elevated after the Bali bombing that killed 202 people including 88 Australians.[2] These concerns were recently increased with reference to 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.[3] These concerns are major drivers of the national security agenda.

In addition to terrorism and radicalisation, law enforcement agencies are also concerned about organised crime. Organised crime is responsible for a range of sophisticated crimes, including cybercrime.[4] Organised crime and terrorism concerns are also linked in the policy debate. The Australian Crimes Commission remarked as follows in *Organised Crime in Australia 2015*:

> As counter-terrorism efforts throughout Australia are enhanced, the linkages between terrorism and the broader organised crime and volume crime environments are being identified. These linkages include, but are not limited to, Australians who finance terrorist activities, Australians who leave Australia to support terrorist causes, and who may return to Australia with the intent of inflicting harm on the Australian community, or Australians who may be recruited by organised crime groups seeking the specialist skill sets they developed in foreign conflicts. [5]

Intelligence and law enforcement powers to access data relating to security and law enforcement threats are regulated by a complex collection of rules. Part of the complexity stems from Australia's federal constitutional structure that positions national intelligence at a federal level and policing at both a federal and a state and territory level. Significant complexity also arises from mechanisms that are designed to protect privacy of individuals

---

[1] Department of Prime Minister and Cabinet, *Counter Terrorism White Paper: Securing Australia – Protecting Our Community* (Department of Prime Minister and Cabinet, 2010) 7.
[2] Department of Prime Minister and Cabinet, *Counter Terrorism White Paper: Securing Australia – Protecting Our Community* (Department of Prime Minister and Cabinet, 2010) 10.
[3] 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>.
[4] Australian Crime Commission, *Organised Crime in Australia* (2015) 2 <https://www.crimecommission.gov.au/publications/intelligence-products/organised-crime-australia/organised-crime-australia-2015>.
[5] Australian Crime Commission, *Organised Crime in Australia* (2015) 1 <https://www.crimecommission.gov.au/publications/intelligence-products/organised-crime-australia/organised-crime-australia-2015>.

and to safeguard operational confidentiality of agencies as well as secrecy of state information relevant to national security. Many of the information sharing rules were adopted before the development of current communication and analytic technologies, and may not operate clearly and appropriately in the current and future data landscape.

This study was informed in part by an inquiry of the Parliamentary Joint Committee on Law Enforcement into Criminal Intelligence. The inquiry considered proposals for a criminal intelligence system that could provide a comprehensive national picture of organised crime in Australia and especially the establishment of an Australian Criminal Intelligence Model for the Australian Crime Commission and its counterpart agencies. This inquiry is of even greater significance following the 5 November 2015 announcement that CrimTrac and the Australian Crime Commission (discussed in greater detail in 3.1) would be merged into a new criminal intelligence agency that will be operative from 1 July 2016.[6] The Committee's 2013 report *Inquiry into the Gathering and Use of Criminal Intelligence* provides the following summary of the criminal intelligence landscape in Australia:

> This inquiry has brought to light serious legislative, technological, resource and cultural impediments to the flow of intelligence which produce unequal intelligence holdings, an incomplete picture of criminal threats and undermine stakeholder confidence. Some law enforcement agencies hold reservations about sharing their own information and seem not to recognise the value added to that information when converted into intelligence and returned to them. Such concerns are exacerbated by the absence of a common approach to collecting, collating, analysing and disseminating criminal intelligence underpinning a common ethos. Efforts to establish an interoperable criminal intelligence system capable of producing a comprehensive national picture of organised crime are hindered for these reasons. [7]

Frustration with the current system was also evident in the interviews conducted as part of this study, both in terms of the piecemeal nature of current legal rules and the common reluctance to share intelligence.[8] Key stakeholders appreciate however that the goal cannot be to simply remove all impediments to the 'flow of intelligence'. Many of the rules were developed with care to reflect the rights of all concerned and to ensure that access to information is appropriately restricted, for example either according to classification level or to those who 'need to know'.[9] The challenge is rather to re-consider existing rules in view of new technological capacities, to ensure that rights are appropriately balanced.

1.2. National intelligence and law enforcement agencies

As the report often refers to specific national intelligence and law enforcement agencies a brief overview of the most relevant agencies is provided. While the terms 'national intelligence agencies' and 'law enforcement agencies' are generally used to distinguish between intelligence agencies and police services that may also have a criminal intelligence function, this is simply a working classification. The classification is used in legislation but

---

[6] Michael Keenan (Minister for Justice), 'New Super Agency to Tackle Emerging Threats' (media release, 5 November 2015).
[7] Parliamentary Joint Committee on Law Enforcement, Parliament of Australia, *Inquiry into the Gathering and Use of Criminal Intelligence* (2013) ix.
[8] This is evident in some of the research participants' statements in the interviews. See especially 2.2, 2.4.5K and 2.5.4.
[9] See especially 2.5.4I and 2.6.4.

membership of these categories is not fixed. Some agencies classified as a 'law enforcement agency' in one Act may not be included in that category in another Act.[10]

1.2.1. Key law enforcement agencies

Law enforcement in Australia occurs at a Federal and State and Territory level.

At a federal level the policing powers are entrusted to the Australian Federal Police (AFP) The AFP was established in 1979, mainly as a result of the Sydney Hilton hotel bombing and the identification of a need to have a federal agency that can combat crime at a national level.[11] The AFP provides police services in relation to laws of the Commonwealth; property of the Commonwealth (including Commonwealth places) and of authorities of the Commonwealth; and safeguarding of Commonwealth interests. It also investigates State offences that have a federal aspect.[12] In general,[13] States and Territories enforce State and Territory laws in their own jurisdictions.

The Australian Crime Commission (ACC) was established in 2003 as Australia's national criminal intelligence agency with specialist investigative capabilities. It works nationally and in partnership with Commonwealth, state and territory law enforcement and key national security and regulatory agencies, to combat nationally significant crime, including organised crime.[14]

1.2.2. Key national security agencies

The national security agencies were generally established in the mid-20th century.[15] The agency-related legislation has been subject to a number of inquiries and independent reviews, including two Royal Commissions conducted by Justice Robert Hope in 1974 and 1983,[16] the Samuels and Codd Royal Commission in 1995;[17] the 2004 Philip Flood Report Inquiry into Australian Intelligence Agencies[18] and the *Independent Review of the Intelligence Community* in 2011 by Robert Cornall and Rufus Black.[19]

---

[10] See 3.3 below.
[11] Australian Federal Police, *History of the AFP* <http://www.afp.gov.au/about-the-afp/our-organisation/history>.
[12] *Australian Federal Police Act 1979* (Cth) s7.
[13] Subject to arrangements, the AFP is also responsible for providing police services in the Australian Capital Territory and it is charged with similar responsibilities in Jervis Bay Territory.
[14] See 3.1 for a more detailed profile of the ACC.
[15] For the history of these agencies, see Parliament of Australia, *Intelligence Services Bill,* No 11 of 2001-02, 1 August 2001 <https://www.aph.gov.au/binaries/library/pubs/bd/2001-02/02bd011.pdf>, 2–3, 6.
[16] The first Hope Royal Commission delivered eight reports. Four of these were tabled in Parliament on 5 May 1977 and 25 October 1977. The report resulted in the adoption of the *Australian Security Intelligence Organisation Act 1979*, the establishment of the Office of National Assessments (ONA) and the passage of the *Office of National Assessments Act 1977*.
[17] Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service* (public edition) (1995).
[18] Philip Flood, *Report of the inquiry into Australian intelligence agencies* (*Flood report*) (Commonwealth of Australia, 2004) <http://apo.org.au/report-inquiry-australian-intelligence-agencies-flood-report>.
[19] Robert Cornall and Rufus Black, *2011 Independent Inquiry of the Intelligence Community* (Commonwealth of Australia, 2011) http://www.dpmc.gov.au/pmc/publication/2011-independent-review-intelligence-community.

Six agencies make up the Australian Intelligence Community:

Two are agencies responsible for collecting intelligence from human sources:

- Australia's domestic intelligence agency, **Australian Security Intelligence Organisation (ASIO**), was established in 1949. It operated on an executive basis until the adoption of the Australian Security Intelligence Organisation Act 1956, since repealed and replaced by the Australian Security Intelligence Organisation Act 1979.
- Australia's foreign intelligence service, **Australian Secret Intelligence Service (ASIS)**, was established 1952. Its establishment and operation was kept secret for two decades, even from members of the Australian Government.[20] ASIS is one of the intelligence agencies that operate under the Intelligence Services Act 2001.

One is an intelligence assessment agency:

- **Office for National Assessments (ONA)** was established by the Office of National Assessments Act 1977. ONA is tasked with assembling and correlating information relating to international matters that are of political, strategic or economic significance to Australia and to prepare reports on and make assessments in relation to those matters that are of national importance. ONA also coordinates Australia's foreign intelligence activities.[21]

Three agencies form part of the Defence Strategic Policy and Intelligence Group in the Department of Defence:[22]

- **Defence Intelligence Organisation (DIO**), the Australian source of expertise for matters relating to global security, weapons of mass destruction, foreign military capabilities, defence economics and transnational terrorism;
- **Australian Geospatial-Intelligence Organisation (AGO)**, the provider of geospatial intelligence from imagery and other sources, in support of Australia's defence and national interests; and
- **Australian Signals Directorate (ASD)**, that provides foreign signals intelligence to the Defence Force and Australian Government to support military and strategic decision-making.

While these agencies are generally viewed as the key Australian law enforcement and intelligence agencies they operate in a broader agency and government context. In different listings the membership of the cluster of the law enforcement and intelligence is defined differently. The government for example presents a list of Australia's national security agencies and authorities as presented in Table 1-1.[23]

---

[20] Nick Warner, *ASIS at 60* (19 July 2012) ASIS Foreign Intelligence <https://www.asis.gov.au/About-Us/Speech.html>.

[21] *Office of National Assessments Act 1977* (Cth) s 5.

[22] See Australian Government Department of Defence, *Defence Strategic Policy and Intelligence Group* < http://www.defence.gov.au/SPI/>. For the position prior to 8 February 2016 see Defence Intelligence and Security Group, *Defence Intelligence and Security Group agencies*, Australian Government Department of Defence <http://www.defence.gov.au/isg/>.

[23] Australian Government, *National security agencies,* Australian National Security <http://www.nationalsecurity.gov.au/WhatAustraliaisdoing/Pages/NationalSecurityAgencies.aspx>.

Table 1-1: Australia's national security agencies and authorities (as per the government)

Agency/Department/Functionary	General function
Prime Minister	Lead role in Australian Government counter-terrorism policy coordination
Department of the Prime Minister and Cabinet	Coordinates Australian Government counter-terrorism policy in collaboration with intelligence agencies and the states and territories, advises the Prime Minister on matters related to counter-terrorism and provides the secretariat for: • Secretaries Committee on National Security; • National Security Committee of Cabinet; and • Australia-New Zealand Counter-Terrorism Committee (ANZCTC) (which it co-chairs)
Office of National Assessments (ONA)	Assesses and analyses international political, strategic and economic developments for the Prime Minister and senior ministers in the National Security Committee of Cabinet
Attorney-General	Supported by the National Security Committee of Cabinet and other ministers, provides operational coordination on national security issues
Attorney-General's Department	Coordinates national security and crisis management arrangements and provides legislative advice.
Australian Federal Police (AFP)	Investigates national terrorist offences, provides overseas liaison and protective services and performs a state policing function in the ACT
Department of Immigration and Border Protection	Responsible for immigration and customs border policy
Australian Border Force	New front-line operational agency within Department of Immigration and Border Protection to manage the security and integrity of Australia's borders
Border Protection Command	Provides security for Australia's offshore maritime areas
Australian Secret Intelligence Service (ASIS)	Australia's overseas secret intelligence collection agency
Australian Security Intelligence Organisation (ASIO)	Australia's national security intelligence service
Australian Defence Force	Maintains capabilities that can assist civil authorities in emergencies
Department of Foreign Affairs and Trade (DFAT)	Advances the interests of Australia and Australians internationally
Department of Health	Leads a whole-of-government approach to strengthening Australia's readiness for disease threats, national health emergencies and other large scale health incidents
Department of Infrastructure and Regional Development	Regulates the security of airports, airlines, sea ports and other forms of transport, with state and territory authorities

Summarised and paraphrased from Australian Government, *National security agencies,* Australian National Security <http://www.nationalsecurity.gov.au/WhatAustraliaisdoing/Pages/NationalSecurityAgencies.aspx>.

Legal drafters have also been challenged to define this cluster. The phrase 'law enforcement or security agency' is defined in section 4 of the *Independent National Security Legislation Monitor Act 2010* as follows:

(a) the Australian Federal Police;
(b) the Australian Crime Commission;
(c) Customs;
(d) the Australian Security Intelligence Organisation;

(e) the Australian Secret Intelligence Service;
(f) the Australian Defence Force;
(g) the part of the Defence Department known as the Australian Geospatial-Intelligence Organisation;
(h) the part of the Defence Department known as the Defence Intelligence Organisation;
(i) the part of the Defence Department known as the Australian Signals Directorate;
(j) the Office of National Assessments established by the *Office of National Assessments Act 1977;*
(k) the police force of a State or Territory;
(l) any other agency prescribed by the regulations for the purposes of this definition.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* governs, among others, access by a range of agencies to the financial intelligence held by the Australian Transaction Reports and Analysis Centre (AUSTRAC) (see 3.1). The agencies listed in this Act are indicative of agencies that have a law enforcement or integrity function requiring access to data on financial transactions of Australians. The Act includes as 'designated agencies' those listed in section 4 of the *Independent National Security Legislation Monitor Act 2010* as well as entities such as the Australian Commission for Law Enforcement Integrity; the Australian Competition and Consumer Commission; Australian Securities and Investments Commission; as well as a Commonwealth Royal Commission whose terms of reference include inquiry into whether unlawful conduct (however described) has, or might have, occurred.

1.3. Selection of agencies and laws for purposes of this study

Lists of agencies such as those set out 1.2 provide helpful perspectives on the agencies and functions that are classified as law enforcement and national security agencies in Australia. For purposes of this comparative study, however, it was important to ensure an appropriate focus. Some additions were also necessary. A number of data collecting agencies that support law enforcement and intelligence and that are therefore highly relevant to the Big Data focus of this study do not feature by name on these lists. These include the Australian Tax Office, CrimTrac and AUSTRAC.

To ensure a sufficiently representative coverage of the national security and law enforcement Big Data landscape in Australia, it was therefore decided to focus on the laws regulating the following agencies, including the oversight mechanisms in relation to these agencies:

Intelligence agencies

- Australian Security Intelligence Organisation
- Australian Secret Intelligence Service
- Australian Geospatial-Intelligence Organisation
- Australian Signals Directorate
- Defence Intelligence Organisation
- Office of National Assessments

Crime intelligence and law enforcement agencies

- Australian Federal Police
- Australian Crime Commission

Agencies sharing data with intelligence and/or law enforcement agencies

- Australian Tax Office
- AUSTRAC

- CrimTrac

In addition to agency-focused laws, general laws such as telecommunications laws and the *Privacy Act 1988* were also identified given their relevance to data in the Big Data questions.

While the study focused on the relevant laws the potential impact of other legislation such as the *Criminal Code Act 1995*, *Public Service Act 1999*, *Financial Management and Accountability Act 1997*, *Public Governance, Performance and Accountability Act 2013* were also considered. Table 1-2 provides a complete list of all the agencies and oversight bodies included in this study.

Table 1-2: Federal national security and law enforcement agencies studied

Name	Acronym	Governing Act	Portfolio	Minister	Agency-specific independent oversight body[24]
Australian Crimes Commission	ACC	*Australian Crimes Commission Act 2002*	Attorney-General	Minister for Justice	
Australian Federal Police	AFP	*Australian Federal Police Act 1979*	Attorney-General	Minister for Justice	
Australian Geospatial-Intelligence Organisation	AGO	*Intelligence Services Act 2001*	Defence	Minister of Defence	Inspector-General of Intelligence and Security
Australian Security Intelligence Organisation	ASIO	*Australian Security Intelligence Organisation Act 1979*			Inspector-General of Intelligence and Security
Australian Secret Intelligence Services	ASIS	*Intelligence Services Act 2001*	Foreign Affairs	Minister of Foreign Affairs	Inspector-General of Intelligence and Security
Australian Signals Directorate	ASD	*Intelligence Services Act 2001*	Defence	Minister of Defence	Inspector-General of Intelligence and Security
Australian Tax Office	ATO	*Tax Administration Act 1953*	Treasury	Treasurer	Inspector-General of Taxation
Australian Transaction Reports and Analysis Centre	AUSTRAC	*Financial Transaction Reports Act 1988; Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)*	Justice	Minister for Justice	
CrimTrac		Operates in terms of an Intergovernmental Agreement, supported by a Memorandum of Understanding	Justice	Minister for Justice	
Defence Intelligence Organisation	DIO	Not functioning under own Act, recognised in s 29 of *Intelligence Services Act 2001*	Defence	Minister of Defence	Inspector-General of Intelligence and Security
Office of National Assessments	ONA	*Office of National Assessments Act 1977*	Prime Minister & Cabinet	Prime Minister	Inspector-General of Intelligence and Security

1.4. Terminology

While the researchers were able to navigate the lack of consistency in the categorisations of law enforcement and security agencies by selecting key agencies (see 1.2 and 1.3 above), the lack of consistency in the use of key terms proved more challenging.

An analysis of information and data-related laws in Australia must contend with a lack of consistent use of terms across legislation generally. While diverse use of terminology across

[24] This is only where relevant, and excluding Parliament and parliamentary committee and general, cross-cutting oversight bodies that also function outside the intelligence and law enforcement context, such as the Australian National Audit Office and the Commonwealth Ombudsman.

legislation may be justified by different statutory contexts, there are also situations where it can create confusion about meaning. For example, statutes dealing with the powers of law enforcement and intelligence agencies in relation to data use a variety of terms to describe the material accessed, including ‘communication’ ‘data’, ‘information’, ‘document’ and ‘record’.

Particularly as data becomes digitised and stored in diverse ways (including in the ‘cloud’), the distinction between these terms is not necessarily clear. As one research participant noted ‘Increasingly there is less of a distinction between data and information. … Increasingly, all will be viewed as data, whether structured or unstructured.’

A discussion of differences in the way that these terms are employed in various Acts is contained in a forthcoming report.

1.5. Australian constitutional framework and concepts

This study is undertaken to identify matters to be considered by Australian policymakers. It was therefore important to locate the investigation within the constitutional framework of Australia and especially the principles that apply to current and future legal measures. The constitutional context determines, for example, the scope of legislative power vested in the Commonwealth in relation to law enforcement and national security and therefore the scope of powers in relation to access and analysis of data in support of law enforcement and national security. It also provides constraints within which the law enforcement and national security agencies operate.

The following discussion briefly examines the relevant powers of the Commonwealth under the Constitution and then proceeds to discuss the principle of legality as an overarching rule of statutory construction, with an emphasis on the test of proportionality as a major criterion.

The powers of the Federal Parliament are set out throughout the *Australian Constitution*. The Federal government has express substantive legislative powers relating to the ability of federal agencies to access and manage data sets for the purpose of safeguarding national security and law enforcement under the 39 paragraphs (placita) of section 51. These include:

- 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*’.

Each of these paragraphs are briefly discussed below.

1.5.1. Section 51(v): ‘Postal, telegraphic, telephonic, and other like services’

The scope of the power conferred by s 51(v) on the Federal Parliament encompasses ‘full and complete power’ in the field of telecommunications.[25]

---

[25] In *R v Brislan; Ex parte Williams* [1935] HCA 78; (1935) 54 CLR 262, 277 Latham CJ wrote that: ‘It appears to me to be impossible to attach any definite meaning to sec 51(v) short of that which gives full and complete power to Parliament to provide or to abstain from providing the services mentioned, to provide them upon such conditions of licences and payment as it thinks proper, or to permit other people to provide them, subject or not subject to conditions, or to prohibit the provision of such facilities altogether.’

The High Court held in *Bayside City Council v Telstra Corp* that:[26]

> The federal object of promoting the development of the telecommunications industry, and ensuring that telecommunications services would be provided to meet the needs of the Australian community, falls within a head of the legislative power of the Parliament of the Commonwealth.

It is arguable that 'the needs of the Australian community' would include both security and a degree of privacy. However, it is up to the Parliament – at the policy level – to determine how much (if any) weight should be placed on each of these considerations.

1.5.2. Section 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

When enacting laws with respect to telecommunications in the context of national security, the Federal Parliament can also rely on s 51(vi).

Although at first glance this paragraph may appear to be directed at naval and military power, this head of power was construed expansively by the majority of the High Court in *Thomas v Mowbray*.[27] The case is particularly relevant to the subject matter of the report as it addressed the applicability of the defence powers in relation to the prevention of terrorists acts in the context of '[maintaining] the laws of the Commonwealth'. Moreover, the High Court's reasoning based on the principle of legality and the criterion of proportionality is specifically applicable to legal analysis undertaken in this study.

In his judgment in this case Gleeson CJ, for example, held that this power is 'not limited to defence against aggression from a foreign nation; it is not limited to external threats; it is not confined to waging war in a conventional sense of combat between forces of nations; and it is not limited to protection of bodies politic as distinct from the public, or sections of the public.'[28]

In the same judgment Callinan J explained how this power would become relevant to the maintenance of law in Australia:[29]

> The language of s 51(vi) of the Constitution is itself expansive. Under it, the Parliament may enact laws for the control of the forces to execute and maintain the laws of the Commonwealth. The real question in every case will be, *is the Commonwealth or its people in danger, or at risk of danger by the application of force, and as to which the Commonwealth military and naval forces, either alone or in conjunction with the State and other federal agencies, may better respond, than State police and agencies alone*. If the answer to that is affirmative then the only further questions will be, are the enacted measures demonstrably excessive, or reasonably within the purview of the power, or, to use the language of s 104.4(1)(d) itself,[30] 'reasonably necessary' or 'reasonably appropriate and adapted' to protection against terrorism.'

---

[26] *Bayside City Council v Telstra Corp Ltd* [2004] HCA 19; 216 CLR 595 [26] (Gleeson CJ, Gummow, Kirby, Hayne and Heydon JJ).
[27] [2007] HCA 33 (Gleeson CJ, Gummow, Hayne, Callinan, Heydon and Crennan JJ).
[28] *Thomas v Mowbray* [2007] HCA 33 [7].
[29] *Thomas v Mowbray* [2007] HCA 33 [588].
[30] *Criminal Code Act 1995* (Cth) Part 5.3 div 104.

1.5.3. Section 51(xxix): External Affairs

Under 51(xxix), the Commonwealth Parliament is vested with a broad legislative external affairs power that 'is not confined to the implementation of treaties',[31] and includes the power to make laws in respect to matters affecting Australia's relations with other countries.[32] In *Polyukhovich v The Commonwealth*[33] Dawson J construed this head of power as follows:[34]

> [T]he power extends to places, persons, matters or things physically external to Australia. The word 'affairs' is imprecise, but is wide enough to cover places, persons, matters or things. The word 'external' is precise and is unqualified. If a place, person, matter or thing lies outside the geographical limits of the country, then it is external to it and falls within the meaning of the phrase 'external affairs'.[35]

Dawson J's formulation in *Polyukhovich* has been acknowledged 'as representing the view of the [High] Court'.[36] This wide doctrine was adopted in *Thomas v Mowbray,*[37] where Gummow and Crennan JJ held that '(t)he pursuit and advancement of comity with foreign governments and the preservation of the integrity of foreign states may be a subject matter of a law with respect to external affairs', and that matters affecting Australia's relations with other countries include prevention of 'terrorist acts' as defined in s 100.1 of the *Criminal Code*.[38]

Thus the external affairs power can be used to make laws that aim to prevent 'terrorist acts' within Australia. The High Court quoted[39] with approval as equally valid for Australia, the following comments of the Supreme Court of Canada[40] which having noted that ever since the year 2001, 'terrorism in one country' may implicate other countries:[41]

---

[31] *Victoria v Commonwealth (Industrial Relations Act Case)* [1996] HCA 56; 187 CLR 416, 485 (Brennan CJ, Toohey, Gaudron, McHugh and Gummow JJ).
[32] *XYZ v The Commonwealth* (2006) 227 CLR 532, 543 [18] (Gleeson CJ).
[33] (1991) 172 CLR 501.
[34] *Polyukhovich v The Commonwealth* (1991) 172 CLR 501, 632.
[35] In *Victoria v Commonwealth (Industrial Relations Act Case)* [1996] HCA 56; 187 CLR 416, 485, Brennan CJ, Toohey, Gaudron, McHugh and Gummow JJ, having noted that in *Polyukhovich,* Mason CJ; Deane J; Gaudron J; McHugh J expressed similar views to those of Dawson J, concluded that they 'must now be taken as representing the view of the Court'. This wide doctrine was adopted in *Thomas v Mowbray* [2007] HCA 33; 233 CLR 307 [151], where Gummow and Crennan JJ held that 'the pursuit and advancement of comity with foreign governments and the preservation of the integrity of foreign states may be a subject matter of a law with respect to external affairs', and that matters affecting Australia's relations with other countries include prevention of 'terrorist acts' as defined in *Criminal Code Act 1995*, s 100.1.
[36] In *Victoria v Commonwealth (Industrial Relations Act Case)* [1996] HCA 56; 187 CLR 416, 485, Brennan CJ, Toohey, Gaudron, McHugh and Gummow JJ noted that in *Polyukhovich* (1991) 172 CLR 501, Mason CJ at 528–531; Deane J at 599–603; Gaudron J at 695–696 and McHugh J at 712–714 expressed similar views to those of Dawson J.
[37] [2007] HCA 33; 233 CLR 307 [151].
[38] *Criminal Code Act 1995* (Cth) s 100.1 defines 'terrorist act' as meaning (i) an action or threat of action intended to 'advance a political, religious or ideological cause'; or (ii) 'coercing, or influencing by intimidation, the government of the Commonwealth', its States and Territories (or parts thereof) or a foreign country, or (ii) intimidating the public or a section of the public.'
[39] *Thomas v Mowbray* [2007] HCA 33 [152] (Gummow and Crennan JJ).
[40] *Suresh v Canada (Minister of Citizenship and Immigration)* [2002] 1 SCR 3, 50.
[41] *Suresh v Canada (Minister of Citizenship and Immigration)* [2002] 1 SCR 3, 50.

> 'First, the global transport and money networks that feed terrorism abroad have the potential to touch all countries, including Canada, and to thus implicate them in the terrorist activity. Secondly, terrorism itself is a worldwide phenomenon. The terrorist cause may focus on a distant locale, but the violent acts that support it may be close at hand. Thirdly, preventive or precautionary state action may be justified; not only an immediate threat but also possible future risks must be considered. Fourthly, Canada's national security may be promoted by reciprocal cooperation between Canada and other states in combating international terrorism.'

From a constitutional law perspective, it is therefore arguable that the Commonwealth Parliament has power to legislate measures to combat terrorism under s 51(xxix) that include authorising access to Australian and foreign data-sets.[42]

1.5.4. Section 51(xxviii) The influx of criminals

While the High Court has referred to s 51 (xxviii),[43] the nature and scope of the sub-section has not been the subject of specific construction by the Court. Two judgments that discussed aspects of this paragraph are relevant to the governance of, the access to, and management of large data-sets by law enforcement and national security agencies.

Firstly, this section has been construed as extending the Commonwealth's external affairs powers. In *Merchant Service Guild of Australasia v Commonwealth Steamship Owners Association*[44] Isaacs J considered that since s 51 (xxviii) 'necessarily [involves] every thing essential to effective exclusion' of criminals,[45] it impliedly extends the prima facie extraterritorial powers of the Commonwealth under s 51(xix) *External Affairs* powers.[46] Secondly, in *Jolley v Mainka*[47] Evatt J considered that the power to legislate upon 'external affairs' includes such enumerated powers as 'immigration of aliens, naturalization, the influx of criminals, &c.'[48]

The High Court is yet to impose limitations on a power of the Commonwealth Parliament to legislate on the matter of the influx of criminals.[49] However, as Gummow J put it in *Re*

---

[42] This power may be further supported by reliance on the reference power in s 51(xxxvii) of the *Australian Constitution*: 'matters referred to the Parliament of the Commonwealth by the Parliament or Parliaments of any State or States, but so that the law shall extend only to States by whose Parliaments the matter is referred, or which afterwards adopt the law' as well as incidental powers in s 51(xxxix): 'matters incidental to the execution of any power vested by this Constitution in the Parliament or in either House thereof, or in the Government of the Commonwealth, or in the Federal Judicature, or in any department or officer of the Commonwealth'.

[43] For obiter dicta see for example, *Lipohar v The Queen* [1999] HCA 65; 200 CLR 485 [166] (Kirby J); *Re Minister for Immigration and Multicultural Affairs; Ex parte Te* [2002] HCA 48; 212 CLR 162; *Truong v The Queen* [2004] HCA 10; 223 CLR 122.

[44] 16 CLR 664.

[45] Expressly adopted by McHugh J in *Re Woolley; Ex parte Applicants* M276/2003 [2004] HCA 49; 225 CLR 1 [63], and Hayne J in *Al-Kateb v Godwin* [2004] HCA 37; 219 CLR 562 [259].

[46] *Merchant Service Guild of Australasia v Commonwealth Steamship Owners Association* 16 CLR 664, 692–693.

[47] [1933] HCA 43; 49 CLR 242.

[48] *Jolley v Mainka* [1933] HCA 43; 49 CLR 242, 286–7. Evatt J, adopted Professor Harrison Moore's comments written at the time of enactment of the *Australian Constitution Act 1900* (UK) (Imp) 63 & 64 Vict. See Harrison Moore, 'Australian Commonwealth Bill' (1900) 16 *Law Quarterly Review*, 39.

[49] According to Gaudron J in *Kruger v Commonwealth* [1997] HCA 27; 190 CLR 1, 115 the proposition that 'a law authorising detention in custody, divorced from any breach of the law, is not a law on a

Minister for Immigration and Multicultural Affairs; Ex parte Te [50] the text of the s 51 heads of power: 'is to be construed with all the generality which the words used admit…and if a sufficient connection with a head of power exists, the justice and wisdom of the law, its necessity and desirability are matters of legislative choice.' [51]

The phrase, 'the influx of criminals' is open-ended and can augment other express powers discussed above[52] in relation to Big Data access and utilisation within and outside of Australia.

1.5.5. Conclusion

Commonwealth legislative powers 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 broad and the High Court supports an expansive interpretation. Where a power falls under one or more paragraphs of s 51, it must be exercised in accordance with the principle of legality. The application of this principle in Australian law is briefly reviewed below.

1.6. Principle of legality

Apart from constitutional validity based on constitutional heads of power, legitimacy of Federal legislation is also assessed in accordance with common law doctrines, of which the principle of legality is particularly relevant in the context of law enforcement and national security legislation. Access to and management of Big Data containing personal and other sensitive information without knowledge, let alone consent, of the persons affected may infringe patients' right to medical confidentiality; statutory rights to privacy; and the right to natural justice.

The principle of legality is the major rule of constitutional statutory construction when validity of legislation is considered. This principle 'protects, within constitutional limits, commonly accepted 'rights' and 'freedoms' … it applies to the rules of procedural fairness in the exercise of statutory powers.'[53] An important aspect of the principle is ''a presumption that Parliament does not intend to interfere with common law rights and freedoms except by clear and unequivocal language for which Parliament may be accountable to the electorate'.[54]

---

topic with respect to which s 51 confers legislative power … does not extend to laws with respect to … the influx of criminals'.

[50] [2002] HCA 48; 212 CLR 162.

[51] *Re Minister for Immigration and Multicultural Affairs; Ex parte Te* [2002] HCA 48; 212 CLR 162 [113] (Gummow J). His Honour added that: 'All these propositions are supported by the joint judgment of six members of the Court in *Grain Pool of Western Australia v The Commonwealth* (2000) 202 CLR 479, 492 [16]'.

[52] In cases where the constitutional basis of a particular statutory provision is uncertain (as sometimes happens when legislation is enacted to implement Government's policies based on the executive power of the Commonwealth under 61), the Federal Parliament may rely on the grant of 'incidental' powers in s 51(xxxix): 'Matters incidental to the execution of any power vested by this Constitution in the Parliament or in either House thereof, or in the Government of the Commonwealth, or in the Federal Judicature, or in any department or officer of the Commonwealth', in *Davis v The Commonwealth* [1988] HCA 63; 166 CLR 79 (Wilson and Dawson JJ).

[53] *Saeed v Minister for Immigration and Citizenship* (2010) 241 CLR 252, 258–259 [11]–[15] (French CJ, Gummow, Hayne, Crennan and Kiefel JJ).

[54] *Momcilovic v The Queen* [2011] HCA 34 [43] (French CJ).

The rule of legality encompasses the principle of consistency and coherence of laws and duties across statutes and the common law.[55] Where pertinent, 'it may be linked to a presumption of consistency between statute law and international law and obligations'.[56]

The test of proportionality, discussed below, is 'a criterion of the principle of legality'. [57]

1.6.1. Proportionality test

In relation to wide-ranging investigative powers of law enforcement and security agencies, the precise criterion to be applied in the proportionality analysis involves 'a test of the legitimacy and proportionality of a legislative restriction of a freedom or right which is constitutionally, or ordinarily, protected'.[58]

The paradigm and elements of the proportionality test are yet to be specifically defined by the High Court. In relation to bodies/persons exercising powers under valid legislation,[59] it has been conceptualised as essentially a balancing process, where the decision-maker must:

(1) identify the purpose of the legislation under which she or he is acting, and
(2) decide whether the proposed action or measure is 'reasonably necessary and reasonably appropriate and adapted for the [statutory] purpose'[60] by applying proportionality criteria.

Depending on the circumstances of the case, proportionality criteria would include the fulfilment of the statutory purpose relating to the law enforcement and/or national security objectives on the one hand, and other relevant considerations, including legally protected rights and freedoms of those who may be affected by the decision, on the other hand.

The test of proportionality is particularly applicable as a measure of control in relation to legislation, as well as non-legislative instruments governing Federal agencies because it 'sets an appropriate limit on the exercise of purposive powers entrusted to a public authority to make delegated legislation'.[61] It is also applicable to decisions made in the furtherance of these purposive powers.

Importantly, the Australian test of proportionality may differ from concepts and tests relating to this notion as developed in other countries for constitutional purposes.[62] In Australia, 'proportionality' is not a legal doctrine, but 'a term used to designate criteria' for

---

[55] *Sullivan v Moody; Thompson v Connon* (2001) 207 CLR 562 [42] (Gleeson CJ, Gaudron, McHugh, Hayne and Callinan JJ).
[56] *Momcilovic v The Queen* [2011] HCA 34 [43] (French CJ). His Honour referred to Wendy Lacey, 'The Judicial Use of Unincorporated International Conventions in Administrative Law: Back-Doors, Platitudes and Window-Dressing' in Hilary Charlesworth et al (eds), *The Fluid State: International Law and National Legal Systems* (Federation Press, 2005) 82, 84–85.
[57] *Attorney-General (SA) v Corporation of the City of Adelaide* [2013] HCA 3; 249 CLR 1 [42] (French CJ).
[58] *Maloney v The Queen* [2013] HCA 28 [130] (Crennan J). Her Honour referred to *Betfair Pty Ltd v Western Australia* [2008] HCA 11; (2008) 234 CLR 418, 477 [102]–[103]; [2008] HCA 11; to *Thomas v Mowbray* [2007] HCA 33; (2007) 233 CLR 307 331–333 [20]–[26] (Gleeson CJ);
[59] The Federal Parliament would also need to identify the relevant heads of power under s 51 when enacting legislation, and ensure that the purpose of the proposed statutory provisions fits within their subject-matter.
[60] *Thomas v Mowbray* [2007] HCA 33; (2007) 233 CLR 307.
[61] *Attorney-General (SA) v Corporation of the City of Adelaide* [2013] HCA 3; 249 CLR 1 [58] (French CJ).
[62] *Attorney-General (SA) v Corporation of the City of Adelaide* [2013] HCA 3; 249 CLR 1 [42] (French CJ). This discussion will be of particular importance once we embark on comparative study, for the UK, Canada and NZ have quite different frameworks, for example, we are the only jurisdiction without Human Rights Charter or its equivalent.

determining the validity and lawfulness ‘of rational law-making and decision-making in the exercise of public power’[63] by reference to ‘rational relationships between purpose and means, and the interaction of competing legal rules and principles, including qualifications of constitutional guarantees, immunities or freedoms.’[64]

In 3.2 the test of proportionality is considered as a control measure serving the principle of legality.

[63] *Attorney-General (SA) v Corporation of the City of Adelaide* [2013] HCA 3; 249 CLR 1 [61] (French CJ).
[64] *Attorney-General (SA) v Corporation of the City of Adelaide* [2013] HCA 3; 249 CLR 1 [55] (French CJ).

2. USING BIG DATA FOR NATIONAL SECURITY: STAKEHOLDERS' PERSPECTIVES

This chapter analyses stakeholders' responses to questions regarding their use of data, their perception of risk and challenges in relation to the use of Big Data for law enforcement and national security, and their views on the regulation of data access, sharing and retention.

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.**

For ease of reading a summary of the broad views expressed by the interviewees is provided after each section. Letters are used to mark quotations from interviews for cross-referencing purposes. Terminology used to describe categories of research participants[65] is described more fully in the Methodology Report. References to the lens and lens numbers are to the lines of inquiry introduced in Chapter 5 of the Methodology Report.

2.1. Current use of data

2.1.1. General attitudes towards computer technology

We asked research participants who were working in or had worked in operational organisations, 'When does digital/computer technology hinder you in your work and when is it particularly helpful?' [O3]. The question is designed to elicit immediate reaction to digital technology in general before discussing specifics in relation to the use of data.[66]

Table 2-1: General Attitudes towards Computer Technology by Role in Operational Organisations (n=19)

	O/O (n=6)	T/O (n=9)	O-P/O (n=4)	TOTAL (n=19)
Both helpful and a hindrance	5	4	1	10
Helpful	0	2	1	3
A hindrance			1	1
No responses recorded or question not asked	1	3	1	5

*Note: Only those who working in or had worked in operational organisations are asked this question.

Table 2-1 shows that while few research participants saw computer technology as unequivocally helpful (three) or a hindrance (only one), the majority (10 out of 14 who were asked this question) saw computer technology as a 'double-edged sword', i.e. it can be both helpful and a hindrance. Helpful aspects of computer technology include the enhancement

---

[65] The abbreviations are: O for Operational, T for Technical and P for Policy, with O/O for example representing a participant with an operational role working in an operational organisation. See Chapter 4 of the Methodology Report for further details.
[66] Note that this whole section 2.1 is about 'data' in general, not about Big Data.

of communication speed, the capacity for information retrieval and sharing, the currency of information, and, more generally, the beneficial outcomes for law enforcement or security intelligence. Computer technology could be a hindrance because of its ubiquity and the volume of data which can cause stress. Three participants pointed out, however, that computer technology was 'an increasingly important part of the business' and 'there is no escaping – it's here' (T/O **A**).

Summary and implications

Most participants in operational organisations saw digital/computer technology as both helpful and a hindrance, with three expressly recognising its inevitability.

2.1.2. Types of data used

We asked all participants from operational organisations, 'What types of data do you (or your unit) use in your work?' [O4] This is a very broad question that elicited a wide range of answers, depending on participants' own perception of what 'data' is and the nature of their organisation. Table 2-2 provides a breakdown of the results. These represent what participants told us in interviews—they do not constitute a comprehensive inventory. For example, although no-one from an intelligence agency specifically mentioned telecommunications metadata in response to this question, they did reference overlapping categories (such as "communications signals") and do, in fact, have access to telecommunications metadata.[67] Further, because we are adopting the terms used by research participants, categories may overlap or coincide. Similarly, the distribution of research participants does not necessarily reflect the distribution of usage in actual practice. It is important to interpret the figures in this table not as a definitive map of what different agencies are using, but more as how research participants characterised them.

Table 2-2: Type of Data Used by Nature of Organisation (n=19)

	Intelligence organisation	Law enforcement organisation	TOTAL
Open source/online data	0	7	7
Telecommunications metadata	0	5	5
Intelligence data	3	2	5
Communication signals	3	1	4
Any data we have legal access to/numerous datasets	0	4	4
Operational /official data /data from other government departments	0	4	4
Data from international partners	1	2	3
Publicly available data	2	0	2
Databases internal to the agency	2	0	2

[67] Malcolm Turnbull, Minister for Communications, Second reading speech on the introduction of the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (30 October 2014).

Information provided by the community	0	2	2
Geo-spatial data	1	0	1
Financial data	0	1	1

*Note: Multiple responses can be coded for each research participant. Only those working in or who had worked in operational organisations were asked this question.

A quick glance of Table 2-2-2 suggests that participants from intelligence organisations and those from law enforcement organisations reported using quite different types of data. For example, one participant from an intelligence organisation mentioned '**communication signals**' as an important type of data they handle:

> This specifically relates to [name of agency] as an intelligence gathering organisation … Let's broadly categorise it as signals. … When you think about anything that sends a signal, any type of communication device that sends a signal, and that includes phones, pagers, faxes all those types of things, anything that sends a signal that can be sucked up, is generally a target source anyway. (O/O **A**)

Other types of 'communication signals' used by intelligence agencies include 'telecommunications intercept, listening devices, [and] tracking devices' in their 'targeted intelligence collection' (T/O **B**). These agencies also make use of **geo-spatial data**, (unspecified) **publicly available data**, and **internal databases** kept by agencies in relation to 'entities of security interest' (T/O **C**).

Participants from Law enforcement agencies were often more explicit about the type of data they make use of. For example, **open source** or **online data** was mentioned most frequently, followed by **telecommunications metadata**[68]**, operational** or **official data from other government departments, information that is provided by the community,** and other data sets, in fact, 'any data that we can get our hands on lawfully' (O/O **D**), as described by these participants:

> Very broadly … Anything that we deem relevant realistically. Any data that we can collate online, whether it be that online evidence that may indicate the commission of offence or assist in making a nexus, a link, to that offence, such as photographs, emails, whether it be data these days, obviously text messages, contacts. Realistically it's comprised of anything that's online that we can, again lawfully, collate for the purpose of our investigation. IP addresses, the metadata behind those, behind the obvious data such as photographs, the metadata within that photograph. … we use any data that we can get our hands on lawfully, certainly, to assist in our investigation. It comes up to the initiative and the imagination of the user or the investigator on how they get their hands on that data. (O/O **E**)

> Well, a broad range of data, so it would be information that we collect from sources, information that we collect from search warrants, information that we lawfully collect over telecommunications interception, information that we get from our international partners. I suppose, in the current environment, you name a data set and we get access to it. I don't think there would be anything that we don't utilise. … overseas data sets as well so we get access to particularly Five Eyes community data

[68] While there has been confusion about what exactly metadata is in the recent Australian debate about data retention, the 'telecommunications metadata' in this section refers to phone numbers, time and duration of calls, location of telecommunication towers, IP addresses, etc but not the actual contents of these communications (which would be categorised as 'communications signals').

sets. We also get data sets from some of our South-East Asian partners on a police-to-police basis. So that means we can't actually use it in any prosecution. (O/O **F**)

We use official sorts of data. So data from partners … intelligence reports or we use information that we get from members of the community when I think about our community liaison functions and we use open source in all of its forms. Often we are responding to what is out there in open source and particularly what people might be putting out through social media. … I'm probably speaking more broadly on behalf of CT [counter-terrorism] than just myself but … one of the ideas around the [name of group] that we've set up is that everybody brings their data to the table around a person of interest … to be able to look and narrow down on people … if it's an Australian based investigation involved in the attack planning and when it'd have a traditional law enforcement response, or people who might be on the outside of that network, what other connections they have with government and how that information or that data set or that power can be brought to bear to resolve that situation. (O-P/O **G**)

All sorts quite frankly. … [In] the area that I'm responsible for we use data that is unit record data available … through a third party where we have legislative ability to obtain it. … We get fourth party data from information that's available on social media and the Internet and we use that. We match all that data together and create some second party data for ourselves which is data that didn't exist until we matched it, until we created it, that's what I refer to as second party data anyway. … – [W]e are entitled because of the powers of the office to seek specific data from any number of sources in relation to the work we do through our access powers and we use that. … I guess finally there are a couple of other types of information that we get. There is information that we comes to us from the community, colloquially known as 'dob-ins', some of which is useful, some of which is not and information that comes to us from overseas. … Usually through [national office] agreements, we get an automated exchange of information and we have automated exchange of information arrangements in place. We also get specific information provided to us on request or when another agency feels it's appropriate within the terms of the arrangement that we have with them to provide us that information. We will match and use any or all of that information I've mentioned to you to form judgements about the integrity of the … systems. (T/O **H**)

Summary and implications

Research participants worked 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. In some cases, data used was identified broadly, as in 'a signal that can be sucked up' or 'any data that we can get our hands on lawfully'.

2.1.3. Types of data generated

We asked participants working in (or who had worked in) operational organisations, 'What types of data do you (or your unit) generate in your work? How is this captured?' [O5] Table 2-3 provides a breakdown of the types of data generated according to the nature of the agencies.

The most frequently cited type of data generated by both types of organisation is **intelligence reports** which may be in a variety of formats:

> Generally the data that we generated ourselves was just reports based on the raw information that was coming in. … We would do preliminary analysis on raw data based on the collection. That information would then be distributed to the analysis organisations on a central repository. So charts, tables, narratives and reports ... (O/O – INTEL **A**)
>
> We provide reports based on analysis of data. … We provide narrative reports and data products that contribute to intelligence operations. They can be narrative or a graph or a network chart. (T/O – INTEL **B**)
>
> A lot of the stuff that's generated I suppose is the resulting intelligence product from the analysis of that data … So … in terms of the data that we would produce, it's more an examination of data rather than data in itself. (O-P/O – LE **C**)

Table 2-3: Type of Data Generated by Nature of Organisation (n=19)

	Intelligence organisation	Law enforcement organisation	TOTAL
Intelligence reports	4	4	8
Other reports	0	7	7
Briefs of evidence	0	3	3
Audit trails	0	2	2

*Note: Multiple responses can be coded for each research participant. Only those representing operational organisations are asked this question.

A range of **other types of reports** are generated by law enforcement agencies, for example:

> Internally, obviously that data that we generate would be evaluated reports, would be information reports. Large data sets of … aggregated biodata for … predictive profiling of hotspots where offences are occurring. Trend analysis … We've had spikes in crime so then we can obviously - with very regular monthly or weekly briefings on spikes in crime rates in a particular area at a local level, but that flows up to command level of overall trends. Again, personal profiling of individuals who are committing offences. It may be data on organised crime networks and trying to make links and associations between individuals and networks, whether it be within our jurisdiction and outside our jurisdiction. Obviously you have internal communications such as internal emails and things like that. (O/O – LE **D**)
>
> We generate a variety [of data] …so it ranges from operational report level data for organisational management purposes. That could be performance data, effectiveness, efficiency reporting. [Q: That would be raw or summarised data?] Summarised yeah. Well it can actually range. If I think about smarter data analytics … It can range from an extract of raw data out of our data warehouse at the request of somebody in a business area through to the creation of a data cube that will allow them to manipulate the data for themselves through to a population level report. What do we know about a population through some an analysis or a risk assessment report? There are various levels of risk assessment report through to reports about the integrity of the [system] … That will be a longitudinal sort of report. (T/O – LE **E**)
>
> I guess it would be technical performance data. A lot of procurement data in terms of the cost of doing business, if you like, with technology. So a lot of licence costs,

> the software costs, the procurement costs … that kind of data. We provide the policy and guidelines on use … or non-use [name of agency]-related infrastructure and services, guidelines and directives et cetera. In terms of the wider organisation, the data we create is telephone interception data. So I guess we generate … data created by people accessing the Internet, conversing over a telephone, meeting in a park. We generate records of [an] interview when we've brought people in or spoken with people in the course of an investigation. We generate enormous amounts of data from seized items, like telephones, laptops, computers, banking networks if there's a - if the investigation is large enough or relevant enough. We generate lots and lots of data round requests … for whether people have accounts with telcos [telecommunications companies]. Criminal history reports, intelligence assessments, enormous quantities of audio-visual data. DNA-related data. Firearms data. Chemical and ballistics data. (O/O – LE **F**)

One participant mentioned that their unit generated audit trail data for compliance purposes:

> We do have an audit trail, so we do generate records of access, requests, approvals - all of that sort of thing. We generate audit records automatically, it's built into the system functionality, when each person logs in they do so with a corporate number assigned to them and unique to them, the number is linked to the payroll code so one can find a person's name, rank and title. … Officers nominate which inspector reviews their requests; normally it follows the department command chain. Everyone needs to nominate and have their requests reviewed, inspectors cannot self-clear their own requests, they nominate another inspector so that it is independent …. The Attorney General's Department review our *Telecommunications Act* compliance.[69] The [State] Privacy Commissioner looks over the Memorandums of Understanding we have with external agencies and between units. Some agencies generate audit reports of all requests to confirm they comply with privacy requirements; it depends on the terms of the MoU. Our unit can also generate audit reports agency by agency which can be called on to review team, unit and organisational compliance. (T/O – LE **G**)

For another participant, what starts off as information collected in the course of an investigation can end up being a brief of evidence:

> [D]uring the course of investigation, we collect information and we pretty much collect information from as broad a source as well can so often we can take surveillance photographs and we store them in the system or if we interview witnesses we might digitally record those witnesses and suspects and also if we attend search warrants and I'm not sure if that's covered by the scope of the interview but certainly when we seize information under warrant. That can be electronic records and emails, documents and stuff from banks and other things. So at that phase [of] the investigation we do put a lot of material together and then we analyse that… for what is relevant to us… it's stored on our systems and if it gets to the point where we transform it into evidence and it's admissible then it might get tendered in a court … and with the DPP. (O/O LE **H**)

---

[69] This may be a reference to AGD oversight of the *Telecommunications (Intercept and Access) Act 1979.* AGD does not have oversight of the *Telecommunications Act.* It is also worth noting that AGD coordinates a range of matters, but formal oversight is undertaken by the Commonwealth Ombudsman.

Summary

Data generated within agencies may be in the form of reports, including text and visual elements, or may be raw data or visualisations that can be manipulated by others. Data is also generated for diverse purposes; their formats include: records of intelligence on individuals and networks, records of criminal trends, reports for internal purposes (such as performance measurement and compliance), and data to be incorporated in briefs of evidence. Such distinctions may be important when developing efficient tools to store and link agency-generated data.

2.1.4. Sharing of data

All participants from operational organisations were asked: 'Does your unit share data with other agencies, and if so, which ones?' [O6] Table 2-4 shows that there is a fair amount of data sharing between law enforcement and national security agencies and between these agencies and other government, non-government and international organisations. In some cases, the sharing may be reciprocal. Note that this table, similar to all tables in this Chapter, is constructed using the interview data which is not meant to be comprehensive.

Table 2-4: Sharing of Data between Organisations

	Australian national security organisations	**Australian law enforcement organisations**	**Other Australian government organisations**	**Civil society, media, community**	**International organisations**
• Australian national security organisations	• Top secret network • Intelligence community	• Sanitised • Case by case		• Data not provided to private companies or individuals)	• Five Eyes community • Other countries require special authorisation; human rights considerations may be a condition for sharing
• Australian law enforcement organisations	• Australian Signal Directorate • Australian Secret Intelligence Service • Top secret network • Australian Security Intelligence Organisation	• Joint task force • Other Commonwealth or State investigative agencies • Australian Border Force	• CrimTrac • Courts, DPP • Parliament • Centrelink • Australian Tax Office • AUSTRAC • Australian Bureau of Statistics • Family and Community Services	• Media • Citizens (FOI) • Social media (emergency)	• Five Eyes community • Other countries 'tear line' used [70] • Interpol, Europol

Source: Interview participants working or had worked in operational organisations.

[70] See quote 2.1.4D below.

A few common themes about data sharing emerged from the interviews:

- **Most of the shared data is data with identification** — this is because most of the data is used for investigation purposes (see next section):

  > Rarely is it de-identified, because the only reason we'd be sharing information is for investigative action or in support of an investigative outcome. So if it's worth sharing them, … it would be a very peculiar case where we'd actually de-identify the information. We're not an intelligence agency per se. We have intelligence that supports operations. Again the purpose of that is to identify who, what, where, how, et cetera. So if we were an intelligence agency, … we might be more inclined to focus on using de-identified data for trend and for a bit of a strategic assessment. The vast majority of information we collect, if it's done under warrant in one form or another, like an interception or whatever it might be, it has to be for the purposes of the conduct of an investigation with an intent to prosecute, and where all other avenues have dried up. So again it has to be entirely focused on either identifying an individual or individuals, or focused on known individuals and individuals. (O/O – LE **A**)

- **Most of the shared data is in the form of summarised reports** rather than raw data:

  > … it would be in the summarised form. So, … you'd have a summary report of the intelligence which would make reference to raw information. So say something was distributed or made available to DIO [Defence Intelligence Organisation] and they said, well, look is it actually okay if we see the raw data associated with that? They would have the information and they could request that, but by standard way of interacting they would have received the summarised information. (O/O – INTEL **B**)

- **Highly classified information is 'sanitised' before sharing** to agencies other than the core national security organisations, requiring careful curation:

  > What you'll generally find is that information is highly classified because the collection of that information and how it was collected denotes capability, Australian capability. That's something which is highly classified… In terms of Defence you're looking at ASD, DIO, DIGO. Then you'd be looking at ASIO, ASIS and ONA would be the national security organisations. They would be the ones that would have regular access to that information. Sharing data at that point in time with the state and federal police was sanitised before it was distributed and was not done at that point in time in an automated fashion. It was done on a case-by-case basis basically, working on a specific target set with those organisations. … we would much rather sanitise information and maybe only give out intelligence that was of a 70 or an 80 per cent proof to protect the capability and protect the ongoing viability of those data sources to protect capability particularly to organisations that didn't have a high security setting…(O/O – INTEL **C**)

  > So depending on the agency we will prepare something for them … but we work on tear lines. So we prepare information that they basically take and use. … So you write an intelligence report and it'll have all the confidential stuff up there. So I'll get something from a partner agency and they'll say, right, [name of person], this is everything here underneath the tear line… So we operate on tear lines in that sort of situation depending on who the partner is. (O-P/O – LE **D**)

- **Sharing is usually restricted** by legislation, procedure or memoranda of understanding.

  > The type of data shared depends on the circumstances, particularly the organisation with whom it is shared. There are very strict rules. The Director General has authority over what is shared. (T/O – INTEL **E**)

> There are restrictions on what we can share. There are quite clear legislative boundaries that we can't cross. We only share unit level data where we are legislatively entitled to do so. Otherwise we will share aggregated information if it's necessary. (T/O – LE **F**)

- **There are special data sharing arrangements with the Five Eyes Community compared with other countries.**

> Yeah, if it's Five Eyes we share a lot. So if that's UK, USA, Canada, New Zealand, we in Australia, we share a lot between ourselves. But if we're working with [name of country] or whatever we'd used tear line and the same with some of the partners who are in the region and that's more individual … depending on the purpose for the information sharing, there's a whole approval process that goes with that, then they're might be death penalty implications for something like that. So I mean … it's a very targeted space that we work in. (O-P/O – LE **G**)

Summary and implications

The sharing of data between agencies domestically and internationally is a highly curated process. 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). 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 relates to identifiable individuals. Data may also be shared with the public, either directly, through the media or through social media, for example in response to emergency situations.

2.1.5. Main purpose of using data

All participants from operational organisations were asked: 'What do you (or your unit) mainly use these data for?' [O10] As can be seen in Table 2-5, a range of purposes were nominated, including (in descending order of frequency) investigation, arrest and prosecution, prevention of incidents or mitigation of risks, intelligence gathering, the identification of trends or risks, law enforcement and compliance, disruption, decision or policy making, and a number of other items that were only mentioned once: reporting, smart service provision, event evaluation, trust building and value adding. Note that in most cases, participants nominated multiple purposes; this is consistent with the fact that there is considerable overlap between items and they often represent different stages resulting in a range of outcomes.

Table 2-5: Main purpose of Using Data by Role in Organisations (n=19)

	O/O (6)	T/O (9)	O-P/O (4)	TOTAL (19)
Investigation	2	2	2	6
Arrest/prosecution	3	1	1	5
Prevention/risk mitigation	3	1	0	4
Intelligence gathering	3	1	0	4
Trend/risk identification	1	2	0	3
Compliance/law enforcement	1	2	0	3
Disruption	1	1	1	3
Decision/deployment/policy making	1	0	1	2
Reporting	0	0	1	1
Smart service provision	0	1	0	1
Event evaluation	1	0	0	1
Trust building	1	0	0	1
Value adding	1	0	0	1

*Note: Multiple responses can be coded for each research participant. Only those working or who had worked in operational organisations were asked this question.

The following excerpts from interviews provide a flavour of the multiple purposes served by data:

- **Prevention/evaluation/strategic analysis.** [Data mainly used for] security intelligence. You're looking at two or probably three areas. One is event prevention, so trying to foresee something or stop something from happening. Two, you're looking at event evaluation, so what happened and now retrospectively that we know something has happened—can we better analyse it to see what we missed, what we could have done better around who was involved now that more players might be exposed? Then I guess the third one was creating the bigger picture, so you find one person of interest and then you look at 10 people that they regularly contact and you look at the 10 people that they regularly contact and then you look at the 10 people they regularly contact and you create a global map or an organisational map of contacts and then you … cut out who's not of interest .... Then you start to look for the links across the networks … so that informs then this strategic analysis … So it's that kind of longer term analysis rather than event based analysis. (O/O **A**)
- **Investigation/prosecution/disruption.** Yeah, we talk about a spectrum of activity. So we've got … traditional law enforcement so we always go for prosecution. If we can't prosecute … depending on where it is in the cycle, we'll look for an intervention like a control order or a preventative detention order … Then we'll go into the middle where we're looking at this sort of disruption thing. … So you have to sit back, bring that data together and actually work out what's the risk we're going to have and how are we going to play that? What's the way to intervene? … Who is that person there? Are they really just somebody who needs to be put back on the right path, do they need religious training, do they just need traditional mentoring from somebody in the community? Are they good for a support program, do they need English language training, do they need an apprenticeship? That's what we're trying to do. (O-P/O **B**)

  Another research participant (O/O) referred to the challenge from an agency perspective in focusing on disruption rather than the traditional mission of prosecution, stating that some within that agency 'lack imagination'.

- **Intelligence/investigation/disruption.** We do what we call security intelligence investigations. In the course of that, we produce lots of intelligence depending on how you define it. … It depends on the national security outcome we are trying to achieve. We deal very much in shades of grey. Gaol may be the best national security outcome where police assisted by [name of agency] have enough evidence to put someone in gaol. But in some situations, it may be just as good to stop them doing something. We can sometimes convince them to stop, that is, disruption that does not involve prosecution. So there is a suite of options. (T/O **C**)
- **Intelligence/value-adding**. The best way to think of it is value-adding to the data we currently have, where we might take a range of satellite imagery and extra[ct] all the features, like what is a road, what is a house and a city and so forth and be able to create a map. Then to value-add to it further we might point out, for example, in the [name of agency] case, here's where the mosque, the hospital and the schools are and so hence we need to obey the laws of armed conflict around those particular areas. Then we might … further value-add to that by being able to say add the intelligence for example, here's the best route that we recommend that you take to get through this town, which is safest and less likely to have a risk of an IED … or here's where we think the bad guys are sitting. (O/O **D**)
- **Information sharing/trust building**. There's a degree to which, if I'm honest, I think we use it also as currency. I'll provide you with this information, … it's either a trust building exercise or it's … another coin in the bank effectively. … [An example is] when the Bali Nine stuff was up and running, there was a big push for us not to share any information with any country that … had a death penalty in its criminal code, … since there's only three countries in the whole of … the Southeast and North Asia that don't have the death penalty … we were saying, well, that's not viable … we can't operate … or expect to be successful if you can't provide information to these countries. What you've got to then put … in is a code of conduct that helps you avoid … the sharing of that information of putting people at risk, but equally is transparent and visible enough to our partners so that they understand that we're still a partner to work with, because we are actually willing to share information. (O/O **E**)

Summary and implications

Research participants from operational organisations nominated using data for a range of past-focused and future-oriented purposes. Past-focused purposes include investigation, arrest and prosecution (nominated by 9 participants), reporting (1), and event evaluation (1); while future-oriented purposes include prevention or disruption of incidents or mitigation of risks (6), intelligence gathering (4), identification of trends or risks (3), policy or service decisions (3) and trust building (1). 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. This is consistent with the observation in 2.1.4 that almost all research participants were only interested in identified, rather than de-identified data.

2.2. Current concerns regarding access to and sharing of data

Participants from operational organisations were asked, 'What are your major concerns in relation to data access from other agencies or sharing data with other agencies?' [O7] Table 2-6 summarises the responses to this question, broken down by the role of research participants in their respective organisations. Three main concerns were raised: legal requirements including privacy issues (real or perceived), technical issues, and issues relating to ownership of data and trust.

Table 2-6: Current Concerns re Use of Data by Role in Organisations (n=16)

	O/O (5)	T/O (8)	O-P/O (3)	TOTAL (16)
Legal requirements/privacy – real or perceived	3	5	3	11
Technical issues	3	4	2	9
Ownership and trust	4	1	1	6

*Note: Multiple responses can be coded for each research participant. Only those working or who had worked in operational organisations are asked this question. Question was not asked of four participants..

2.2.1. Real or perceived legal requirements

The most frequently cited concern is in relation to real or perceived legal requirements including in relation to privacy issues. Some examples of what participants said are excerpted below:

> First concern is following the [name of legislation] and what we're allowed and not allowed to do. So for example … we frequently receive requests from private companies wishing to access our data information which we aren't able to fulfil …. (O/O **A**)
>
> [T]he legal impediments in some instances are still a concern where, for instance, some agencies that we deal with can only share information with law enforcement based on fairly tight criteria. [Name of agency 1] is a good example where they can only share information with us where it has a direct nexus to protecting the Commonwealth ... So legally there are some impediments. (O/O **B**)
>
> There is a stringent complex legislative framework regarding the intelligence and law enforcement agencies community. It puts limits on what data can be legally and appropriately shared. We always want more in the sense with better access to data we believe we can produce better national security outcomes. (T/O **C**)
>
> The Act is prohibitive about what can be shared. (T/O **D**)

Legislative requirements are compounded when attempts are made to share data across State and Territories under our federated system:

> Under [the] Federated Model we have nine governments and different ways to look at the issues, [it's] difficult … to share and negotiate terms, conditions and agreement — even just different laws makes it difficult, and share in accordance with the lowest common standard so that everyone should comply—so it is challenging … each State has its own regime from *Human Rights Act* or *Privacy Act*, or Commissioner for Law and Enforcement Data Integrity. When those jurisdictions provide [information] to us, one challenge is that there is an expectation that the conditions and terms on information attached in their State continue to apply nationally, so once in the Commonwealth regime it moves to new rules. For example, Freedom of Information – we have to reconcile different laws and we have negotiated agreements as to how we consult with people – Commonwealth makes decision to release so we are governed by Commonwealth Act but State/Territory might have an objection. (O-P/O **E**)

It was pointed out that the legislative and procedural framework dictates the 'business model', of process, under which an agency operates:

> We operate under a 'join the dots' business model. The Act and internal procedures both work like that. If we have a lead, we follow the lead to its logical conclusion, joining the dots. We don't access data until we have cause to use it, a need to link another dot. For example, suppose we have a partial name … The next dot is to go to a dataset to find a match for the name and link it to an actual person … We can't just go and requisition information from a government agency because we feel like it. We need to make a case. There are different levels of authorisation. (T/O **F**)

While recognising the need to balance privacy concerns with agencies' desire to share data, a research participant cited an instance where legal rules could be unnecessarily restrictive to the detriment of law enforcement operations:

> [The main obstacle is the] need to balance between the need to share, desire to share for operational reasons, and the need to protect privacy of individuals and ensure that people only get access to data that they are legally entitled to. For example, NSW Driving License – my understanding is that in NSW the photographic images collected for [driving license] purposes cannot be used for law enforcement purposes except for traffic related identification – police don't have access to driver's license other than [a] 10-second glance (T/O **G**)

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:

> One of my greatest concerns and I don't know whether it's a real reality or it is just in the concerned space … The issue that we have is each agency … they have a clear role, function set and that relates to what their confidentiality, secrecy, sharing provisions, their legislation are. If we're taking them into new spaces we may be asking them to share information which on the face of their legislation they may not be able to do. Even for [name of agency] … We've got pretty broad functions where we can actually share information for a whole range of reasons which are police or police support services and things like that, so that's served us well. But that's something we need to keep under review as well as the other agencies. Just because of my history I know that particular things, particularly around really good data sources like most accurate sets in Australia, your electoral role, Medicare, and when we've tried to do things like a health access card and stuff like that, [we get] just the standard policy approach and legislative approach is no law enforcement or no this, no you can't have that, people are only giving us — it's their information and it's privacy. (O-P/O **H**)
>
> The concerns about data going out to other agencies are simply whether or not we're legislatively enabled to do so. … Sometimes it's convenient for us not to share data. I have observed in the past although I think this is changing, I have observed in the past people standing behind the legislation saying you're not entitled to that we won't share it with you. When in fact an attitude of 'are there ways in which we can legitimately share information with you might lead to a different outcome?' I don't mean going against the legislation but looking for ways to actually do it legitimately. (T/O **I**)
>
> Sometimes there's an air of frustration particularly around when agencies — look, it's a lot less now than it used to be—but not sharing because of they'll put up Privacy Principles under the Act when clearly they're not appropriate or clearly they're not right. Information can be shared under the *Privacy Act* from other

> Commonwealth departments etc for law enforcement purposes, that's pretty broad. If we're investigating something and we're given the power under the [agency legislation] to do so, then clearly it's law enforcement purposes. It's just that there are some individuals who don't think that means law enforcement purposes. I don't know what they actually think that means. (O-P/O **J**)

> There's also inconsistent understanding and views of privacy laws. So different agencies will take a particular interpretation of personal data or privacy and can put up artificial barriers or misunderstanding when it comes to us accessing it under the *Privacy Act*. (O/O **K**)

2.2.2. Technical issues

The second most frequently cited concern relates to technical issues such as data format, data 'silos', and their agency's ability to deal with the volume of data.

The **lack of an integrated system** was mentioned by some participants:

> In terms of access to the information it was frustrating at times that there wasn't one central repository which reports could be sent out to and accessed by everyone all the time … so we would send things out but a lot of the time we … only had limited information [on] some of the other organisations' reports. I guess when you're working as an analyst and you're working on a target set, one of the things that we worked very hard to do was to corroborate identity. I mean you could imagine that working in the CT [counter-terrorism] area there's a whole lot of people that have … the same names. A lot of the time distinguishing that you're looking at the right information pertaining to the right person you need to look further past what information would be available in your collection set. So you need to understand things like their family structures, how many sons and daughters did they have, how many wives did they have, where were they based, where did they travel. If someone else in another organisation had done that analysis and could corroborate that you were looking at the right person because they confirmed that someone was in the right area where that collection took place, that would make your job a lot easier. (O/O **A**)

> There would [need to] be changes around the systems themselves, technical changes, around the need to better integrate data so instead of so that the police could answer more complex questions on the data. Instead of having to gather birth date, then address, or gather data around a particular location – all of that is difficult to do nationally because of the way the systems are siloed… because systems have evolved over time and have been in place for a decade. Up until recently new capabilities have been delivered in an isolated manner … so you end up with all of these separate systems existing in isolation. There are some significant links between some systems but it's nowhere near as integrated as police would like or need. (T/O **B**)

> There is no capability to put in a name and draw from various different sets of data … can't put in a name and get an answer like you can with Google. (O-P/O **C**)

Getting data in a **compatible format** was another concern:

> [Another concern is] trying to get the data you need and a format you need that you can utilise. There's a wide array of different format types and software around different resolution of data in terms of the accuracy of it over different parts of the world and what it captures. So it's constant trying to get that and then managing it is quite tricky as well, because there's just so many different terms and conditions

> attached to that data depending on the license that you purchased it under, and being able to effectively manage that when you're disseminating or sharing that with your partners is quite a challenge. (O/O **D**)

> Well the difficulty sometimes is format so it's got to be in a way that's able to be integrated into your system, that's always difficult. When you get data from banks and so on some give us hard copies, so some give us PDF documents, some give us actual data in a format under warrant that's able to easily go into our system, same with CCR data [call charge records] from telecommunications companies. Sometimes it's electronic; sometimes it's hard copy PDF documents. (O-P/O **E**)

The problem of compatible format is compounded when historical data is being sought, in addition to the fact that such **data may be have been destroyed or lost**:

> Historical information is a major issue for investigations – for example older serious crime cases such as unsolved homicides, cold cases and that sort of older investigation information is very difficult. With older information, the data is destroyed, lost, and inaccessible for many reasons. Telecommunications carriers have limits on how long they hold information. Data retention laws do not change much, and they may even make things harder. We have great difficulty with requests based upon dated serious crimes which are still being investigated. … Each agency and telecommunications company provides its own results in its own format and this lack of any standardised presentation can make things very difficult. (T/O **F**)

The exponential **growth in volume of data** has created technical problems:

> The challenges that we're facing … the Big Data thing, we're seizing more than terabytes now when we do warrants. So the Big Data issue is becoming bigger and one job we did recently … there was so much information … that we physically did not have the assets in Australia to download it quick enough to start to look at it. So we literally had to [send] terabytes of data over to the US for them to crunch it for us. So the problem we had when we started this is getting bigger because the amount of data we're seizing is definitely increasing. (O/O **G**)

> Data is so big it is now impossible – cannot capture the world. That is too ambitious. Do we have to capture and store the whole lot or are there other ways? Over time, capturing everything is neither sustainable nor desirable. (T/O **H**)

2.2.3. Data ownership and trust

Issues of data ownership and trust between agencies or individuals appear to explain some of the reluctance to share data. One could also include in this category the comment from one research participant that it can take a long time to obtain relevant data from companies located in a different jurisdiction: '6 or even 18 months for getting an authorised record from Facebook that is admissible in court' (T/O).

One participant was very upfront about the kind of **cultural issues** (turf protection, gender hierarchy, agency rivalry) that could make data sharing difficult (see also examples in section 2.2.1):

> What I generally found was that collection agencies were very good at collecting, analysing and distributing information. The analysing agencies were trying to protect their turf a little bit … so they were less willing to reciprocate with putting as much information up and making as much information available. If you would send out requests for information specifically to support some of your work that you'd generally find that the turnaround times weren't great which was immensely frustrating. So again that touches on some of those cultural issues …

> Inherently the defence and national security sector is a male domain… it's an old boys club. If it's not filled with military men it's filled with former military men. If there's one thing that military folks like to do is get into pissing contests about who did what, when, how, who did you used to work for, where did you go? Unfortunately a lot of that travels across the barrier into the civilian agencies as well from the military, … yeah so there's that cultural issue of who's doing what which inhibits information flow, you know, who was the lesser sibling.
>
> … So if you're an analyst at [name of agency 1] does that mean you're the same as an analyst at [name of agency 2] or at [name of agency 3] or, you know, those types of tensions and where do you cross over? In those instances some of the tensions were often quite obvious which would make it I guess a little bit of a pissing contest at times about who had ownership over certain data and who should be actioning certain data and who should be dealing with potentially … say the military forces they might be acting on that data —should they be filtered through an analysis organisation when realistically if they're conducting military operations they're going to want access in real time to the raw data? If they want access to the raw data well then they need to be dealing with the collection agencies and some of those frictions about who's dealing with who.
>
> … Yeah each of the organisations considers them like an individual and they've all got their own personality and culture. Sometimes you just don't get along well with people for whatever reason. So some of the time there was a little bit of tension between the organisations, particularly when it comes to … who has the roles and responsibility for doing the data analysis. (O/O **A**)

According to two participants who worked in the same agency as each other, '**ownership' of data** is an issue that has become a sensitive one nationally, and it has impeded the sharing of data across jurisdictions and agencies:

> Who owns the data that your agency holds? It's a very sensitive issue nationally. The obstacle is that there isn't a common legal view. (T/O **B**)
>
> Yes, that's probably right. States believe it's their data, and that's not compatible with a strict interpretation with Commonwealth law. Once a record comes to us, a duplicate is made and now you have two regimes applying to the same information. We cannot agree as a country on that. (O-P/O **C**)

These participants told researchers that this reluctance to share could be related to **trust** and **confidence** regarding how the data would be used if shared. Typically police agencies did not like sharing information with non-police agencies and this feeling 'is mutual' (T/O **D**).

The cultural issues mentioned above also meant that data access would often rely on **personal relationships**:

> From an investigator point of view the main frustration I think we find is even though we've been doing this a long time and we're a mature agency, trying to actually find a point of contact within agencies to go to and to go back to it seems like every time when I was running investigations and you needed data out of an agency you had to re-invent the wheel in terms of who you asked and what form they used to get it. We never had a consistent and stable process to access [name of agency 1]'s information team. The [name of agency 2] is pretty good now but yeah most of the others really were hard to figure out how to plug into that agency. … Unless you knew someone in there that you'd dealt with before and it was a contact that you'd met and you'd groomed him and said if I need something can I call you, you'd get it, otherwise you're playing for luck on someone, on some cases. (O/O **E**)

Another participant pointed out that sometimes information is **over-classified** in a way that impedes data access:

> Obviously the classification of material does also sometimes make it difficult to share information. So, for instance, our Australian Intelligence Agency partners sometimes classify information at very high levels that means that …probably … only two other people in my division can see it and that makes it very difficult to action it because not everyone has the relevant security clearances. … the Snowden event didn't actually do us any favours because, I think, there's now been a tendency to over-classify information which is an issue for us across the board. I would be very surprised if other people haven't mentioned over classification as being a concern because I see documents now … I look at them and say, well, there's no way in the world this should be TS [Top Secret]. It's not a top secret document and we face that internally. People over-classify stuff. It's common … Yeah, and I think it's just a default situation sometimes … people just put everything to 'protected' when realistically it's either 'unclassified' or 'for law enforcement purposes only' but anyway, that's an internal training issue for us which I'm sure all other agencies have the same problem. (O/O **F**)

These complex issues were summarised by a participant who described how the reluctance to share data might have stemmed from a **fear of losing control over the information**:

> … my concern is that — and I'm sure the concern … would be shared by others, because agencies exist for very specific purposes. They're created by government to perform a function … those purposes drive agencies to derive expertise and capabilities to generate and manage and exploit that information. … a lot of those capabilities are actually very expensive. Some of them are quite unique. Certainly they're valuable. There's … always that risk that … the misuse of that information, or the lack of control of that information, will provide insight to people as to how we might do things, what we focus on, where we focus on them, what to look out for etc so you can counter it. … The concern around an agency is that we've got very strict controls over what sort of criminality actually generates the state to approve us to use those powers, and the concerns around privacy and the like. So what you end up with is a fear that … if it's misused … or inadvertently used, you'd run the risk of losing the capability itself. We're mandated to use this, unlike a lot of other agencies, because of our purpose and because of the controls on it. So … that data sovereignty idea I think is really a catch-all for the fear and loathing that we have as a group of agencies around concerns for the misuse of our data. I think it sets us up for a natural distrust, if you like, more with the unknown. Then of course what happens there is you get lots of personal relationships that form that - where you and I have spent 10 years working together. You've never once misused the information, burnt me or whatever it might be. So I'm more inclined to share with you, either an individual or an agency, because we have a mutual understanding as to how treat and control that data that we decide to share. I think as well one of the problems is — and we see this at times, is there's a lot of effort that goes into de-confliction. … You've got to be careful that the information you provide and then de-conflict to ensure that … other agencies aren't targeting you or don't open up an operation or investigation and start to target the same people or the same criminality that we're interested in, unless it's co-ordinated… so excess of information can create opportunities for blue on blue… (O/O **G**)

Summary and implications

Three main concerns were raised: 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 related to real or perceived legal requirements, including in relation to privacy issues. 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.

2.3. How problems can be overcome

We asked the same research participants 'How can these problems be overcome?' [O9]. Table 2-7 provides a summary of responses broken down by the current concerns expressed in the previous section [O7].

Table 2-7: Current Concerns by How Problems Can Be Overcome (n=19)

	Legal requirements/ privacy (11)	Technical Issues (9)	Ownership and trust (6)
Law reform/guidelines/policy decision	3	2	1
Education/training of practitioners	1	1	0
Better data management	0	1	0
Conversation with public	1	0	0
Cultural change	1	1	1
Political environment	1	0	1

*Note: Multiple responses can be coded for each research participant. The number in brackets in the first row represents the number of research participants who raised that issue, see Table 2-6. Only those working or had worked in operational organisations are asked this question. Two participants were not asked this question. One participant answered this question but was not asked question O7 (re concerns) – these answers are not included as it is not clear what problems they relate to.

2.3.1. Legal requirements or privacy issues

With respect to the real or perceived legal requirements or privacy issues, a range of solutions were offered. Not surprisingly, **changes to laws, guidelines or policy decisions** (the specifics being discussed at 2.5.4) were advocated by some participants:

> The legal ones can be overcome reasonably quickly by some amendments to legislation which we are working through now with Government particularly around the sharing of information with [names of agencies]. I think that will be resolved in the next sitting so hopefully that will be sorted. (O/O **A**)

For this participant, the current **political environment** has made it favourable for the required amendments to be passed by Parliament:

> I think … we're in a different environment … particularly in the counter-terrorism world … certainly things have changed dramatically …since ISIS basically started, so the last three years. So what we're after is basically the ability to use information for national security purposes … I don't think there will be a problem with that but that will get bipartisan support as long as there's adequate checks and balances in place to ensure that we don't abuse the information we've provided and we're okay with that. (O/O **B**)

One participant saw **education of practitioners** as one way of overcoming the problem, in addition to stronger guidelines and policies:

> [Compliance with] [Name of Act] is overcome in terms of education for all people within the building, quite stringent policies within that we require people to follow with guidelines and that sort of thing. (O/O **C**)

Another suggested that what is required is a **conversation with the public**:

> I think it's just one where unfortunately we're going to have to be reactive, I don't think we can be proactive. I think it's really about — and this has been something we've tried before — having a decent conversation and a non-hysterical conversation with the community and particularly advocates about what is privacy. I mean, it's not helpful for people — it could have been the Facebook or it could have been somebody from Google or Microsoft who said famously a few years ago 'privacy is dead'. That's not actually really constructive. We actually need to be able to say, right, privacy is different. There's still a lot that you can do to remain anonymous if that's what you want to do but if you're having different interaction points and for government you actually need to be able to say it is that [name of person] not a different [name of person]. You actually need to be able to do that and from a big data set to a small data set, for us in our business that could be the difference between stopping something or responding to something. For us, if we're responding we've failed, we like to stop. (O-P/O **D**)

Finally, one participant called for some form of **cultural change**:

> For me it just seems to be you've got to get the right group of people around the table who come with a mindset of let's look for ways in which we can share information rather than ways in which we cannot share information. (T/O **E**)

2.3.2. Technical issues

Participants also suggested a range of strategies for overcoming technical issues, including the formulation of better laws and guidelines, education of practitioners, better data management and cultural change.

One participant suggested that technical issues are more likely to be solved if **law and policy** enabled the solution:

> There is a technical issue and a policy issue. There is a lot more we could do with technology if the law and policy enabled it. But that is a question for the policymakers, parliament and the Australian people to decide. How much they want us to use data to produce national security outcomes. (T/O **A**)

Regarding issues with data format, **standards and guidelines** had been set up, but unfortunately they were not followed through:

> …the structuring of the format … is a big thing. There actually is a provision in the Australian Government Investigation Standards which is a provision about information sharing [in] which it articulates that a guideline and responsibility for agencies to set up a central point of contact and to maintain — virtually advertise processes about how law enforcement can request information and what types of data they hold, what format you need the request to be in and what sorts of information would justify you releasing it to us. So those sorts of things if you can standardise and systemise that both on the investigator side asking for it and knowing it exists and then once it's found and approved to be given then easier for us to manage and access … all agencies are bound by it from a CEO sense where they're actually obligated to follow those rules. They're not mandatory in that they're lawful but the agency head is held accountable for maintaining — if they run investigations or are involved in law enforcement — … that standard… But it's not followed. Well, that particular principle is really not being followed through. (O/O **B**)

Some of the technical problems could be addressed by providing **better training, communication and support for frontline officers**:

> In reality I think solutions are limited. We cannot do anything about time limitations on data storage, and the data retention issue is now resolved. They key is better training and communication for front line police, letting them know what is available and what is not. We also run a 24/7 call centre … which has [more than a dozen] staff, they help explain what can be achieved. (T/O **C**)

Better data management would go some way towards resolving some of the technical issues:

> The technology side is managed by continual updates to our systems to ensure currency and interactivity with our partners. The data management issue I won't say we've resolved. I think that's an ongoing challenge … Some paths have been to concentrate on one particular type of data and companies to service [that data], which simplifies your problems but then you're locked in to that particular company which has its disadvantages. Other ways of attacking it have been making sure the terms and conditions are captured better and more available for people making the decision and to be aware of what decisions they need to make and how they can make them. (O/O **D**)

For one participant, **the lack of integration of data systems can only be addressed by changing the cultures of organisations**:

> …look, while you'd like to think that there's some type of magic system that one of these engineers out here or one of the researchers are going to develop which is going to enable all of this to happen seamlessly, I think that it's not realistic that it's going to happen that way. I think where work needs to happen is around culture. There needs to be more work done around making sure those cultural barriers and those personalities between the organisations are taken down and there's a focus on producing the best outcome for the community, or the best outcome for the [officers] on the ground... (O/O **E**)

2.3.3. Ownership and trust

Only three participants offered suggestions to address ownership and trust issues, these range from law reform, cultural change to waiting for a change in the political environment

In terms of the over-classification of documents, one suggestion is to have some kind of **international agreement**:

> As far as the classification issue, a lot of it is something that's out of the control of the Australian Government because a lot of the information that is classified and sent to our intelligence partners is actually classified by other governments. The handling instructions on that information is placed on the AIC [Australian intelligence community] by, say MI5 or MI6 so we're a little bit hamstrung in that. You would need some type of international agreement. (O/O **A**)

To deal with some of the trust issues, one participant spoke strongly in favour of **taking down cultural barriers** between organisations and changing aspects of the 'competitive culture' (O/O **B**, see quote from the same participant 7.2.2A).

Finally, one participant did not think that 'wholesale legislative change' would be appropriate, given that 'we police by consent' and 'we don't believe that [there is] public confidence in agencies to use that information wisely'. This participant expected solutions would always be uneven and 'fragmented' in achieving change. However, some of the problems could be overcome when the **political environment** changes:

> … as I said before, they'll be overcome … when there's something that brings the problem to light… when we finally recognise just how serious the problem might be. … that might be that CT (counter-terrorism) environment, where you start to realise that people are actually planning on blowing people up or chopping people's heads off or whatever it might be. You sort of start going, well, maybe that is a bit more serious, so you start to say, well, we can't really allow people to hold this information and not share it, and almost become the Royal Commission, would be the quote. You don't want to be the one … [in] a 9-11 type situation where people with 20/20 hindsight said, oh well, if they'd linked that, that, that, that, oh and that thing over there, it would have brought … so to become a Royal Commission imperative I think is one way. (O/O **B**)

Summary and implications

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 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.

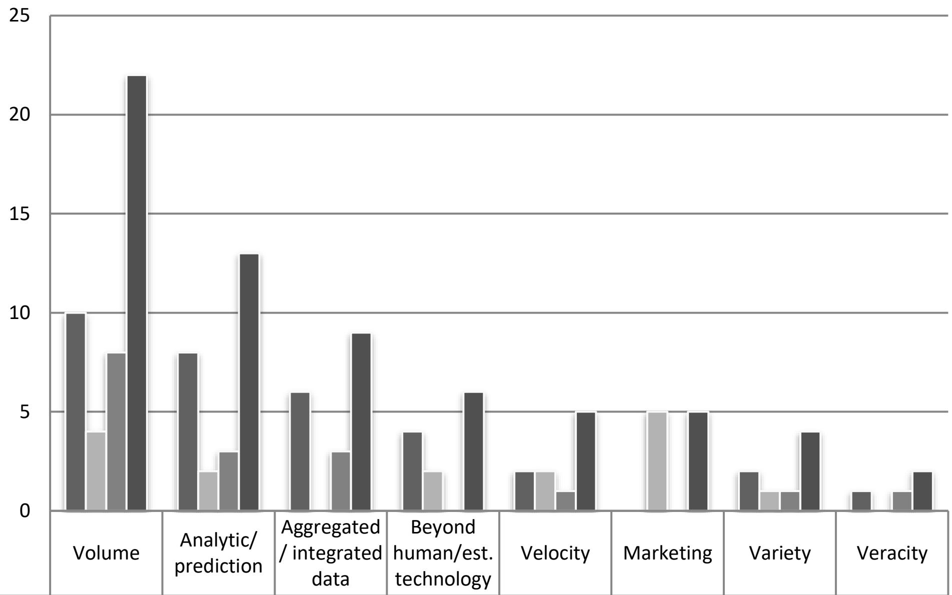
2.4. Big Data: potentials, limits and risks

This section describes stakeholders' perception of what Big Data is, what opportunities and risks they bring, and how to mitigate these risks.

2.4.1. What is Big Data?

Figure 1 provides a list of the main responses from research participants to the question: 'How would you define Big Data?' [O15, T3, P3] broken down by their role and the type of organisation they worked in. The most frequently mentioned attribute of Big Data was in terms of its volume (22/38), followed by its analytic or predictive capacity (13/38), the fact that it consists of aggregated or integrated data from different sources (9/38), and that the volume of data makes its handling beyond the capacity of humans, the skills of existing analysts or current technology (6/38). Some mentioned velocity (5/38) and variety (4/38) as characteristics of Big Data. Five participants—all from technical organisations—saw Big Data as a marketing term that covers a variety of techniques. Only two research participants mentioned veracity as a challenge of Big Data.

Figure 1: Conception of Big Data by Type of Organisation Employing Participants (n=38)



	Volume	Analytic/ prediction	Aggregated / integrated data	Beyond human/est. technology	Velocity	Marketing	Variety	Veracity
Operational	10	8	6	4	2	0	2	1
Technical	4	2	0	2	2	5	1	0
Policy	8	3	3	0	1	0	1	1
TOTAL	22	13	9	6	5	5	4	2

*Note: Multiple responses can be coded for each research participant. There were 19 participants from Operational, 7 from Technical and 12 from Policy organisations.

Volume was often mentioned together with the need for new technology:

> An ever-increasing, an exponentially-increasing volume of information which is beyond the capability of a human to analyse without computer assistance. (O/O **A**)
>
> A data set or stream that is beyond the desk level analyst to be able to effectively manage. Not just equipment and computing power, more about skills. It is about something beyond what an intelligence officer is able to manipulate. (T/O **B**)
>
> My understanding is Big Data is enormous data sets or combinations of data sets that require advanced and analytic techniques in order to make sense of them or analyse them. There's particularly techniques that maybe weren't available until recently. (P/P **C**)

Around one-third of the participants saw the capacity of Big Data to **make predictions** or 'unlock the secret that's within the data' (T/O) as its defining features.

> I would describe Big Data as the consolidation of large amounts of information in a single or multiple repositories that can be manipulated or explored to release information or findings that could not be found if the data analysed individually or

> separately. It's primarily associated with trying to find much more complicated, complex relationships – it's this trying to unlock the secret that's within the data. (T/O **D**)

> [Big Data is] a verb rather than a noun. … It's about leveraging what you've got available to you in different ways that reveals things to you that you wouldn't otherwise know. (O-P/O **E**)

While the majority of participants with a technical role mentioned volume as one of the characteristics of Big Data, a number of them admitted that they disliked the term Big Data which some saw as a **marketing term**. They would prefer to focus on analytics or predictive techniques—the size of the dataset may or may not be essential:

> Big data is something that's obviously more of a marketing term than anything specific … Big Data is not a term that I generally use mostly because I find the ambiguity around it and the interpretability around it somewhat challenging. … To me Big Data is a little bit of a misnomer because it focuses a lot on the data itself … it's sort of a distortion of what's important which is ultimately about the outcome that you're deriving. The way that you're generally doing that is through analysis so I prefer, from a personal perspective, to focus on that analysis framing as a way to understand what it is that's important and what it is that we're ultimately trying to do. (T/T **F**)

> I use terms like analytics and data mining interchangeably. I don't like the term 'Big Data' because it makes people think that Big is the emphasis when that isn't always the case. Yes, for the stock market, it is, but not really for government agencies. Someone came up with the term and has retrofitted the definition involving Vs – I don't mind that, but I hate the term. It should be 'complex data' or something else. (T/O **G**)

> It's a very broad term. It's not particularly useful as a technical term at all because it's almost like a marketing umbrella under which a lot of things can be fit. (T/T **H**)

> I think Big Data is a bit of a marketing terminology that captures the current trend for generation of a lot of new data sources and the need to make use of that. The Internet of Things is the cause of the Big Data deluge if you use all of the good *marketecture* terms and it's a way of framing it for a conversation about what's causing it, what do we do with it and how do we make use of it. … One of the things in the defence space is there are so many new sources being procured and envisaged and that sort of stuff is that they go, crikey, what are we going to do about it? It helps the conversation and it's that easy grab phrase, like Y2K or dot.com and Network-Centric Warfare, all those sorts of terms that affected people's thoughts in that space. … So it's a useful term, it's not a thing you sell. You can't buy a Big Data, you can't buy an Internet of Things, you couldn't buy a Network-Centric Warfare. It wasn't something, there are components of it and that's where our play is in that. (T/T **I**)

Almost one in four research participants defined Big Data in terms of the aggregation or integration of data from different sources. The majority of this group worked in operational organisations:

> For me Big Data is there's a lot out there, and I mean big in the terms of there's a lot. So Big Data is everything — because I actually consider what we hold, agencies, as Little Data. The Big Data that's out there is a lot of the stuff that sits in the public space, like Facebook, like Twitter and things like that. Then you move to the next phase which data being held on all of us which is held in different sort of areas like our licensing material, our passports material, our movements material. All this sort

> of stuff that sits in silos which when analysed on its own really means nothing but when you aggregate it all up can actually build a pretty good picture about somebody. … So that's what I mean by Big Data, is all of that material that actually exists. Not necessarily what we've got because what we've got is Little Data. (O-P/O **J**)

> … it's the accumulation of large datasets beyond what would normally be held within one organisation or entity containing many different aspects of information within that dataset. Therefore the analytics of it is how can you identify those useful pieces of connections between those disparate pieces of information. (O/O **K**)

> … it's the aggregation of different data sets that are together and how you make sense of the aggregation of those data sets … to analyse them to get a picture of what's in front of you. So I see it as being the whole aggregation of everything … not taking things in isolation. (O/O **L**)

> It's like if you input a name and everything comes up. Big data would be the mass pool of conglomerate information like everything is in a big bucket of data. (T/O **M**)

> … in terms of Big Data in the government space for us I would have thought we'd be accessing those key data sets that our partner agencies have. So tax information, however that might be structured, social security and welfare payment type information, the electoral roll, I mean it may not be Big Data for some people but to me it's a data set that's great. (O-P/O **N**)

Summary and implications

'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, 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.

2.4.2. Capability of Big Data

In order to delve deeper into research participants' concept of Big Data, we asked the non-technical groups (operational and policy/citizen groups) the question 'As far as you know, what is Big Data capable of doing that 'ordinary data' can't?' [O16, P4] We were aware of the danger of focusing on the *data* aspect of Big Data by asking contrasting Big Data with 'ordinary data', but decided after pre-testing with several participants that for non-technical people, it was a question that was easily understood as contrasting Big Data with existing technology. For the technical and policy groups, we also asked a more direct question 'What do you see are the opportunities or possibilities that Big Data (or data analysis/data science if they use these terms) can open up for law enforcement and security intelligence?' [T8, P8]

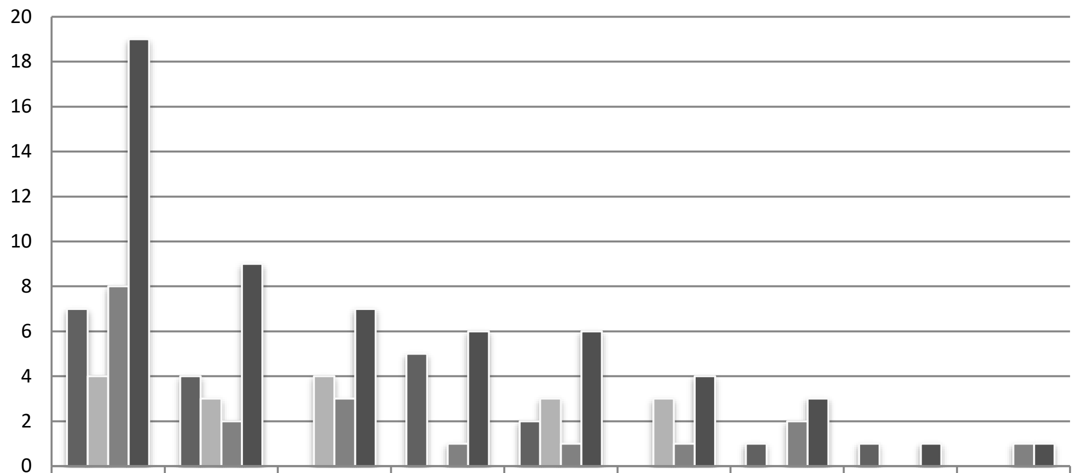
As the distribution of responses shows in Figure 2 the question elicited a range of responses that did not simply focus on the data itself.

Half of research participants referred to Big Data's more advanced analytic capacity:

> Most importantly I think predictive trending potentially. Retrospective networking or even real-time networking analysis. Associational analysis of individuals, groups, and organisations. (O/O **A**)

Big data analytics. Well, I sort of make a distinction there between … the term Big Data and the term Big Data analytics. Big Data is the data whereas Big Data analytics, of course, are the tools, techniques and procedures that we use to analyse it. What makes it different is that increasingly using better tools and techniques we can gain insight from data that to date are not humanly possible. So it helps us join the dots where we can't possibly do it ourselves. (O-P/O **B**)

Figure 2. Perceived Capability and Value of Big Data by Type of Organisation (n=38)



	Analytic capacity	Richness of data	Proactive/preventative policing	Investigative advantage	Improved efficiency/ effectiveness	Better government decisions/ services	Confidence in data	Need caution re expectations	Don't know
Operational	7	4	0	5	2	0	1	1	0
Technical	4	3	4	0	3	3	0	0	0
Policy	8	2	3	1	1	1	2	0	1
TOTAL	19	9	7	6	6	4	3	1	1

*Note: Multiple responses can be coded for each research participant. There were 19 participants from Operational, 7 from Technical and 12 from Policy organisations.

A smaller proportion (24%) did mention the 'richness' of Big Data or its 'completeness' as the advantage of Big Data, which was then linked to its analytic capacity:

> Well, it's providing a more complete picture of exactly what's going on. (O/O **C**)
>
> Well I guess then you come into these sorts of areas in terms of volume or velocity. So what these big data analytics allow you to do is to use all of your data, rather than a subset. In the past because of technology constraints, you had to restrict the amount of data you ingested into these systems because otherwise it would take weeks to run a particular model. So what you can now do is use all of the data, use large longitudinal data sets, and therefore get a much more complete picture of what's there, and therefore get much more valuable and highly qualified insights. The other is that it allows you to implement a lot more real time analytics, in other words analytics that run in the background in real time. That coincides with the advent of government's pushing more and more their services to online. So where people apply for visas or whatever it may be online, it allows you to run real time analytics in the background to analyse whether what they're saying appears to be correct. Very much the way banks do with credit card transactions. So that's the big change really. (P/T **D**)
>
> The difference is between populational data as opposed to a sampled data set. If you have complete data, the potential for analysis is not subject to the risk of modelling but is observed fact. In other words, richer analytical capacity. (P/P **E**)

The 'richness' of Big Data was also linked with an investigative advantage by participants who worked in operational organisations, by providing historical and contextual details, as well as the ability to cross-check information and identify new targets:

> … let's say for example we were analysing past activities of what terrorist suspects have been like. So analyse their movements against when they applied for their passports, who went guarantor for them, where they went to school, what their license is, when they got it, all that sort of stuff and we analysed all that for individuals. Out of that we might be able to pick up some patterns. … Then if you … develop an algorithm from that and then you ran it right across all the systems you may very well pick up targets that are previously unknown to us based upon, not dissimilar to using regression theory for mathematics in terms of statistics. So using … an analysis of previous data in terms of predictive type activity. None of us have the capability to do that at the moment even though the information is probably out there to do so. (O-P/O **F**)
>
> [Big Data's] interrogation potential. You can cross check against multiple things. (T/O **G**)
>
> You can actually build profiles and identify people, patterns of life, things like that. I mean from a private sector and a public sector perspective that actually gives you a greater level of understanding about somebody before you actually approach them. So for us — I've talked a lot about targeting, identifying people, it would probably give us, and I don't know if we're doing this at the moment, greater capability in terms of how we actually plan to interact with people. Whether we're setting up a surveillance plan or we're planning when we're going to execute a search warrant and all those sorts of things which are traditional law enforcement, trade craft which we do for a whole range of reasons, a lot of it around safety and our own people in the broader community, but also about actually understanding … a situation. Because while it gives you the opportunity to target in on people it also gives you the opportunity to not target people … I mean that's my understanding of the power

> of big data and why actually understanding the richness of the data that you have. (O-P/O **H**)

Four out of the seven research participants who worked in technical organisations and two from the policy group mentioned preventative policing and strategic responses to trends as an opportunity that Big Data could open up for law enforcement and security intelligence:

> More importantly I think there is an ability to allow these organisations to spend more of their time on the things that are related to their mission and actually therefore drive better outcomes in the community. Which for law enforcement is going to be manifested through decreasing crime rates and other things. In the counter-terrorism space it's going to be manifested through a better ability to prevent – although you can never prevent but to be able to intercept, detect and otherwise intervene in potential events before they happen. (T/T **I**)

> The biggest one, I think, is prediction and probably the most challenging. Trying to change the way policing works so that it's not reactive, but is more proactive about looking for potential anomalies or indicators that something might be occurring. So you're not waiting until the report of the crime, but you're monitoring the data to understand, well actually - and one example that we used to use when I was selling products was - by connecting different data sets you could uncover situations where children might be at risk because they're living with people that have been convicted of certain crimes, whether it's family violence, or things like that. So it's that sort of indicator that could change the way that policing is actually performed. (T/T **J**)

> I guess the shift that everybody talks about, which I think is a reasonable way of putting it, is to move towards preventative policing and preventative law enforcement national security. In other words not to react to an occurrence, but to be able to anticipate occurrences, anticipate where law enforcements resources may be required ahead of time. So to move from a lagging indicator regime to a leading indicator regime. We're not talking about Minority Report type of stuff here, arresting people because you know that they are thinking about something, but really being able to make good decisions with limited resources as to where best to deploy them. To be able to anticipate where certain types of crime or offences may occur, and to be able to get ahead of the game. … A number of police forces have moved towards much more… predictive sort of approaches in terms of, for example, being able to map certain crime patterns say around burglary in certain neighbourhoods. Actually being able to make pretty good predictions about where they'll go next, and what the most vulnerable areas are, and then to take preventative approaches around that simply by increasing police presence or whatever's appropriate. (P/T **K**)

Prediction was mentioned by only one research participant in an operational organisation, who stated "We look at trend analysis to try and predict crime areas" (O/O). This suggests that there may be a disconnect between the expectations of many of the operational and those of the technical participants. Participants in operational organisations generally saw the investigative advantage that Big Data could bring, but participants from technical organisations were suggesting that Big Data could offer a different way of doing policing and intelligence work.

Improved efficiency or effectiveness was mentioned by six research participants as what Big Data can provide:

> We are so restricted. A number of teams may request the same data but they cannot communicate. Big data use would open communication and reduce request

> redundancy. Special squads would do checks to make sure they had access to all the data. Now a big task force that does all the checks first may still be duplicating requests. The problem is that the same information maybe important to two different things. (T/O **L**)
>
> I think a lot of it is around more effective prosecution of what's already done. The low vision answer to that is well there's a lot of effort and energy that's spent on things that are fundamentally grunt work, that aren't necessary. It's necessary because of limitations in what's deployed to these organisations rather than limitations in terms of what the technology can actually do and there's a great deal of waste and inefficiency that occurs because of that. So at a very sort of low vision level that's an opportunity. There's an opportunity to actually fundamentally change the efficiency of these organisations. (T/T **M**)

Four participants (three were from technical organisations) pointed to the opportunity for Big Data for governments to make better decisions or providing better services:

> Look, my view and the view that I put to senior public servants, is that … your two most valuable assets are your people and your data. The value of the data has been unappreciated for a long, long time. As I said earlier, I think this whole discussion about Big Data and data sharing has raised people's consciousness to the gold that's 'in them thar hills', right, in all of that data. That you can actually use it for better government, better citizen services, for improving the lives of citizens, if you can understand them better … and if you talk about better government generally, and you talk about evidence-based policy development and fact-based decision making and all the good things. (P/T **N**)

Only three research participants mentioned **confidence or accuracy** as an advantage of Big Data:

> There is … a level of a surety that can be obtained through the analysis of Big Data … (O/O **O**)
>
> I would think that big data would just have a more accurate reading of whatever it is trying to get a reading of … it could give them a deeper insight (P/P **P)**
>
> So I think probably the most important component of it is that it probably provides with a higher degree of accuracy future trends in both the near and distant future than you can with a smaller data set. (P/P **Q**)

One participant with an operational role cautioned against having unrealistic expectations about the claims of Big Data:

> The problem I find … with the Big Data hype element, is that that assumption that the more data you collect—in that Big Data mentality—that the better our ability to contextualise, therefore the better ability for us to understand and to make judgements on what we derive. It's still got to come back to that first step, which is … not even asking the right questions, but you've still got to set the right rules up, against which those questions need to be asked or thrown. … So your Big Data piece should in theory allow you to get better appreciation, better decision making, better predictive, almost forecast type activities. If your starting proposition is flawed or disagreed with, or contested, then all the stuff in front of it — and I think climate change is an awesome example of that. We've got extraordinary amounts of data on what's going on meteorologically, what's going on within microclimates, within our human experience. Yet you're still getting people contest the [findings] … I know obviously part of that is ideological. Well that's another problem with Big Data…it almost presupposes truly objective data in social science ... This is in the criminal

> aspect here, not more broadly. Let's face it, even in things like … weather forecasting, with the amount of data being thrown in and the 100-odd years-worth of data readings and that ability to at least to try and have a crack at a forecast based on a trend, even in Canberra where it's blue most of the time, they'll still get it wrong. So … is it the model that's wrong? Is it the data that's wrong? Is it just the fact that we expect too much from it? (O/O **R**)

One participant (from the policy group) confessed they didn't know what the advantage of Big Data was.

Summary and implications

> In terms of capability, Big Data was seen by 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: 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 different way of doing policing and intelligence work.

2.4.3. Use of Big Data in work

To investigate the extent to which Big Data (including Big Data analytics) is currently being used for law enforcement and security intelligence, we relied on three sources of information.

First, we asked participants from operational agencies the following question: 'To what extent are you (or your unit) making use of Big Data tools in your work?' [O17] Their responses represent the primary source of information about use of Big Data for law enforcement and security intelligence. Note, however, that there could be multiple research participants from some agencies.

Secondly, participants in the policy group were asked the question: 'To what extent is Big Data currently being used for law enforcement and security intelligence in Australia?' [P5] Some of the responses were based on direct knowledge, while others were based on media accounts (see 2.6.7).

Finally, participants in the technical group who worked in or with law enforcement/security agencies were asked, 'Do you use Big Data in your work/systems?' [T4] These responses were based on participants' direct knowledge.

Table 2-8 shows the distribution of responses from the three groups. While eight research participants reported that Big Data was currently being used by law enforcement/security agencies, a larger number (13) reported that this was not the case. Four participants qualified their 'yes' answers by explaining that there were variations between agencies, for example in terms of 'sophistication' or resources:

> … there is a broad spectrum of sophistication across the law enforcement and intelligence communities… I'll call that the national security community or agencies … So within the national security community there's a vast difference in the maturity and sophistication of the use of Big Data and Big Data analytics. For example the

> intelligence agencies, in particular the [name of agency]…is probably the most sophisticated user of Big Data and analytics for intelligence purposes in the country, with other intelligence agencies also being highly sophisticated but not quite so as [name of agency]. Then the sophistication and maturity drops off and … within the national security community those at the lower end of the scale may well be the state police forces, for example. … Other agencies such as [names of agencies] fit somewhere along that spectrum in terms of their sophistication and maturity. But in general Big Data and Big Data analytics is used prolifically across the national security community. (O-P/O **A**)

> … it's very largely a question of resources. The intelligence services have many more resources proportionately speaking than the police do for this kind of work. (P/P **B**)

Table 2-8: Use of Big Data by Role and Type of Organisation (n=38)

	O/O (6)	**T/O (9)**	**O-P/O (4)**	**T/T, P/T (7)**	**P/P (12)**	**TOTAL (38)**
Yes	3	2	0	0	3	**8**
Yes but varies	0\	1	2	0	1	**4**
Perceived yes	0	0	0	0	2	**2**
No	3	5	2	0	3	**13**
Perceived no	0	0	0	1	0	**1**
Don't know	0	0	0	0	3	**3**
Not applicable	0	0	0	6	0	**6**

Notes: Frequencies in cells do not represent number of agencies, as there were multiple research participants from some agencies, eg, JCA38 and JCA53 were from the same agency, and LBA28, LBA29, LBA31 and LBA33 were from the same agency.

A number of participants not in operational agencies were unsure but two perceived that Big Data was being used, while one perceived that it was not. Three participants admitted that they did not know. Six participants from technical organisations did not provide answers that were relevant to the use of Big Data for national security or law enforcement.

Summary and implications

More than half of the participants working in law enforcement and national security agencies 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.

2.4.4. Current use of data analysis tools

Research participants were asked about the types of data analysis they currently perform. For those with operational roles, the questions were: 'Do you (or your unit) do data visualisation or data analysis? If so, what techniques or software do you (or your unit) use? Are these off-the-shelf or custom tools?' [O12]. For those with technical roles, the following questions were asked: 'What types of data analysis do you or does your organisation do? What are the outputs? How reliable/accurate are these outputs?' [T5] and 'What data analytic and data visualisation tools or software do you use when dealing with large datasets? What do these tools provide you with? Are they useful?' [T9]

A review of the responses suggests that participants working in operational organisations were not always aware of specifics, whereas those working in technical organisations were developing tools rather than using them for national security or law enforcement. The following discussion is therefore focused only on those who worked in operational organisations.

Table 2-9: Current Use of Data Analysis Tools by Role in Organisations (n=19)

	O/O (6)	T/O (9)	O-P/O (4)	TOTAL (19)
Data analysis (in general)	6	6	1	**13**
Data visualisation/Mapping	6	5	1	**12**
Data browsing/ searching/ sorting/ linking/ summarising	4	2	1	**7**
Network analysis	3	1	0	**4**
Predictive/ automated/ machine learning tools	1	2	0	**3**
Not in my unit	0	2	1	**3**

*Note: Multiple responses can be coded for each research participant. Only those representing operational organisations are included in this table. LBA02 (O-P/O), JCA54 (T/O) and JC62 (O-P/O) were not asked these questions as they did not work directly in this area.

As shown in Table 2-9, the majority of participants who worked in operational organisations reported that they (or their unit) currently made use of data analysis tools, three reported that they did not use these tools in their unit, while three others were not asked these questions because they did not work directly in this area. Among the specific tools used, data visualisation (including geospatial mapping) was mentioned most frequently, followed by various data browsing, search, sorting, linking and summarising tools and network analysis. Only three participants mentioned specifically that they currently made use of predictive, automated, or machine learning tools in their work. The vast majority reported using a combination of off-the-shelf and custom made tools.

Summary and implications

A variety of data analysis and visualisation tools are currently used in national security and law enforcement 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.

2.4.5. Barriers/challenges to Using Big Data

To understand the barriers or challenges to the use of Big Data, we asked participants several questions. First of all, we collect responses from participants from the operational group to the question: 'What are the most serious issues/problems that may prevent you (or your unit) from making more use of Big Data?'[71] [O18]. This is supplemented by responses to two questions we asked of the policy group: 'What are the barriers (to the use of Big Data

[71] Questions were worded slightly differently in the first few interviews.

for law enforcement and security intelligence)?' [P8] and 'What are the challenges … of Big Data technology to support law enforcement and enhance national security?' [P9][72]. Finally we draw on responses by the technical group to the question: 'In your organisation/system, what are the main challenges you face with respect to Big Data or data analysis?' [T7].

Table 2-10 shows the distribution of responses. **Legal or privacy issues** were most frequently raised (by 12 participants). For example, one participant said that it was virtually 'legally impossible' for law enforcement agencies to access certain types of data:

> Well, I mean, in a perfect world we would have access to a lot more data than what we currently have access to. For instance … we spoke about Google and the banks. Now, having access to some of their data would be reasonably beneficial. We'd get an idea of pattern of life of individuals, what people are … viewing online would be really interesting to know particularly some of our targets. A lot of this is obviously legally impossible and I know that there's some grey areas here in relation to what law enforcement can use and what we can't use. (O/O **A**)
>
> … also a limitation on … the privacy principles. Because there has to be for a law enforcement purpose so some say that the definition of that is that that doesn't include trawling our data because we can't point to a specific law enforcement purpose ... (O-P/O **B**)

Table 2-10: Barriers/Challenges to Use of Big Data by Role and Type of Organisation (n=37)

	O/O (6)	T/O (9)	O-P/O (4)	T/T, P/T (7)	P/P (11)	TOTAL (37)
Legal/privacy issues	3	4	1	4	1	**13**
Public acceptance/ trust	1	3	2	2	3	**11**
Access to/sharing of data/data silos	1	4	1	3	0	**9**
Technical and other resources	1	5	1	0	1	**8**
Data format/data quality	2	3	1	0	0	**6**
Confidence in technology	2	2	0	1	0	**5**
Cultural issues	0	0	0	2	1	**3**
Understanding of user needs	1	1	0	0	0	**2**

*Note: Multiple responses can be coded for each research participant.

Another current barrier to the use of Big Data mentioned by 11 participants was the **lack of public acceptance or trust in the agencies**. This was raised by participants in all three groups, but especially by those working in operational organisations:

> I think [the challenge]'s probably around actually understanding primary and secondary use of data and … having a conversation across government around how actually we're going to manage that and explain it to the community. Because I guess it goes back to that — my ideal world would be you touch point with

[72] These questions for the policy group were added after some initial interviews, so not all participants in this group were asked this question.

government and everybody knows that's that person, that's there, get that quite easily. Then have some access to different layers of information depending on what you need. But that scares the crap out of people, that's Big Brother on steroids or whatever you want to call it. But I mean we've always got to recognise … that agencies have their primary function. The bit that we have around [counter-terrorism] is being able to use the information that we have as government agencies to protect the community. We protect the community in a number of ways. I mean it's around preventing attacks, it's around actually intervening if we can so that people make a better life decision than going to Syria on a Contiki tour of terrorism. But it's also about assuring that the limited resources that governments have are actually used for the purposes and the people that need them. (O-P/O **C**)

If you want a [government data] system that works and that people will voluntarily participate in like any system … you need to feel that you can actually understand it, it's transparent and you can influence it. If we hold a view about you but we don't tell you what that view [is] and we just say you're risky, (1) you've got no trust in the system, (2) you don't understand why we've formed that view, and (3) you can't influence it, why would you participate in it? … I think this is one of the challenges the government will face or is facing up to right now … how do you benefit society from the availability of all this data, how do you put it into their hands in a way that is safe? (T/O **D**)

We talked about the law enforcement agencies and the corporations before and the fact that the public sees these risks for law enforcement agencies having access to this data when they don't see that risk for corporations having access to data, which is unusual. … when we were doing the data retention stuff, the public is just losing their minds about these sorts of concerns. But a lot of them were kind of like shadow concerns, in the sense that this information is in the dataset, it's scary. This is going to be held for two years, even though large parts of their information are held for seven years for taxation and no one cares. So … this is complicated and the public doesn't understand currently, maybe through lack of communication or maybe because no one really wants to put in a big effort to understand the intricacies of this or maybe because it's just more fun to scare people about Big Data than it is to engage sophisticatedly with the problems. (P/P **E**)

The challenges, I think, are going to be in community trust. They're all around trust. Can we trust law enforcement and authorities to actually do this without breaching our privacy, without overstepping the mark? There's an intrinsic distrust of authority and their use of power. So I think that's a challenge, that will be your biggest challenge. (P/P **F**)

In law enforcement and national security, we could use the current data retention legislation as a case study. There is a massive trust issue with the community which of course Snowden has amplified. The community does not trust government with what the community regards as private data. That is a challenge. Then of course Snowden provides a current illustration of the point – the community needs to trust as to the potential for abuse, trust that the government is able to keep it secret. (P/P **G**)

So certainly, massive issues around … around the ability to share information between agencies. That's going, in the first case, to be probably the biggest benefit but also the biggest challenge, and a massive challenge. I think the use of, or sharing that data will invoke a lot of scepticism from the public around, why should this information be shared for policing or counter-terrorism purposes? For example, tax information and should that be available for different purposes than it currently is?

> It's going to be a very hard road to sell that message. I think as people become aware their use of publicly available services, you know, Foursquare, Google and LinkedIn and all those sorts of things. If that comes to be harvested, by Defence and Intelligence for their purposes that will actually cause some anxiety as well. So it's really that — will the public change the way they behave because of perceived usages by government agencies, or is the benefit that they derive from using those services so great that they'll put up with whatever usage occurs behind the scenes? (T/T **H**)

The next most frequently mentioned barrier relates to issues surrounding **access to or the sharing of data** among agencies, some of which relate to legal or privacy issues. For example, law enforcement agencies must request specific pieces of information from other agencies rather than have access to databases:

> … the way it works is we will request specific pieces of information within the data. We don't say I want access to your database. I'm sure out there, there would be the ability if all the databases were aggregated up, hypothetically, and let's say for example we were analysing past activities of what terrorist suspects have been like. So analyse their movements against when they applied for their passports, who went guarantor for them, where they went to school, what their license is, when they got it, all that sort of stuff and we analysed all that for individuals. Out of that we might be able to pick up some patterns ... Then if you … then develop an algorithm from that and then you ran it right across all the systems you may very well pick up targets that are previously unknown to us … So using … an analysis of previous data in terms of predictive type activity. None of us have the capability to do that at the moment even though the information is probably out there to do so. (O-P/O **I**)

> With everything that everyone's doing there's more and more metadata and actual content that's out there for everyone. So gaining access lawfully to that material is a big challenge for us. Finding ways to receive that data, finding ways to deal with those ever increasing sets of data … I suppose a big challenge for us is then from that myriad of metadata or data itself creating linkages between disparate sets of data and bringing those together for our investigations. … There's a whole bunch of opportunities for us to obtain more and more data but part of that opportunity is the challenge that we have to be able to access that data and get what we need from it and link all that together in a sensible fashion, or fashion that can be used. (T/O **J**)

The way data is currently collected also created a barrier to sharing of information:

> … we collect data in silos as an organisation and how we can actually get better use of that siloed information collectively could be something that … could then be our Big Data … so our telecommunications interception system would operate here and, at the moment, our computer exploitation system acts here and our listening device data set [connects] us here and then our human sources is here. What my guys type in the computers is over here and what we get from witnesses is there. So you've almost got six disparate lots of data and really no way of bringing that all together and aggregating it up. Now, it's done by people looking at different systems and the human brain trying to work out what the connections are. (O/O **K**)

A number of participants (8) nominated the challenge of maintaining **technical, human and other resources** as one of the barriers:

> Well we've got good analysts but they're in short supply. They're a valued commodity right across - particularly across the national security space so one of the

issues for us is trying to maintain capability in an analyst sense that we can use for serious and organised crime that's not being poached by others in the national security space. (O-P/O **L**)

Probably the lack of skills, shortage of capability, personnel capability … There's a worldwide shortage and I don't believe that's going to be closed quite frankly. I think the software will close the gap more than the educational institutions will close the gap. (T/O **M**)

For us, some of the challenges are the ability to receive the volumes of data that we might want… so our network for delivery of product into us is a challenge. Storage is another challenge that we are working on. I suppose for us, in obtaining the value that we get from the data we create a myriad of information that has to be stored as well. So again our databases and the size and structure and long term management of our database is a major issue for us. Like I said, everything we do and every system we have has to be maintained for an indefinite period of time and we have legacy systems that go back 15, 20 years that we have to look to try and maintain the ability for people to access that data and provide evidence from it or just gain access to it. We just have to keep maintaining those for as long as we can, as long as we need to unfortunately. (T/O **N**)

One research participant also referred to cost as one of the current impediments to using Big Data:

… telecommunications companies charge for information, which stops us making broad requests. The requesting department/team has to cover these costs in their budget, this is part of the approval process. This is a big limitation factor and a disincentive to Big Data type requests; so we get small window, section or slice information requests made case-by-case to limit expenditure. We do the invoicing, forwarding journals out to the requesting teams for payment. So we cannot do Big Data because it is too expensive. In some cases, the seriousness of the offence overrides cost concerns. (T/O **O**)

The **consistency of data format and data quality** presented another type of challenge to the use of Big Data, according to 6 of the participants, all working in law enforcement or national security agencies:

Still an inordinate amount of our time is spent cleansing data, wrangling it into shape so that you can actually make use of it. So you can match it, it's always a problem. (T/O **P**)

Accuracy is an ongoing concern. In particular that analysts will believe and not think too carefully. If you are a new analyst you may just believe and act. Challenge is building systems that can communicate uncertainty. (T/O **Q**)

A number (5) of participants mentioned **confidence in technology** as an impediment to the use of Big Data, four of the five are from law enforcement or national security agencies:

I mean we're trying to predict the future which has traditionally been a fairly challenging thing to do. If you say you can predict the future and what you predict isn't at least somewhat accurate, it's not the most useful thing. There are plenty of people who can just guess what's going to happen. Unless you can do better than those guesses it's not really useful. (T/T **R**)

Yeah I think that the biggest issue that you'll have with the take up of the analytical tools by the analysis or by the analysts currently will be their level of assurance that the tools being developed are going to do what developers say they can do. (O/O **S**)

As some of the participants pointed out, they did not rely totally on technology to do their work:

> We do not rely on technology to make decisions or do analysis. We do things very much with a human in the loop in the organisation … The investigation process has multiple steps. Essentially looking at identifying a person, locating them, who they are associated with, who they influence, who influences them, intent and capability. Through data should be able to automate simple/formal things like identifying and locating. It will take a while to go beyond that. I would be cautious about relying on anything computer generated to gain a complete understanding about intent and so forth. Not in my lifetime. … We are acutely aware of the consequences of our work. We can ruin someone's day … we cannot delegate that to machines. But there is potential for machines to perform other functions like identification, locating links. (T/O **T**)
>
> … in the end you need someone actually processing the data, whether that's automated or not. You still someone sitting behind it to evaluate that data, and to obviously be aware of what that data … it potentially is just information. Obviously the difference between information and intelligence needs evaluating. (O/O **U**)
>
> I don't think that we can primarily rely on analytical tools for the actual analysis of that information to provide something which is actionable. I don't think the tools will ever get to that point where they have 100 per cent accuracy in doing that. What you want is that if there are a thousand pieces of information we want the analytical tools to do the analysis, to understand the context and prioritise to say do this one first, this one second, this one third and go through the thousand pieces of information because we think the top ones are the best ones ... (O/O **V**)

This led to another barrier mentioned by two participants, the **need for technical developers to understand user needs**:

> I guess one of the biggest gripes that we always had internally at [name of agency] was that the technicians aren't analysts but they're the ones that are tasked with the development of tools for analysts. So a technician would go hey I've got this great tool for you, you should try it out and it's got more widgets, buttons, more things that were a hindrance than an actual benefit to the analysis … they may have found to be cool and they may have been able to integrate and understand but it didn't take into account what the analyst needed so we always had that fight internally … and it's the same gripe that you'll have with these Big Data tools developed now is that they need to be informed by the person that's going to be sitting in front of a computer using them, not the person designing them that wants to create something flash, bang and whizz and shiny and bright. (O/O **W**)
>
> The challenges are … [being] able to provide the training and expertise to the people who are going to be looking at that in an operational sense. Because at the end of the day, I can have a great technical system that brings in all the data in the world and creates all these outputs but … if it doesn't work in with all the information that our investigators have in a way that they can understand, in a way they can draw the conclusions that they need, having all that data is of no use to them whatsoever. That's one of our key things is being technologists … we've got some very smart people who you would definitely call geeks but they think they understand what people want from data but they understand the data in a completely different way … One of our challenges is making sure that what we provide from the data actually meets the requirements of the organisation. (T/O **X**)

While legal and technological impediments were mentioned most frequently, three participants (not members of law enforcement or national security agencies) saw **organisational cultural issues** as another major problem:

> A big challenge right now is that it's very, very difficult for any individual organisation to draw together all those strands of relevant data and be able to look at things that can only be determined through the analysis of that complete — not even complete but more complete view of the problem. That's a space that there's a lot more that needs to be done. A lot of it is not necessarily around the technology. The technology exists to support that right now. The products that we build support that right now. The challenge is more around the cultural and organisational and in some cases legislative barriers around making that happen. (T/T **Y**)

> There are regulatory barriers some of which are totally legitimate, others are not and there are cultural barriers which are not legitimate and need to be addressed. If [we] look in the privacy area, there is a perception that unit record data about an individual or household cannot be revealed because of risks to privacy. That is true if what we are talking about is publishing data or analysis of data that would enable an individual to be identified. But if the record is part of a Big Data set analysed for trends and policy insight, the power of unit record data could be exploited without breaching privacy and security. It requires people to think differently about how [to] protect privacy. Just saying no as a first response is wasting potential of the data. How do you think this would be done – through de-identification of unit records? It could be de-identification or just not publishing them, depending on the nature of the analysis. So a regime that enabled access to unit record data but was scrupulous in terms of what was published. Or one could publish de-identified records. Both are valid techniques. Now, one can reverse engineer and discover unit record data. It is an issue so it is hard. But it isn't so hard that we can't take it on. (P/P **Z**)

> For me I think it's about a cultural change within organisations of actually sharing internally even first. So there are departments that have large sets of data that they've got together as a result of often a merger of departments and even externally so it's just sharing between departments. You're starting to see a bit of a shift now with [names of agencies] are starting to share a little bit of their information with each other because it helps with fraud detection particularly. Even internally those organisations still aren't comfortable sharing their own data with people because in their mind, and it's not necessarily a bad thing, … they're trying to protect their clients, the citizens' privacy. However they're taking possibly a little bit too hard a line on it rather than saying, well, how can we share it in a way that's useful more holistically rather than individually? Then we are seeing some opportunities as a result. So I think there is a mind shift changing but I think from my perspective that's one of the big challenges to overcome in the future. (T/T **AA**)

Summary and implications

Many of the barriers and challenges to the use of Big Data listed by 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 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. Here and in the following section, research participants stressed the potential negative impacts of both false positives and false negatives, and the adverse reputational impact that could follow.

2.4.6. Risks of using Big Data

To examine participants' perception of the risks of using Big Data, we asked a similar question of each group: 'What are the risks of using Big Data for law enforcement or security intelligence?' [O19, T12, and P9].

Table 2-11 provides an overview of the responses from the three groups. While participants in operational organisations mentioned all of the listed risks, those who played a policy role were most concerned with privacy, data security, and misuse of data, and those with a technical role were most concerned about misplaced trust in Big Data technology.

Table 2-11: Risks of Using Big Data by Research Participant Organisation (n=38)

Risks	O (19)	T (7)	P (12)	TOTAL (38)
Privacy	5	1	6	12
Misuse of data	2	2	6	10
Misplaced trust in technology/ assumptions behind analytics	6	3	1	10
Data security	3	0	6	9
Political and reputational risks	6	0	1	7
Public perceptions	5	0	1	6
Overload	4	0	0	4
Data integrity	2	0	0	2
Discrimination	0	0	1	1

*Note: Multiple responses can be coded for each research participant.

Invasion of privacy was a risk nominated by 12 participants:

> I think also citizens' privacy has got to be balanced with law enforcement needs. That was a strong theme that came out of the Court of Justice of the EU's judgement on the EU data retention directive, which invalidated that directive. Although the court viewed that the … fight against serious crime and terrorism was what they called a legitimate objective, the scheme itself was disproportionate interference with the privacy of European citizens. I think that has to be balanced. I'm not convinced that in Australia we have the right balance, particularly in light of the … data retention laws … (P/P **A**)
>
> If properly/intelligently interrogated, it can tell you almost everything about an individual. People do not necessarily realise it. … Someone said that eventually everyone will be able to access everyone's emails, and that nothing will be private. Could be an individual now who already can. The thought is horrific. (P/P **B**)
>
> Well, you could build a profile of a person's life in minute detail, who their friends are, what they like eating, what they like viewing. ... Then if you mash that up with what you search on the internet, so if you mash that data up with what maybe

> Google are collecting, and then you [link] that up with what government authorities have got on you … – it'd be Big Brother in every sense. (P/P **C**)

> The challenges of course in building new tools, techniques and procedures for Big Data analytics is that those capabilities may well be extremely intrusive in relation to individual's privacy. So the catch cry that we've used is that just because we can build those tools doesn't mean that we can use them ethically or legally. .... I think an example is that many people think the privacy they have in the hard copy days, the expectations there should be maintained in the digital days and I just don't think that's possible anymore. (O-P/O **D; see also 7.2.6K from the same research participant**)

Misuse of data was nominated as a risk by 10 research participants.

> When you start to rapidly increase numbers in the value chain or the intelligence chain, you start to lose the ability to control the quality of those people going in. … [S]o there's a risk that (one) information is going to be lost, (two) there's an increased risk that information is going to be mishandled or misused. (O/O **H**)

> … it starts with what I call corrupt or malevolent official use. Every now and then you hear about some delinquent policeman accessing information not permitted to be accessed by him about a connection, so there's that. Is that serious? Yes, though individually they tend not to be very serious, but collectively they're terribly damaging for the unfavourable suspicion it excites and disaffection it creates with the apparatus of law and order. The thing that's most damaging about corrupt and malevolent policemen in their access to data they're not permitted to have access to is that it lends substance to what I regard as misconceived opposition to the collection and retention of the data in the first place. It's hard not to sympathise with somebody saying why should we let them collect and keep this material when these bastards misbehave like this. … There's no excuse for any infringement and so … there need to be both disciplinary and criminal offences which are treated extremely seriously. … By and large we are very good secret keepers in our society. (P/P **I**)

> … one of the premises of the *Privacy Act* is about people having control over their personal information and an understanding of why it's being collected and how it's being used. Although the power relationship is often unbalanced in terms of people being asked to provide their personal information in order to get a service or in order to interact with government, nonetheless one of the safeguards is the transparency part of the equation. So then, if it's then used for unintended purposes that has the potential to undermine community trust and confidence. (P/P **J**)

One participant gave numerous examples of how data could be misused, including the risks of 'vendetta policing', harassment, criminalising association, and the 'repurposing' of data:

> I think there is also risk – a much higher risk of what I can vendetta policing which is where law enforcement or intelligence has some sort of bee in their bonnet with a particular person or group of people who may or may not have broken the law or just people of interest. Instead of just being able to target one sector of their lives, because of having these multiple big data sets, they'll be able to completely encircle them. Then there's risk either directly or indirectly of harassment. … My deep concern with the opportunities that exist for improved mapping of criminal networks through data linking and analysis of big data is that you will end up back in the bad old days of criminalising association rather than recognising your best friend or your husband might be a convicted criminal. They might even be an active

> criminal but that doesn't make you a criminal. We didn't really talk about repurposing but that is a really vital issue… (P/P **K**)

Ten participants saw a risk in users' **misplaced trust in technology**. Users need to be aware of assumptions underlying analytic tools:

> … once you deploy a tool last week's assumption might be different from next week's assumption so things are going to be constantly and instantly changing. Who … is working at the back end to make sure … constantly that information is prioritised within even current political contexts, within the current use of emoji's and slang from people around the world? … No system is infallible but that needs to be constantly updated as well, those assumptions need to be constantly updated. That's a limitation of the system I guess. (O/O **L**)
>
> I did read [a book] about Big Data … This particular book was positive that with the increasing volumes of data and the ability of machine learning that really you had the opportunity to just go with correlations. We observe that most people who make it CEO are men in organisations; their glass ceiling is alive and well. There's a correlation there. Would you draw conclusions from that? Well you could probably draw some but I think you'd be unwise to draw some others. You'd be unwise to say therefore men are smarter than women, quite honestly who'd go there? … That's the sort of correlation that if you drew the wrong conclusion from a correlation that could get you into difficulties. I think if I was to believe that hypothesis that says the use of Big Data means that previously statistically valid approaches to information understanding are no longer required I think mm-hmm, I'm not convinced. (T/O **M**)
>
> I've talked about predictive policing as being a benefit, or a way things might happen in the future. The risk really is there that it overtakes the due diligence of the law enforcement agencies to check what comes out of the machine, so to speak …[They need to] look back and analyse them – check the assumptions. (T/T **N**)
>
> I think there's two categories there, there's mistakes where the systems made bad predictions or the analysis is incorrect and therefore a wrong decision gets made based on that. I think that's fairly self-evident, that problem. But the other one which I think is probably more insidious is … with Big Data, suddenly all those minor laws [like jaywalking] become detectable and enforceable. So it's quite easy to see that suddenly almost everyone is breaking the law in some minor way. It's not clear to me what happens with that… I think that … it's important to have humans in the loop. We're designing tools that are designed to support humans, rather than to just substitute for them. But you could certainly see the potential that people might choose to start building tools to substitute humans and that goes wrong. (T/T **O**)
>
> I think there is a risk that smart systems will deskill people… Rule of law is undermined if … people stop listening to intuition. Instinct is replaced by a screen … Data analytics can be used really poorly … If a decision is made because 'computer says no'[73] then this will not stand up in court so the agency and decision maker is affected (possibly with gaol depending on circumstances/nature of decision). Also the person about whom the decision was made. Even the people creating the technology – are they responsible? For example, who is responsible for stock market algorithms? (T/O **P**)
>
> I think there are risks around expectations … historically in [name of organisation] we've talked about it as the 'find terrorist' button. That was the genesis of our

[73] This is a reference to an episode of the comedy *Little Britain*, see <https://www.youtube.com/watch?v=0n_Ty_72Qds>.

> organisation was working on counter-terrorism problems and probably for the first three or four years of our existence the most requested feature was some manifestation of which button do I press to actually find the bad guy? There is, particularly among non-technical people, a yearning desire based on movies and otherwise to actually think that there is an ability to just automatically do their job for them. The reality is that that's far, far from the truth and far, far from desirable … So there's a risk that the expectation will never be met and there's a risk that the expectation is just misguided to begin with. There's a risk that people will unquestionably trust systems that are providing automated or semi-automated outputs as well and there's a rigour that needs to be maintained in keeping a human in the decision-making loop who is trained and competent at actually looking at what the data is, where the data comes from and the characteristics, traits, properties. And a fairly deep understanding of what it is that they're doing and what the data is that they're making the decisions on to be able to make informed and reliable judgment calls on how to interpret the outputs of an automated or semi-automated or even just an integrated set of data. There's no substitute for having an intelligent human being in their intuitions and understanding of the world and you very much, as I've said before, want that person to be there. There's a risk that that is not well understood and there's a risk of software companies coming to the table and saying, well, technology is the answer and due to that mismatch of expectation too much willingness on behalf of these agencies to accept that as true which could ultimately have pretty bad outcomes. (T/T **Q**)

Data security was a risk nominated by 9 participants.

> Certainly some practice in Australia … does not fill me with confidence. There have been important data breaches, particularly that major data breach last year of asylum seekers' data … arguably a particularly vulnerable group of non-citizens here had personal data about themselves exposed by the Department of Immigration. That does not fill me with a lot of confidence about the security of data. The *Privacy Act* in Australia – my understanding of that is that data security is included as one of the Privacy Principles, but is not strongly enforced. … There isn't necessarily obligations to keep data on shore. There is for e-health records in Australia, but not necessarily for other kinds of data. My understanding of the data retention law here is that there is no requirement to keep the data retained onshore. That also brings up other risks about ensuring data is being stored securely offshore—maybe it's more difficult to ensure rather than onshore. Also, the possibilities of access by foreign Law Enforcement agencies or other foreign actors if it's stored offshore ... (P/P **E**)

> I get very worried about lack of security of data because though the custodians and those related to the custodians are, as I say, pretty bloody good really if you look at the track record, there are bad people out there. Those who would hack into customs database for the purposes of drug smuggling, for example, are legion, and so it follows that quite apart from my Pollyanna view about the culture of respecting secrets, we also need alongside that a very robust technical security for I'll call it electronic data, digitised data. … I'm troubled by the fact that sooner or later some really dreadful malevolent person is going to get access to a lot of stuff. (P/P **F**)

> I think from the perspective of the privacy principles and the regulation under those principles, one of the key challenges is securing the data. So amassing greater quantities of data, drawing greater linkages and storing that data all creates a higher risk of that data being attractive to criminal elements and others. So as a result under the *Privacy Act* you have to take reasonable steps to secure personal

> information. What's reasonable depends on a number of factors including the sensitivity of the data held, who is holding it and for what purpose, their resources, and the consequences should that data be accessed by unlawful means. With the ever-changing technological context, that's the challenge. So for example, a case that we looked at recently dealt with an issue of encryption and a decommissioned database that used encryption. That database not being an active one hadn't had new security protocols applied to it and the encryption methodology that was used at the time to store the data was no longer secure. It could be easily penetrated by those with the technological means. So it requires an increased resource from government … and potentially business depending on who's storing the data. (P/P **G**)

Seven participants mentioned **political and reputational risks** associated with the use of Big Data, six mentioned **public perceptions** and four nominated **information overload** as possible risks. The three types of risk are somewhat related:

> … a risk that the public don't understand exactly what your role, responsibilities and limitations are within those agencies and politically there is no mouthpiece to explain to the public well what it is we do… You need to sell why these things are needed very well and it's not as if we as analysts could go out and do it or the heads of the departments could do it, or the heads of the organisations would do it. We rely on politicians to do it and unfortunately not all the time there's a coherent communication of mission to political ambition as well … Because I can tell you now that the intelligence agencies only make the papers and you are only in the headlines when something went wrong not when something went right. When we did our jobs we were never in the paper. When the military did something or something was stopped it was never publicised but a bomb goes off in Bali, the second Bali bombing, and all of a sudden it was an intelligence failure. Or if something happens … it's an intelligence failure. The failures at that point in time were how can we do this better and how can we do this? So it ebbs and flows. I can tell you now that if things start to go wrong here in Australia and there's more adverse terrorist activities then public sentiment will swing one way. In 12 months if nothing has happened public sentiment will swing the other way. (O/O **R**)

> The risk is false promises that if we have data, an attack will not occur. The purpose of collection may change … People are uncomfortable with data being used for a different purpose. … The risk is public discomfort with change, it is hard to adapt. (T/O **S**)

> Some of the risks for us … is that public perception of our requirements and our oversight and our access to data is far from the reality. That means that if we request additional powers to access data, the public perception is that we already access too much and … that we're turning into Big Brother ... For us to actually make legislative changes the risk is that it's very difficult for us to make the changes that we need to keep up with technology and with crime. Even if the government and legislators agree with us, public perception and the fact that governments are there at the whim of the public opinion is a risk for us in getting through the legislation to allow us to gain access to the data that we need in order to perform our function. (T/O **T**)

> Do we carry that risk of law enforcement knew about that person, it wasn't picked up through Big Data analysis, yet we knew it. … [T]hat's probably one of the biggest risks, I think, of Big Data, that from an organisational point of view, if you know something you haven't acted on that information, therefore are you liable in the public sphere that you knew the risk and you did nothing with it, regardless of

> where that data sits, or where that risk sits. It's in one piece of data in millions and millions of other bits of data, then obviously that is a risk. (O/O **U**)
>
> Well the risks are that there'll be an expectation that if we have access to everything that we've mitigated our risk down to zero of something happening or occurring. So they'll say you wanted access, you've got it all, so it's the old 20/20 hindsight. When something happens someone will go back and do a full examination and everything will be there, why didn't you pick it up, which happens all the time. That's a risk that comes with everything so be careful about access to material. If you don't have the ability to analyse it properly then you're better off not having it to be quite frank. … So unless you've got the tools that have the ability to analyse and come up with some sort of accurate assessment then there's no point in having access because all you'll do is carry all the risk and it's something you can never fix. So that's a rather big risk. (O-P/O **V**)
>
> I think there's also a risk in relation to the community in relation to the view they'll have that Big Brother is watching them. So it's almost a political risk I suppose and that therefore becomes a reputational risk as to how we use it and obviously if we did get a situation where someone exposed — like a Snowden …, that would be obviously a significant reputational risk. (O/O **W**)

Two research participants mentioned **data integrity** as a risk, while one participant identified a risk of **discrimination against people in particular communities**:

> I guess if you use big data and you then form policies on it, it sort of paints everyone with a single brushstroke. … As long as they have a beard and relatively dark skin you get searched. … [T]he risks are that we simplify … how we view people. (P/P **X**, also referring to the fact that the insights gained from Big Data could be 'skewed')

Summary and implications

Overall, privacy, 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.

Overall, research participants collectively identified most of the risks discussed in the literature (see Methodology Report 2.3). The risk of inappropriate local application was not identified, but was largely irrelevant given the types of analysis research participants described. A more significant issue is the variability of identified risks between individuals and organisations, suggesting that broader awareness of the diversity of risks across sectors would be beneficial.

2.4.7. Who is exposed to these risks?

For the policy and the technical groups, we asked 'Who is exposed to these risks?' [T12 and P9]. Table 2-12 provides a cross-tabulation of the people identified as being exposed to the risks of Big Data by the role of research participants. The most frequent response was 'everyone', 'the community', or 'citizens as individuals'; this is followed by government and government workers in general, and law enforcement/national security/defence agencies or personnel; marginal people, children and young people, or people of certain socioeconomic status; academics or researchers; people identified in data or lone citizens; and informants or undercover police. Some examples of these responses are provided below.

Table 2-12: Who is exposed to risks of Big Data by Role of Participant (n=16)

People at risk	P (11)	T (5)	TOTAL (16)
Everyone/the community/Australians/citizens as individuals	6	3	9
Government and government workers in general	4	1	5
Minorities/marginal people/young people/people of certain SES	3	1	4
Law enforcement/national security/defence agencies/personnel	1	2	3
People of interest to law enforcement/security agencies	1	1	2
Academics/researchers	2	0	2
People identified in data/lone citizens	2	0	2
Informants/undercover police	0	1	1

*Note: Multiple responses can be coded for each research participant. Questions were posed to the policy and technical groups only. Not everyone responded to this question.

Everyone

> Who is exposed? Australians; potentially anyone. (P/P **A**)
>
> The community – that is citizens as individuals. (P/P **B**)
>
> Everyone I think is exposed to the risk in some ways, so the public in general, they're exposed to the risks if their data that they – in some ways I think the public don't even understand where their data is, or what data's out there, or don't care. So there's a risk there when they actually find that their data is being used, that they didn't know it was there. (T/T **C**)
>
> I think everyone is [exposed to the risks]. (T/T **D**)
>
> I think everyone's exposed to a risk in one way or another. It depends on the angle you want to take. If I take an extreme example, if you have your entire population on a database and that falls into a … a hostile country or organisation, then they suddenly have a lot more information about your entire population they may not have had before. Although a lot of that information is publicly available anyway. (T/T **E**)

Government and government workers in general

> Well it's potentially an exposure for government … one of the challenges that government has is attracting and retaining skilled technologists. The cyber security review that the government is currently conducting and a white paper goes to that issue about the skilled workforce of government. So there's a potential issue there. There's exposure for government should there be a data breach and the publicity that would go with that. Potentially internationally in terms of how that was perceived by our international counterparts. (P/P **F**)
>
> … the government as a whole if it goes badly and the community loses trust in government and agencies, that is not good in long run either. (P/P **G**)

Law enforcement or security agencies/personnel

> I think there's a risk for the police and law enforcement and intelligence agencies — really about perception. If they are seen to be using data that society didn't think they had access to. So it's about setting the agenda really, so that people understand what data is being used and what purpose it's being used for, and what benefit it brings. (T/T **H**)
>
> The other issue is …, I think, a reasonable paranoia on the part of the law enforcement national security agencies themselves, is the embarrassment of a false positive. A lot of the sophistication in the system really is about reducing the number of false positives, and for that matter of false negatives. So that's an area that gets a lot of attention. That's really an area where you might even end up catching totally innocent people, just through a set of circumstances that made a suggestion that turns out to be unwarranted. (P/T **I**)

Minorities/Marginal people/children and young people/low SES

> I guess it's those people on the fringes, if you will, that may not be totally clean but they're not threats to national security or hardened criminals either. They just don't behave in a way that's totally socially acceptable, and that they may get caught up in this and be treated rather more harshly than is appropriate. (P/T **J**)
>
> Yeah, I think children and young people obviously are very vulnerable to this. I think they live their lives online. They don't differentiate between online and offline. They don't read terms of use. They don't read things about what data is being collected. Even if they do I'm not sure that they fully understand or care at the moment. It's a bit interesting because young people are … not deemed capable of consenting to a lot of things. Yet they are deemed capable of consenting to letting people access all this information that they give about themselves online. (P/P **K**)

See also 2.4.6X.

People of interest to law enforcement/security agencies

> Well, people that the government or the law enforcement agencies have got a particular interest in, it may be fairly or unfairly. This goes back to what we said before, that they really need to have really good evidence as to why they should be looking around in someone's stuff before they're able to do it. … (P/P **L**)

Academics /researchers

> It depends what space you're looking on. So if I look at it from a national security space, you might have — and this could even be an academic for argument's sake, who trawls the Internet and looks at sites that have to do with Muslim radicalism and so forth. It might be easy to jump to the conclusion that this person is emerging as a threat, whereas it was only academic interest. It's a very simple example, but you can easily see how, if they start watching who's looking at what, they monitor these sort of radical sites, that they might, if their systems aren't sophisticated enough, jump to conclusions that are incorrect (P/T **M)**.

People identified in data

> People who are in the data (people identified in data), and third parties that may be identified, and the community overall – privacy isn't just an individual benefit but beneficial to society, fundamental and a practical aspect to a democracy and society.

In a way privacy acts to hold governments accountable. Privacy is a public good used to obtain and achieve a society which has civil liberties. (P/P **N**)

Informants/undercover police

The most at risk in my view would be informants and under-cover officers. If their identities are able to be pulled into big data and searched upon without levels of security being maintained, or details obfuscated somehow. Well, the chance is low but impact is massive. (T/O **O**)

Summary and implications

Research participants identified a broad range of groups who may be subject to the risks associated with Big Data. In particular, the most common answer to the question, who was exposed to risks, was 'everyone'. 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.

2.4.8. Management of Big Data risks

For the policy and the technical groups, we also asked 'How should these risks be managed?' [T12 and P9]. Table 2-13 provides a cross-tabulation of the risks against suggested approaches to the mitigation of these risks. A number of suggested approaches are applicable to several types of risks.

Table 2-13: How Big Data Risks can be Managed (n=38)

	Privacy	Data security	Misuse of data	Misplaced trust in technology	Political risks	Public perceptions	Discrimin-ation
Education	0	0	0	3	0	0	0
Appropriate regulation	3	0	0	1	0	0	0
Balance	2	0	0	0	1	0	0
Controls/ oversight	3	3	4	0	0	2	0
Better communication	2	0	0	0	0	1	1
Provenance/ transparency	0	0	0	1	0	0	0
Risk mitigation via design	0	0	1	1	0	0	0
Honest marketing	0	0	0	1	0	0	0
Smart use of technology	0	0	1	0	0	0	0
Citizens' right of reply	0	0	1	1	0	0	0
Constant adaptation	1	2	1	0	0	0	0

*Note: Multiple responses can be coded for each research participant.

Invasion of privacy

In terms of the risk of invasion of privacy, a range of suggestions were offered by participants, ranging from regulation, oversight, better communication to constant adaptation:

- **Appropriate regulation.** Yeah, I think one of the critical things that we're looking at … is examining the laws and regulations that exist and seeing how they fit with technological developments. It's quite often said that law is always behind technological development and I think that is the case with Big Data analytics as well. … As I say just because we can do it doesn't mean we should. (O-P/O **A**)
- **Balance.** You've got to get the balance right. You wouldn't be achieving crime prevention outcomes if people knew that law enforcement were onto them. The ability to do what has to be done to get good policy outcomes, without alerting them to show that you're monitoring them. (P/P **B**)
- **Controls/oversight.** [W]e recognise the civil libertarian sort of concerns around the use of authorities — the use of this data. We understand … that it should be tightly controlled, and access limited to those that absolutely need it. The AAA approach, which is … authorise, authenticate and audit… (P/P **C**)
- **Better communication.** I think a lot can be learnt if this is the path government is considering… that it's authentic and that there has to be a really good reason why this is necessary and that has to be articulated very carefully, very clearly to the community. They have to believe that that is [necessary], and the way to do that, I think, is to gather [people] around the policy makers who are at the front line. … you've got to get community leaders behind this. … Because I think a challenge would be to bring the community along, and they're going to have to believe that this is necessary, and they're going to have to trust that it's all going to be done with lots of transparency and lots of authenticity. (P/P **D**)
- **Constant adaptation.** Mitigated is surely the word you mean, not managed. 'With great care' is the trite answer. It is extraordinarily difficult, and it will keep evolving. Mitigation measures will evolve, will have to evolve because data sets and power and incentives or motivations will evolve quickly as well. Whatever mitigation you are using today will be inadequate next year. You need to constantly worry about it test it and adapt/evolve your mitigation techniques because the environment is changing so quickly. (P/P **E**)

Data security

Participants suggested appropriate controls or oversight and constant adaptation as ways of protecting data security:

- **Controls/oversight.** To manage the risks – need to be aware of potential for accidents and resolve them, need strong oversight of intelligence agencies. (P/P **F**)
- **Constant adaptation.** Look, managing the security risk is something that requires a very dynamic response because it needs to be informed by that security landscape. I don't think there's one thing that would manage that challenge, it is about going back to the notion of reasonable steps. Making sure that all aspects of the security equation are covered off. That's going to be the extent to which the IT security is impenetrable or moves towards ensuring it's as secure as possible. But then also the other aspects of the security clearance of personnel who have access to the data, the training of those personnel, the

policy frameworks that guide it. So the ability to have audit trails, to be able to have all those mechanisms that are inbuilt that flag irregular access or use to the data. So the whole security equation requires a whole number of aspects to it and also includes infrastructure, resources, and properly trained personnel. Even with all of that, in terms of the *Privacy Act* that could equate to taking reasonable security steps, but nonetheless data could still be hacked or still go missing notwithstanding having taken all of those steps. So it may not be a breach of the *Privacy Act* because obligations have been fulfilled, but still there could be a risk that data is breached. (P/P **G**)

Misuse of data

The risk of data being misused can be mitigated through a variety of methods:

- **Controls/oversight.** Controls are always the important element and they have to be appropriate for the level of risk that's there. (T/T **H**)
- **Risk mitigation via design.** There are ways and means already in technology to monitor the law enforcement people themselves to make sure that they're not performing inappropriate searches, or undertaking inappropriate activities.(P/T **I**)
- **Smart use of technology.** [I]t does get mentioned as one of the big concerns, that while you can de-identify, de-personalise individual data sets, could you use it to then triangulate to re-identify the data? That really comes down to the sophistication of the technical processes you use to de-identify the data. (P/T **J**)
- **Citizens' right of reply.** That there is a right of reply by the citizen when that information is incorrect. (P/P **K**)
- **Constant adaptation.** See earlier quote under Data Security (7.4.8E)

Misplaced trust in technology

To avoid the risk of placing too much trust on technology, participants suggested education (of leaders and senior decision makers) on technical issues as well as appropriate regulation to address the problem:

- **Education.** I think it's a matter, to some degree, [of] education but what does that mean? There's a real challenge here because in many cases the current cadre of leaders in the organisations that we're talking about in this space are not themselves deeply technical so they don't have the ability to really firsthand assess the credibility or otherwise of claims that are made about technology. That is a huge problem so step one would be having them with a very trusted and credible cadre of advisers who can actually give them an informed opinion on that. How you build that set of people is a question that I'm not exactly sure … otherwise there need to be ways of educating the senior decision-makers in these types of questions around technology. They shouldn't be afraid of technology. They have to understand that technology is a necessary part of their business. They can't believe that they can just keep doing things in manual ways, the way they've potentially already been done because that is a massive impediment on their ability to achieve what they need to achieve. But they similarly shouldn't go too far the other way and just believe the hype that a salesperson is going to tell them about what's possible with technology, to do things for them rather than believe that technology is there to support people. (T/T **L**)

- **Appropriate regulation.** I think that depending on the exact field, there is a role for regulation in some places and what form that that would take depends on the field in which we're talking. (T/T **M**)

Public perceptions

Research participants expressed the view that the risk of hostile public perceptions of Big Data could be overcome through controls or oversight, although better communication is needed particularly about the existence and extent of such controls:

- **Publicity around controls/oversight.** Well, it's almost as if the risk … is managed, in the sense that the ombudsman does exist. The oversight agencies do exist. We have a lot of infrastructure around preventing misuse of data and … police are prosecuted for this stuff. There are police officers in gaol today for wrongdoing under the *TIA [Telecommunications (Interception and Access)] Act*. So this isn't some mythical regime that exists on paper but isn't enforced. But … for whatever reason, the public doesn't believe in it. This is the whole Edward Snowden story, … it's not satisfying to the public to be told about there's some ombudsman who reviews every third piece of paper or whatever. This isn't a compelling story. … I think Snowden has shaped public perception here and increased the risk aversion of the public to change. So every time some legislation comes forward, it looks to the public as if it's some kind of giant mass surveillance program that's going to be full of wrongdoing, unconstitutional and all this kind of stuff because that's the conversation around Snowden, … so even if that has no relationship to the actual facts of the legislation, the conversations turns straight to this sort of magical thinking around Snowden, rather than any kind of substance of what's in the legislation and what the policy actually is. (P/P **N**)
- **Better communication.** I think government and organisations such as us are quite poor at is our public personas, so the way we deal with the media to let them know of how we deal with this sort of stuff. I suppose the way we present ourselves to the public for this type of thing is very poor and we need to have a bit of strategies in getting out our needs and requirements and getting out the checks and balances that we have in place. (T/O **O**)

Discrimination

The research participant who raised the potential for discrimination, particularly concerning minorities, also identified **better communication** as well as **human engagement and data collection**, particularly with minority communities, as a solution.

Summary and implications

A wide variety of suggestions were offered 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 diverse types of risk.

2.5. Regulation

In this section, we analyse the responses of research participants to questions relating to how Big Data as a category, or the access, disclosure, use and destruction of data more specifically, is or ought to be regulated. Different questions addressed different aspects of regulation, which are dealt with as follows:

- 2.5.1: Description of laws, regulations, and internal guidelines
- 2.5.2 Description of accountability, transparency and oversight 'mechanisms' other than those embodied as above
- 2.5.3 Views on the appropriateness and effectiveness of 2.5.1 and 2.5.2
- 2.5.4 Identification of specific shortcomings of 2.5.1 and 2.5.2, and proposals for reform
- 2.5.5 The extent to which technical tools are, could or should facilitate 'regulation by design'

2.5.1. Laws, regulations, and internal guidelines

Research participants with operational, policy or combined roles, and some of those working in technical roles within operational organisations, were asked to identify the legal framework for the use of data by law enforcement and security agencies. Those whose role was more operational or technical were asked to identify 'laws, regulations or procedures governing the use of data by law enforcement or security agencies' [O2] whereas those whose role related primarily to policy were asked to identify how the use of Big Data was being regulated and 'the laws, policies, codes of practice, standards etc in place in this jurisdiction' [P10]. Table 2-14 shows the legislation identified by different research participants. As can be seen, sector was more predictive of responses than role, with those in the government sector or an independent office/agency more likely to mention agency-specific legislation, the *Archives Act*, internal documents and memoranda of understanding compared to those in the private, NGO or research sectors.

Table 2-14: Legislation and regulatory material identified by research participants according to (1) organisation sector, and (2) type of role and organisation (n=28)

Category	Private/ Research/ NGO (7)	Independent (4)	Government (17)	Policy role (15)	Operational or technical role (13)	Total (28)
Privacy Act, APPs, state privacy laws	3	2	10	9	6	15
Internal documents[1]	1	3	7	6	5	11
Dataset specific legislation[2]	2	2	6	7	3	10
Agency-specific legislation	0	2	8	4	6	10
Archives Act (and retention rules)	0	0	4	1	3	4
Memoranda of understanding	0	0	3	1	2	3
International instruments	0	1	1	2	0	2
Security classification	0	1	0	1	0	1
State human rights legislation	0	0	1	0	1	1
Nothing specific to Big Data	1	0	1	2	0	2
No specific response/unsure[3]	5	0	4	5	4	9

*Multiple responses can be coded for each research participant, including in the final two rows. Where relevant, categories relate to a former role.

[1] Includes manuals, protocols, guidelines, codes of practice

[2] Includes the *Telecommunications (Interception and Access) Act*, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act* and the *Surveillance Devices Act* as well as legislation relating to, for example, taxation data.

[3] Includes respondents who were not asked this question directly, those who were unsure, those who stated they were not qualified to respond and those who did not comment (sometimes because they took part in a joint interview and the response came from another research participant). In some cases, research participants mentioned specific legislation in the interview, despite not being confident to answer this question; those respondents are coded in this row and elsewhere.

The ***Privacy Act* or *Australian Privacy Principles*** or state equivalents such as *Privacy and Personal Information Protection Act* (NSW) were nominated most often. The Privacy Principles were described by one research participant as ‘principle based and technologically neutral’ (P/P **A**; see Lens 5.1.3). Although privacy legislation was mentioned frequently by those with current or former government roles, it was sometimes mentioned in relation to the exemption of some agencies from its jurisdiction rather than its direct applicability, for example:

> My understanding is that certain parts of the *Privacy Act* do not apply to certain Law Enforcement agencies, particularly national security agencies (P/P **B**)
>
> … the intelligence agencies like ASIO are not subject to the *Privacy Act*. … under the *Privacy Act* an exception which allows disclosure of information is where it’s authorised or required by law. (P/P **C**)

However, as one research participant stated, the fact that the legislation did not apply directly did not necessarily mean it was irrelevant:

> We actually have an exception from the *Privacy Act*, but as a result the minister stipulates basically … we apply the privacy principles [where] at all possible, where it's in alignment with our functions. (O/O **D**)

Internal manuals, codes of practice, protocols or guidelines were mentioned by eleven research participants. These are sometimes developed in collaboration with either the Attorney General or the Privacy Commissioner. The Attorney-General Guidelines for ASIO were mentioned, including their use of a proportionality test (see 8.2.2). The AFP guidelines were specifically mentioned, although we were unable to procure a copy of these. The Victorian Police Standards for Law Enforcement Data Security (SLEDS) were mentioned and are available online. Internal policies such as Codes of Conduct, Statements of Value, Information Security Policies, and Victims' Charters were also mentioned.

Ten research participants mentioned **legislation dealing with specific datasets**. Of these, the most commonly mentioned was the *Telecommunications (Interception and Access) Act 1979*. One research participant P/P (**E**) pointed out the lack of any statutory requirement to delete data when it is no longer relevant and also commented on the low legal threshold for access to telecommunications data in one of the agency acts but added 'I am not saying the threshold is too low, but it isn't a high threshold.' Another research participant discussed its application to Big Data analytics, together with that of the *Surveillance Devices Act 2004*, at length:

> So there probably is scope inside these agencies to do all kinds of Big Data analysis … but the things that they're telling you about probably aren't things that have been done with [*Telecommunications (Interception and Access) Act*] data and surveillance device data because the legislative use provisions are quite constrictive … There is some possibility that some of these agencies have legal interpretations of those use steps that allow them to do bigger access to data. Lawyers can read things in many different ways …. So there is some chance that there's imaginative legal interpretations of how those provisions work. But I suspect that the vast majority of Big Data analysis that is happening is not happening on [those datasets] … these two bits of legislation just drop an iron fist on Big Data analytics. (P/P **F**)

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* was on the political agenda during some of the interviews. Mentioning or failing to mention this legislation was thus likely a question of the timing of interviews relative to the Act's progress through Parliament. The link between this particular data set and Big Data was commented on by one research participant:

> The [*Telecommunications (Interception and Access) Amendment (Data Retention) Act*] as it is now is probably an interesting case study of the Commonwealth government legislating access to a Big Data set. It happens to be a big distributed data set, held in multiple locations by different corporate entities. It gives the government rights to access data, and puts restrictions on terms and conditions of that access … (P/P **G**)

Only three research participants mentioned **legislation dealing with specific data sets other than telecommunications and surveillance devices data**, such as legislation governing Medicare numbers, tax information or immigration data as well as legislation governing data matching. One research participant made some interesting observations about the restrictiveness of tax information:

> [I]n the taxation area … [confidentiality] was regarded probably 100 years ago as a trade-off for what appeared to be the appalling degree of frankness called for in

> your average income tax return. You must be frank, otherwise we'll punish you, but … no one else is going to get this. But it may be that culturally that approach to individual information … really stems from the social trade-off we performed for income tax. (P/P **H**)

Agency-specific legislation was mentioned frequently (10 participants), except among research participants in the private/research/NGO sectors where it was not mentioned at all. The agency-specific acts varied, but included the *ASIO Act*, the *Intelligence Services Act*, as well as Acts governing agencies such as the ATO, AFP and State police.

> … the *Intelligence Services Act* is obviously the highest element of that regulation and that gives the Minister for Defence certain powers to authorise the Australian Signals Directorate [or ASIS] to carry out its roles and functions. … The *ASIO Act* does the same through the Attorney General in relation to its roles and functions. … [T]here's a mechanism within the ISA that prevents the non-ASIO agencies from doing things that are not related to national security. So for example if [ASIS] wanted to do something in relation to an Australian citizen overseas … the Defence Minister cannot alone sign off on that capability. He has to get the joint authorisation of the Attorney General as well. Because the Attorney General is responsible for national security under the *ASIO Act*. So that's at the legislative and the ministerial level. … Really, from a legislative perspective, you look at the ISA for example, what it does is regulates what [agency] can collect, or law enforcement, it regulates what they can collect and how they can collect it. It doesn't necessarily regulate what analytical techniques they can apply to that data once they've collected it. It does regulate how they can report the output of that analysis. (O-P/O **I**)

> [The] go-to source for us it the [Agency Legislation]. That defines what our role is and therefore gives us lawful authority to ask – we can ask for anything, it's whether or not they give it that's the other question. What we've got to obtain under warrant and what we've got to obtain under sharing agreements. (O-P/O **J**)

Because of the different agency-specific Acts, rules could be quite different. One important distinction is that between foreign and domestic intelligence:

> … [W]here an Australian was involved with a foreign signal then the minister needed to sign off on that. We were hammered home, absolutely hammered home, to the fear of god do not collect anything on an Australian and if you do encounter an Australian stop what you're doing. There was a specific person within the [counter-terrorism] team whose sole responsibility was liaison with the minister's office and would be making sure you would be declaring that to that person and then they would go through the process of informing the minister. If any more work needed to be done, so say that was of interest and you needed to do it, then there was a long chain of justification as to why that needed to happen. … Then only when the minister's signature was on the page could only specific people then do the analysis on Australians. (O/O **K**)

The ***Archives Act*** was referred to by four research participants, all in the government sector. In one case, it was in the context of the employer agency's exemption from that Act. One research participant commented in more detail:

> The *Archives Act* says we can keep [telecommunications] information for a fairly long time. I think it's about 15 years so we tend to make sure that we keep it for as long as we can … if we collect biometric data such as fingerprints the legislation is quite specific there as well that we have to get rid of it after a certain period of time. (O/O **L**)

The ***Evidence Act*** and the ***Policing Act*** were also identified as the basis of rules around retention and deletion of data. In this context, it was noted 'Physical data we're bound to retain. There's not so much policy on online data' (O/O **M**).

Memoranda of understanding with government and external agencies at both state and federal level were referred to, only some of which are publicly available.

A few things were identified by low numbers of research participants. Two **international instruments** were mentioned – the International Convention on Civil and Political Rights and the Cybercrime Convention (the latter in relation to data sharing with foreign agencies). One participant referred to **rules governing classification of information within government**.

Two research participants commented that there was **no legislation specific to Big Data**. For example:

> … there actually is no law or regulation around Big Data, per se, or Big Data analytics. The regulation relates to the ability of law enforcement and intelligence agencies to collect, analyse and report on data that they've collected. So it's not Big Data analytics per se that's subject to the law. (O-P/P **N**)
>
> So when you talk about what regulations are covering [Big Data in the commercial sector], zip I suspect. … It's a big thing that you can't control. I think that's the scariest thing about this Big Data, the use of Big Data, … – who is going to control it and when? Because we could never get international cooperation around that. So whatever rules we set here can be breached anywhere else. (P/P **O**)

One research participant, (P/P **P**), commented extensively on the **structure of existing legislation** in general. This research participant classified rules into three categories:

- *limits on access* (for example, through a warrant process) that operate in different ways for different agencies and different data sets. For example:

  > So if you're the [Australian Taxation Office], your access powers are easier because people submit a form to you with a whole bunch of data in it. So access happens to you much easier than access happens to law enforcement and national security agencies.
  >
  > really the [T*elecommunications (Interception and Access) Act*] and the [*Surveillance Devices Act*] are probably the most access controlled bits of legislation on the books.

- *limits on how the data is used*, or 'how do I get from my data to my action'. The research participant noted that '[t]he way I think of Big Data is as a use question', explaining:

  > I think Big Data analysis is one type of that use which would involve getting a lot of your accessed information and then trying to find inside it some sort of information that's going to lead you to an outcome. So I've accessed all this telecommunications data under a whole bunch of lawful powers. Wouldn't it be interesting to put it all together and then run some analysis through it and figure out who was doing what and where so that I can then achieve the outcomes of my organisation in step three?

- *limits on what can be done with the data in terms of action*. For example:

  > So you can put it into a court proceeding in the following circumstances if the following tests are met. Well, it has to be a serious offence. It has to be a prosecution of a terrorism – whatever the legal test is for when you can take an action with that data.

This research participant also talked about data sharing and disclosure, sometimes within the second category (data sharing as an aspect of use) and sometimes within the third category (data disclosure as the action).

However, some of the distinctions raised by this research participant are different to the experience of other research participants. For example, another research participant observed that access issues arise at the individual level as well as the agency level, so that access rules could block the ability to use data for a particular purpose:

> To look up someone, you need a cause and a basis in authority. Even the entity database, you cannot look it up to find out when someone's birthday is – there needs to be a nexus to security even to use the internal database. You need a justification threshold and there is paperwork that increases as the capability increases (for example more is required to use a listening device than looking up a name in a database). (T/O **Q**)

Summary and implications

Research participants were asked to identify laws, regulations and procedures governing the use of data by law enforcement and security agencies to observe the differences between groups in terms of the kinds of laws identified. It does not replace the legal analysis in chapters 1 and 3 of this report.

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. Some participants stated that they relied directly on legislation whereas others stated that they 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.

2.5.2. Accountability, transparency and oversight mechanisms

We asked research participants with a policy role to identify 'accountability, transparency or oversight mechanisms' that are in place in their jurisdiction [P12]. Some research participants were unsure and one stated that there was 'nothing in particular with regards to Big Data'. Other research participants identified other mechanisms which fall into three categories – external (to agency) accountability, internal (to agency) accountability and personal accountability. The last group are not truly 'accountability, transparency and oversight mechanisms' but have been included as they reflect how some research participants saw individual behaviour being controlled. Similar mechanisms were also identified by research participants in the Operational and Technical groups, and they are included here where relevant.

External accountability

A range of monitoring and oversight procedures carried out by external agencies were nominated by research participants as mechanisms for making agencies and individuals accountable.

Parliamentary and ministerial oversight (See Lens 5.1.7). Parliamentary oversight was mentioned by five research participants and ministerial oversight and directions by two.

Independent oversight (See Lens 5.1.6). Many research participants identified the existence of an external or independent oversight officer or agency who looks over the activities of law enforcement or national security agencies from either an operational perspective and/or a policy perspective. This role was said to be played by the Inspector-General of Intelligence and Security (IGIS), the Privacy Commissioner, the Commissioner for Law Enforcement Data Security, the Law Enforcement Integrity Commission, the Commonwealth Ombudsman, the courts and anti-corruption bodies. One research participant observed that there are sometimes 'stacks' of oversight bodies 'like another oversight body that oversights the oversight body'. There were some comments specific to the role played by IGIS.

> [Describes two to three hour interviews with IGIS or an advisor to go over all of the activities undertaken by an agency.] That covered absolutely everything we did and my role in that was to make sure that every single thing we did was covered completely to [IGIS's] satisfaction. (O-P/O **A**)

> IGIS both assesses conduct against the benchmark but also critiques the benchmark. At first instance, issues are raised with the agency concerned. Maybe later it will end up in an Annual Report. (P/P **B**)

> …we have the IGIS who basically has the powers of a standing Royal Commission. She comes in on a regular basis, has full access to all our files and systems, and … can ask any questions in terms of any of our activities. So she is there to provide the public with a level of trust that our activities are following legislation and policies. There's probably a level of oversight that's higher than you'll see in a lot of private sector organisations and other government organisations, but that's reasonable given the intrusiveness of our activities and our capabilities is higher. (O/O **C**)

Requirement for warrants (See Lens 5.1.6). This was identified by two research participants as an important mechanism.

Transparency reports (See Lens 5.1.8). One research participant identified the requirement on some agencies to table reports in parliament that provide aggregated data on access to some datasets such as telecommunications metadata. However, there were limits to this requirement:

> There are reports that are tabled in Parliament, but it seems that there is other data access by Law Enforcement agencies that goes on that we don't have a very clear picture about. (P/P **D**)

Internal accountability

In some cases in response to external oversight, agencies normally adopt internal procedures for ensuring compliance and accountability.

Internal compliance and accountability measures generally, including complaints procedures (see Lens 5.1.6). This category was identified at a general level by three research participant, but specific examples within this category were identified by others below.

Audit trails (See Lens 5.1.6). This was mentioned by seven research participants, including some not asked this question directly, as a very important accountability and oversight mechanism. It also links closely with the existence of independent oversight to review the audit trails.

> It should be a very, very serious disciplinary infringement for an officer to grant the officer of another agency access to something without a record to that effect….it doesn't happen. … By and large, their record keeping is very good. (P/P **E**)
>
> [t]he IT system records every keystroke, which is 100% fully audited and available to [IGIS]. Everyone here is aware that IGIS is watching. (T/O **F**)
>
> The main feature is auditability. We have a really strong audit system in place and the team is effective and motivated to protect its integrity and maintain it. Audit reports are available on inspection. You cannot run away from it. (T/O **G**)
>
> Our ability to access data is highly regulated and it is quite highly audited so the [independent overseer] has the ability to come and look at our data holdings at any time and they've got the full right to access any of our data for their purposes. We've got quite stringent internal procedures that are in place. (T/O **H**)

One research participant (P/P) mentioned the requirement to record warrants in a register and/or file a copy with the Attorney General's Department.

Required responses to accidents and mistakes (See Lens 5.1.5). Two research participants identified procedures that came into effect where an accident or mistake was made as an important accountability mechanism. This mechanism is closely linked to the existence of audit trails (mentioned above), which provide a strong incentive for following appropriate procedures in the event of a mistake.

> One of the biggest issues for ASIO is where [a] telecommunications company sends the wrong information. This is infrequent. Then ASIO officers find the information, quarantine it and attempt to destroy it as well as report to the Inspector General for Intelligence and Security. (P/P **I**)
>
> So if you accidentally looked at something – and accidents did happen – if you accidentally clicked into something that you shouldn't have clicked into …you would declare that and they would track how long that information was accessed for, who it was accessed by. …[T]he onus was on you to self-declare that and make sure that they understood it had happened and the reasons and the surroundings behind it. Nobody wanted to … put themselves into that situation where you were accused of accessing something that you didn't want … (O/O **J**)

Training and Assessment (See Lens 5.1.6). Some research participants pointed to the training and assessment that those involved in data collection, analysis or reporting were required to undertake on relevant legislation. One research participant (O-P/O) also identified the ability of investigators to get advice through an internal intra-web. Another research participant discussed the level and frequency training received:

> Whenever new information sharing legislation was brought in between us and the UK, if there was an update about a new capability or tool that was going to be shared with us, the legislative mechanism which allowed that to be shared we would receive a new training session on to say what we could or couldn't do with the information, what restrictions were being placed on us like from a technological perspective and also from an analytical perspective. So they couldn't put a complete lock and a lot of the time it was reliant on the analysts to not do something. … [W]e regularly got dragged into a room and were updated on changes. Particularly the *Telecommunications (Interception and Access) Act* was the big one. (O/O **K**)

Personal accountability

Research participants also mentioned personal factors that strengthen a sense of individual accountability.

Fear of publicity (See Lens 5.1.8). The awareness that matters may become public due to freedom of information legislation and subpoenas was one such factor:

> The police put information on a government system, that means it becomes transparent, not necessarily available but requests can be made. For example, a member of the public could ask why a telecommunications request was made and get a copy of the request. We can refuse the request. But anything we do in writing can be opened up, we are accountable, we have to justify our actions... There are also subpoenas that require us to produce documents relating to anything. We can object. But the fact that it could result in public embarrassment if any abuse was made public, this increases the demands for justification. (T/O **L**)

Another research participant (P/P) referred to whistle-blowers and the *Public Interest Disclosure Act*, which enables staged disclosure of wrongdoing (boss, independent oversight, departmental secretary, media) as another factor that motivates compliance.

Professionalism. Professionalism and a culture of compliance were mentioned by some research participants as important factors. For example:

> We were acutely aware that we were in a position of trust as analysts, that we had access to information that was very sensitive. We took that – everyone took that responsibility very seriously. I never saw an instance of anyone abusing that privilege, and we saw it as that, as a privilege. (O/O **M**)
>
> I think my impression of the intelligence officers is they're much more professional today [than in the era of J Edgar Hoover]. However, that could change. (P/P **N**)

Summary and implications

Research participants 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 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 not well-known or trusted outside the agencies concerned, which may also explain differences in perceptions of the appropriateness and effectiveness of the regulatory regime (2.5.3 below).

2.5.3. Appropriateness and Effectiveness

Research participants with operational, policy or combined roles, and some of those working in technical roles within operational organisations, were asked about their views on the laws and regulations they had identified, although the questions were worded slightly differently. Research participants with primarily operational or technical roles were asked about whether they were 'appropriate' and 'effective' [O20] whereas research participants with primarily policy roles were asked about effectiveness of laws and regulation and also the appropriateness and effectiveness of 'accountability, transparency and oversight mechanisms' [O10, O12]. The latter group generally did not distinguish in their answers between their evaluation of laws and regulations and their evaluations of accountability, transparency and oversight mechanisms. We thus merged their responses (which were consistent) in Table 2-15. There were four kinds of responses – positive, positive about oversight but concerned about restrictiveness or red tape, positive with a different critique and negative.

Table 2-15: Evaluation of appropriateness and effectiveness of laws, regulation and oversight by research participants (n=28)

	Private/ Research/ NGO (7)	Independent (4)	Government (17)	Policy role (15)	Operational or technical role (13)	Total (28)
Positive comments	0	2	7	4	5	9
Positive about oversight; negative about restrictiveness, red tape or reduced capacity	0	1	7	2	6	8
Generally positive with other critique	0	1	4	3	2	5
Negative comments	3	0	0	3	0	3
No specific response/unsure**	4		1	4	1	5

* Multiple responses can be coded for each research participant in the two intermediate categories under 'Positive comments'.
** Includes respondents who were not asked this question directly, those who were unsure, those who stated they were not qualified to respond and those who did not comment (sometimes because they took part in a joint interview and the response came from another research participant).

Of interest here is that those working or connected with government generally reported more positive assessments about the effectiveness of oversight than those in the private/research/NGO sector. Negative comments from those in or working with government focussed on specific concerns, most commonly concerns around restrictiveness, red tape or reduced capacity resulting from otherwise effective laws and oversight mechanisms. The difference between sectors (albeit based on low numbers) is partly the result of different levels of knowledge as to what the mechanisms were and how they operated in practice.

A number of research participants commented on the effectiveness of procedures and auditing within particular agencies and independent oversight (such as by IGIS) with which they had experience. The view here was highly favourable among those who commented. Positive comments often pointed to the success of regulatory and oversight mechanisms in practice, such as the low number of scandals, the culture of compliance, and effective auditing systems. For example:

> I've never seen a deliberate breach by an individual or the organisation of any legal instrument in relation to its collection or use of data … the regulatory and oversight mechanisms have been particularly good. … [The] culture of compliance … was extremely strong. … If you meet an ASIO officer they … know the *ASIO Act* back to front, a DSD officer knows the [*Intelligence Services Act*] back to front…. loopholes in the [*Intelligence Services Act*] … were immediately flagged to the Minister rather than being used as loopholes (O-P/O **A**)
>
> You get the odd scandal but they're usually fairly confined scandals (P/P **B**).

> ASIO does the right thing. They don't access what they shouldn't, they set a pretty high standard … a technical error was reported in the media but this was fixed. They are very good. (P/P **C**)

> It's quite stringent in terms of what we can and can't do and [we] can't impinge on the privacy of Australian without sufficient justification. (O/O **D**)

Some research participants praised particular aspects of the legal or regulatory regime. For example, one research participant (O/O) commented favourably on the flexibility of the current AFP guidelines compared to the now-defunct Commissioner's Orders (see Lens 5.1.3).

Purely negative comments were all from non-government research participants. Examples:

> Maybe inappropriate and too effective (P/T **E**, discussing privacy protections)

> They're not appropriate. I don't think they're particularly effective from the end user or citizen point of view. (P/P **F**)

Some of the comments from government research participants were mixed: positive about the oversight mechanisms in controlling bad behaviour, but negative about it involving too much red tape or reducing capacity. For example:

> We are heavily scrutinised at every level. Compliance reduces our capacity quite significantly. (T/O **G**)

> My personal view is that the focus on privacy is too strong to meet the current challenges in the environment, especially the security environment. … [T]hey are effective at protecting privacy of individuals … there's a stronger focus on privacy than there is on freedom to share information. (T/O **H**)

> I think they're effective in protecting privacy but they're not necessarily effective in terms of … access to information by agencies that need it. (O-P/O **I**)

> [Laws] are not as effective as they could be … to support national information sharing. … [Oversight and accountability mechanisms] are adequate. They're all logged, audited, independent bodies who can investigate with extensive powers. (O-P/O **J**)

> It certainly doesn't allow a lot of stuff that would make sense … from a policy perspective. By dropping that iron fist on Big Data use, you probably prevent a whole bunch of good stuff from happening. But it's effective in doing what it intends to do. It's just that maybe its intention isn't what that intention ought to be. (P/P **K**)

> … there may be a degree of sclerosis in the system … a little bit too much difficulty in people accessing information. But I don't actually mean that seriously, but it's a way of emphasising that I see no sign of debauched security, just none at all (P/P **L**)

One research participant thought that concerns about red tape should not override the need for oversight:

> So what became, if you will, muddled was the idea that it might take police or intelligence officers a whole day of paperwork to be able to get into someone's very private life. I agree it shouldn't necessarily have to take a day but I don't think that we should intertwine administrative inefficiencies with the importance of oversight for use of those powers. (P/P **M**)

Five research participants were generally positive but negative about some particular aspect, either in addition to or instead of the more common concern about restrictiveness and red tape described above. One research participant (P/P) believed that oversight mechanisms 'could be improved' and mentioned the value of a national and consistent approach to privacy law and the fact that whether new legislation as prepared for new data analytic centres would be 'an indication' of the appropriateness of existing laws. (see Lens 5.1.3) Another (P/P) was concerned about the potential for the *Telecommunications Interception (Interception and Access) Amendment (Data Retention) Act* to degrade in effectiveness over time given changes in communication technologies and globalisation, but nevertheless accepted its value. One research participant (O-P/O) stated 'Lack of uniformity [in different state and federal jurisdictions] inhibits the ability to work in this space and creates complexity.'

One research participant was concerned about complexity as well as the lack of policy logic and consistency, suggesting that 'this could be so much better than it is'. Some examples were given:

> It seems unusual to me that political parties can access the data on the electoral roll fairly freely whereas investigating agencies cannot fairly freely access data on the electoral roll. ... Explain to me what the policy rationale under those two provisions is? ... There's also a question about how you can give [information] to another agency. … [H]ow the ACC can give information to the AFP is tightly regulated. This is just a mystery to me. Why should it be that the ACC is allowed to know something about serious organised crime but isn't allowed to give it to the AFP to know about serious organised crime? I just don't understand that. (P/P **N**)

Another research participant was generally positive, but also mentioned inconsistencies (see Lens 5.1.3), and commented more generally on the difficult balance between simplicity and nuance:

> You legislate and you control and you regulate at a macro level. … But you can always find instances, examples, moments where it's totally wrong, totally inconsistent, and … the rules can't be nuanced enough in my view to allow what I think would be legitimate. If you did try and nuance them to that extent, they'd be unworkable… you'd have an incredibly complex decision tree at the very best, getting you to a point where you would say oh okay, it's legitimate for me now. Overall, I think … I've got lots of complaints but none of them are really the ones that you die in a ditch over. … It's better to have us constrained and checked than have us unconstrained and unchecked. (O/O **O**)

Two research participants commented specifically on the limited effectiveness of the *Privacy Act* / *Australian Privacy Principles*:

> Well you've got things like the *Australian Privacy Principles* which are better than nothing. They're not exactly The Hound of the Baskervilles [with teeth] but … they have some good principles (P/P **P**)

> … there's a lot of problems around the enforcement of the *Privacy Act*, particularly vis-à-vis companies that may be based overseas and providing services in Australia. Even if the laws exist, the actual enforcement may not be particularly effective. (P/P **Q**)

On the other hand, one research participant was positive about the *Privacy Principles*:

> [T]he Privacy Principles strike an appropriate balance. … [T]hey provide … flexibility. They enshrine concepts such as reasonableness that can be interpreted subject to the particular circumstances. It enables government and business who know their operations best, to form views around how they should apply in their own … context. (P/P **R**; see Lens 5.1.3)

Summary and implications

Those 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 difference may follow 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 (see 2.6 below). Those who commented on internal auditing and procedures and the effectiveness of independent oversight mechanisms such as IGIS did so positively. Views on the appropriateness and effectiveness of privacy laws were more mixed.

2.5.4. Perceived shortcomings in law and regulation and proposals for reform

Research participants with policy roles were asked to identify shortcomings in the current legal and regulatory regime as well as future strategies for Big Data [P10, P14]. Research participants with technical roles were asked what advice they would give policymakers on the use of Big Data or data analytics for law enforcement and national security purposes [T11]. Research participants with operational roles occasionally commented or gave suggestions, but generally deferred to Parliament and policymakers on these issues. There were some specific comments about gaps in the current legal framework, issues not addressed by current law and areas where the current legal, regulatory or oversight framework could be improved. Some of these involve relatively minor changes to specific laws, whereas others call for a large-scale change in approach. In this section we describe the various proposals, although we do not evaluate any of them here. It is important to note in that context that research participants' understandings of the existing legal regime may not be accurate and may not correspond to our, or the government's, interpretations. They are grouped into specific reform proposals, proposals dealing with the alignment of law and community practices or standards, proposals framed in terms of the need to 'update' law and proposals that would involve large-scale reform.

Specific reform proposals

Reduction in red tape (See Lens 5.1.1). A number of research participants commented on the need to reduce the time and paperwork to get approvals to access or use data. Some observed that this could or should be done without reducing oversight.

> I know that the police we work with are often very frustrated because they've got to apply internally to get access to funds, access to data. (P/P **A**)
>
> These kids are in danger now, and really, we have to keep that in mind. Or there's a threat, a terrorist threat now. So to wait days or even weeks to get that process underway is dangerous in itself. (P/P **B**)
>
> You could say well, what is it in here that is achieving the effect of oversight and could we run red pen through 90 per cent of the oversight mechanisms, take the 10 per cent that work, put them on steroids and end up with a more effective, cheaper, better oversight regime? (P/P **C**)

> I understand that those administrative burdens can be high. It may make sense to reduce the administrative burdens in a sensible way using a sort of cradle to grave experience study without removing the oversights for them. (P/P **D**)
>
> We are flooded with laws … any additional burdens in place would probably risk crippling the system, reducing capability (T/O **E**)

Duplication of oversight (See Lens 5.1.1). In a related point, one research participant (P/P) suggested that no agency needed more than one ombudsman or independent oversight body whereas 'the police can be subject to two different ombudsmen'.

Circumstances where a warrant is required to pass data between agencies (See Lens 5.1.2). One research participant (P/P) suggested a need for greater thought as to where a warrant is required to access particular data about a named individual from another agency and where there is a legislative standing authorisation in place through which larger volumes of data can be passed between agencies for a proper purpose.

Warrants for data use/analytics (see Lens 5.1.6). One research participant (P/P) made the suggestion that one could introduce administrative warrant system for dredging Big Data, where the requesting officer would have to say 'we're looking at this because of X and we are interested in potential culprits A, B, C.' According to this research participant, the warrant requirement 'can and should be an iterative process so that you produce some information by one set of algorithms and the information thus produced can and should be inputted into another one.'

Deletion of data (see Lens 5.1.2). One research participant (P/P) suggested that data relating to a criminal investigation should expire after a period of time and 'intelligence Big Data' relating to a person should expire once they are assessed as not being a threat. Another research participant (P/P) was similarly concerned about the lack of a deletion program, noting '[t]he public now expect there to be deletion when data is no longer required. A risk based approach to data retention is needed.' If the concern is the potential that data may be needed later, this research participant suggested that agencies could 'keep references to material without keeping the material itself'.

Improved inter-agency collaboration and communication (see Lens 5.1.1). One research participant discussed the potential benefits of greater communication and collaboration among federal and state law enforcement agencies, including the potential for learning from good practices:

> We need better inter-agency communication. We do share data with other agencies [listed]. But how do we share our data with them and how we access their data with security and privacy in mind could be improved. …We don't do [collaboration with agencies] enough. The decisions any agency makes – if they're well thought out and researched decisions it would be nice to see why they came to that conclusion. [We need] collaboration at the big CTO [chief technology officer] level…but you need to have some form of lower level group or some way to [show] low level technical staff how to communicate to their counterparts, best practices of how to meet the requirements for business, and how to implement those type of systems. For example, how to best store video images so that it's not a dumb repository of data. (T/O **F**)

Online data as evidence (see Lens 5.1.3). One research participant (O/O) proposed changes to policing, evidence and assumed identities legislation to provide greater clarity on 'online data'. For example, this research participant did not believe there was sufficient clarity on whether data imported from the Internet needed to be retained for statutory periods by law enforcement agencies or on the rules for the collection of data about investigation targets by law enforcement officers through an assumed identity online, as where police use fake social media pages.

Right to view and correct data held (see Lens 5.1.4). One research participant (P/P) was of the view that 'individuals should be able to see the data which is theirs or their personal data or data about them and certainly are aware of what has been collected, so they can see whether it's accurate or not … it's important that individuals do know what's happening to their data.'

Need to enhance clarity and reduce complexity (see Lens 5.1.3). One research participant (P/P) stated 'If you sit down one day to understand the [*Telecommunications (Interception and Access) Act*] by reading it you will have a bad day trying to do that. So it's ineffective in that sense.' Two other research participants (P/P; O-P/O) also commented on the problem of unnecessary complexity, for example:

> [a]ll our laws are too complex, all of them are too verbose, they're unbelievably over-sophisticated … law needs to be completely accessible to anyone with goodwill and a modicum of intelligence. … [C]ounter-terrorism is the great example – is let's enact a whole lot of law, unbelievably sophisticated law, and we do. I don't know if you feel safer against terrorists because … we've got all those bits in the criminal code. I don't. We already had really good laws against murder. (P/P **G**)

Need to enhance consistency (see Lens 5.1.3). Two research participants (O-P/O; P/P) argued that there was a need for a more consistent legal framework around data sharing. One of them specifically stated that this should work 'across all of Australia, not just in one State or jurisdiction'. A third research participant (T/O) made a similar point, pointing out that New Zealand had the advantage of having 'only one police environment so that they can get on with it and get work done'.

Need for resources. The question of funding or resources was referenced by two research participants (T/O; P/P), in particular as regards the Privacy Commissioner (P/P)

Application of privacy law to Big Data (see Lens 5.1.3). A few research participants raised the need to consider how current privacy law could apply to Big Data approaches to intelligence and investigation. For example:

One research participant (P/P) described the need to rethink the application of Privacy Principles in a Big Data context, including '[h]ow to get properly, fully informed and freely given consent where … dealing with sensitive information, [h]ow to give notice that's contextual and relevant to people's particular interactions or dealings.' This research participant was not proposing diminishing privacy protections, but rather exploring 'greater innovation in applying the current law'.

Another research participant (P/P) also referred to need to revise privacy law stating that 'Big Data requires Big Privacy…. There's a lot of data and there needs to be the appropriate redress…I think there's a need to recognise that when you have vast amounts of information held you can magnify potential outcomes for breaches.' This research participant also referred specifically to difficulty of getting consent, suggesting the need to ensure laws allow for 'anonymity and pseudonymity' where consent is insufficient as well as the special nature of health and genetic information where 'it's not just the individual who is affected'.

One research participant (T/T) expressed the view that insights could be gained with selective disclosure of information that protected privacy rights and preserved operational secrecy while enabling investigations:

> I think for me it's about looking at the way the data could be used with benefit. That means noting that there's an appropriate way of using it and it might not always be about sharing individuals' entire content. It might be just relevant information that

> might not provide details about you as an individual but it might be able to tell another agency for example, trends that are happening in that space. I just think it's not as simple as closing the door because there's some information there that might give away who that person is. There's lots of opportunity as you say, de-identifying records. If you look at CrimTrac I think is a good example. A police force can go there and say, I've got this individual, I need to know if there's anything else out there. They'll search it they'll come back with a yes or a no. If there's no other criminal records, the answer will be no, they know that they're clear. If they get a yes and they get a reference to say you might want to talk to these people about it. They don't tell you what it is because they don't manage the need to know. They give a flag that there's more information out there that you might want to investigate. Here are the people you should talk to about it and that person can decide then. I think that's a good example of protecting the people's rights but not making it so you can't actually find it because you have no access to it at all because you don't know if I need to know yet. (T/T **H**)

Timing of public access to information (see Lens 5.1.8). One research participant (P/P) suggested reducing the time before which one could access ASIO information to 10 years, so that people 'have the opportunity to see what it was that was done [eg if they were 'falsely' investigated] … and where it was incorrect, to contest it.' Another research participant (P/P) commented more generally on the potential for over-classification of information and how this can lead people to 'jump to the wrong conclusions'.

Critique of telecommunications data retention regime (see Lens 5.1.2). One research participant (P/P) expressed the view that the *Telecommunications (Interception and Access) Amendment (Data Retention) Act* failed to take account of the concerns raised in relation to the European Data Retention Directive around accountability, oversight, breadth and data security.[74] One research participant (P/P) proposed a warrant regime and aggregated reports to Parliament for access to telecommunications metadata.[75] Another research participant (P/P) also supported warrants for access to metadata, but believed that they could be 'administrative warrants' signed by 'relatively senior officers' whose purpose was primarily to create a paper trail.[76] It is worth noting that interviews took place before, during and after parliamentary debate on this legislation; participants' comments may not reflect a full understanding of the enacted Act.

Regulation of trans-border data flows. One research participant (P/P) argued that there was a need for regulation around trans-border data flows, particularly in New South Wales.

Alignment of law with community standards or practices

A number of research participants pointed to community standards or practices as a measure against which laws should be evaluated (see Lens 5.1.2). This argument was used to suggest the need for either greater or lesser protection of privacy. This was closely linked to participants' attitudes towards privacy as a value and participants' perceptions of community attitudes to privacy. Most of the suggestions reflected the view that the

---

[74] For more information regarding security requirements in Australian law, see 3.5. Also see section 3.6 on accountability and oversight mechanisms under the *Telecommunications (Interception and Access) Amendment (Data Retention) Act*.

[75] See section 8.1.3 on the existing regime for access (comprising a combination of warrants and authorisations). There are reporting requirements in the legislation: eg *Telecommunications (Interception and Access) Act 1979* Part 3-6.

[76] See section 8.1.3 on the existing regime for access (comprising a combination of warrants and authorisations).

community was relatively unconcerned about privacy or that modern life was inconsistent with privacy. For example:

> Sometimes standards change and community expectations change and therefore the laws need to make sure they're kept up-to-date to ensure that the community's kept safe. … I think the laws need revision. I think if the broader Australian community knew that I couldn't access tax data to undertake a [counterterrorism or child pornography] investigation they'd be flabbergasted.… If information [is] held by another agency, the community would expect that law enforcement would have access to that as long as there's appropriate safeguards. (O/O **I**)

> I think it's so strong out there in the marketplace that I think it's a naïve view if you think you go through life anonymously. I just don't believe it exists anymore. I think therefore the laws need to be … cognisant of the realities of life as they play out and not believe that you can actually put the genie back in the bottle. (T/O **J**)

> …many people think the privacy they have in the hard copy days, the expectations there, should be maintained in the digital days and I just don't think that's possible anymore. (O-P/O **K**)

Need to update laws (see Lens 5.1.7)

Several research participants felt that current law was out-dated given the new capabilities enabled by Big Data, particularly data analytics. This is not a new problem, and one research participant (O-P/O) commented on the history of the various agency-specific acts and how they had needed changing over time. The specific suggestions for bringing the law up to date bifurcated into those who felt privacy laws needed strengthening in the face of the new threat and those who felt newer intelligence or investigation techniques needed to be rendered permissible. Although views on privacy were important in understanding the ways in which research participants felt laws needed updating, the focus in this section is different from that above in that it was technological change, rather than a change in community attitudes and practices, that was central in the need to change law.

Examples of research participants who felt privacy laws needed to be strengthened:

> the more capable the intelligence and law enforcement agencies become, the more robust the governance and oversight mechanisms have to be (O-P/O **L**)

> [Privacy laws] are arguably a bit out-dated. [The laws were enacted] way before many of the innovations that we see now, which … do have privacy implications, were even conceived (P/P **M**)

> Sometimes bits of information are not individually intrusive but when you join the whole together you get a larger picture. Here, there can be a very low level of authorisation because the authorisation required is set at the level of the individual bits of information, even though in reality you can get a lot of information by a series of bits of individual information. Technology changes quickly, so you need to be alert about the volume of information that can be obtained. (P/P **N**)

Examples of research participants who felt new techniques ought to be permissible:

> The orthodox approach is to describe purposes and seek authorisation upfront. Whether this is still necessary is a society wide question. … Implicitly or explicitly we agree that information will be used in certain ways. … What is implicit will evolve. … So old constructs break down as people born digital (the digital generation is the kids in primary school today), as that group matures, the expectations will evolve. … [T]he first evolution is an opt out regime, instead of ticking 'I consent', if you don't

> tick then it can be used. … Parliament will lag behind … technological capabilities to exploit data for good. (P/P **O**)
>
> [T]echnology and time has changed the world drastically and the legislation has half-heartedly kept up with this … I think the whole Edward Snowden thing has again slowed down the pace at which you can pass legislation because as soon as you introduce the [*Telecommunications (Interception and Access) Amendment (Data Protection) Act*] the world grinds to a halt as everyone panics about what you're doing and – there's a lot of jumping at shadows as well. (P/P **P**)
>
> I think that some of the things we deal with today, … when they were written was actually valid but now new opportunities present in a way they couldn't imagine at the time. They should really be often re-visited, not necessarily to be removed, maybe modified to allow the elements of analytics to occur where before it would have been prohibitive because they were just concerned about getting two data sources together. It's just that the technology now allows you to link things in ways that you couldn't do before. (T/T **Q**)
>
> You can't tackle it from a bottom-up, you have to look at it [as] we want to do this, and this is the benefit that will be derived, so you've got a good convincing argument for what you're trying to do. (T/T **R**)

Some comments lay in between the two positions, and are examples of a more balanced approach, urging a neutral or balanced reconsideration of laws in response to technological change:

> It's quite often said that law is always behind technological development and I think that is the case with Big Data analytics as well … because we can do it doesn't mean we should. … I think that's one of the greatest challenges is making sure the law can keep up with the technology and the technology is not constrained, or the users of the technology are not constrained because of that failure to keep up with each other…. Assuming that Big Data had been proven effective in other instances, are there ways that Big Data techniques or analytics … could be used appropriately? So what kind of laws, regulations and accountability mechanisms would need to be put in place? (O-P/O **S**)
>
> … how you create a regulatory framework around this that is far more modern and in tune with the twenty-first century, from what the *Privacy Act* is at the moment, … that fulfils both functions of providing all the benefits of more data sharing, while at the same time respecting reasonable privacy expectations and rights. (P/T **T**)
>
> [T]here needs to be some reform to modernise the legislation that we have and in some ways make it technology-agnostic to allow us to adapt to the future changes in technology that we don't know about without having to change the legislation but still ensure the privacy of individuals. (T/O **U**)
>
> The pace of change means that things need to be constantly under review. (P/P **V**)
>
> The laws and legislation are always, and will always be slow to react to the speed of technology change. … So the advice is that whilst laws and legislation have to be enacted, we have to formulate a policy that deals with the technology and the speed of the technology at which we create data. Which new functions and features come out and new ways to exploit data [so] that laws and legislation will eventually catch up? It's an extremely hard problem to solve in that space. Data privacy laws, it's just forever and never ending but we can't rely on those laws to give us protection against what we intend to do or what we are trying to do with analytics sometimes. (T/T **W**)

Broader reform proposals

Some interviewees' suggestions for law reform were on a much larger scale, involving an overhaul of existing regulation of the collection, access, use, and disclosure of data and actions based on data or data analytics.

Big Data Bill of Rights (see Lens 5.1.2, 5.2.5). One research participant (P/P) proposed extensive reform by someone 'fearless about protecting the individual' and 'a little bit fierce and definitely independent', in which the establishment of a 'Big Data bill of rights would be paramount'. This would provide protections for 'the individual citizen in their life' and include features such as checks and balances, transparency, and independent oversight.

National laws (see Lens 5.1.3). Two research participants (T/O; O-P/O) emphasised the importance of establishing a national system. For example:

> [Y]ou need national leadership to say this is the way you are going to do it and the commitment of the states to make the necessary environment with the support of the Commonwealth too (T/O **X**)

Rewriting laws with common framework (see Lens 5.1.3). One research participant (P/P) painted a three tier picture of current legislation (set out above 7.5.1P). This research participant used this to discuss how we might move from the current regime of the regulation of data access, use, and action around a particular purpose to a new regime that enables appropriate use of Big Data investigatory techniques, without promoting public panic. This would require an evidence base, including an understanding of how crime and terrorist attacks would be reduced and how much more quickly offenders would be caught, in order to be put to government. It would involve streamlining oversight of law enforcement, so that there is a single ombudsman and a single oversight mechanism that applies across all law enforcement activities but scaled based on the level of risk and privacy intrusiveness. The research participant drew an analogy to the reform of criminal law in the creation of the Model Criminal Code – changing ad hoc provisions dependant on political timing into a consistent framework that recognised difference in terms of mental element, evidentiary standards, seriousness of offence and so forth through standardised categories. The idea of standardising the regulation of data access and use was also mentioned by another research participant:

> [T]he point about standardising is that it helps you to make sure that the thing's comprehensive, is something that's a good idea [and] that should be deployed in all circumstances justifying its deployment, not patchily. (P/P **Y**)

However, the search for a technology-neutral principles-based framework may not be possible or desirable:

> We talk about being able to write technology neutral legislation but that's really difficult because there is still in the heart of anything a concept of technology, as much as you try and make the language neutral. Particularly around data and I think particularly around the scale and volume of data that we have at the moment. If it's going to continue growing the way it's growing that's not going to be something that you can do easily. (O-P/O **Z**)

Adjust balance between regulation of access/collection of data and regulation of the use of data (see Lens 5.1.2). There were a number of research participants who commented on the current balance in the law between the regulation of access to and collection of data on the one hand and regulation of the use of data (including data analytics) on the other. The specific suggestions were diverse:

One research participant commented on the fact that, in the context of data retention legislation, there was a lot of attention on which agencies could access the data but not what might happen after an agency is given access. In particular:

> [W]hat other constraints might exist around the use of that data, the retention of that data within that agency and other ways that you might control how that data is used and by whom, given the tacit acknowledgment or even explicit acknowledgment that it's somewhat sensitive data? That I think is a gap. I think there's a more informed and nuanced conversation … that needs to go into those sorts of issues. (T/T **AA**)

One research participant (O-P/O) felt that you could not apply legal provisions to analytical techniques, and that laws should continue to focus on collection of data and reporting.

Another research participant (P/P) suggested that in some cases it may be optimal to expand the permitted use of data by agencies, even if that means sacrificing some of their powers to access data, and observed that the trend is otherwise to expand access powers at the expense of use powers.

A third research participant (P/P) stated 'It's quite important that any constructs that are around controlling oversight applies not just to the officers, i.e. you shouldn't leak secret intelligence data, but to the data itself and to its interpretation [and] use.'

Change function of IT in agencies to making data available (see Lens 5.1.1). One research participant (P/T) suggested that IT within government agencies could change its function so that it aimed 'to make the data available, accessible, digestible, make sure it's clean, it's good quality' and then provide the various departments with tools to explore that data. Data sharing between agencies could be the next step, once the capacity was created within each agency.

Summary and implications

Research participants 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, also evident in the discussion of values in 2.6. 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.

2.5.5. Regulation by design

One research participant in the Policy group spoke favourably of 'that idea of building governance in to how you deal with data and making sure it's built into the systems and processes of organisations.' (P/P). In line with this idea, research participants with technical roles were asked about the extent to which some of the risks of data analytics could be mitigated through the design of analytical tools [T15]. They were then asked about the extent to which particular issues, such as privacy and data integrity, were taken into account in the design of their system. Table 2-16 summarises the responses.

Table 2-16: Mitigation of issues/risks associated with data analytics/storage systems through design

Issue	Taken into account in design			Not taken into account in design		
	T/O	T/T	Total	T/O	T/T	Total
Privacy and personal information security (see Lens 5.1.2, 5.2.5)	7	4	11	0	0	0
Communications confidentiality (see Lens 5.1.2)	6	3	9	1	1	2
Data integrity (see Lens 5.1.4)	6	4	10	1	0	1
Regulatory compliance (see Lens 5.1.2)	7	4	11	0	0	0
Testing and evaluation (see Lens 5.1.5)	7	4	11	0	1	1
Comprehensibility to decision-makers (see Lens 5.1.6)	5	2	7	2	2	4
Avoiding discrimination (see Lens 5.1.6)	0	1	1	7	4	11
Re-identification risk (see Lens 5.1.5)	2	1	3	5	3	8
Cost	7	4	11	0	0	0

*Two prompts (privacy and personal information security) were asked separately but treated as the same thing by most research participants, so answers are collected under a single heading. One prompt (avoiding unintended consequences) was treated as an aspect of another prompt (testing and evaluation, data integrity, comprehensibility to decision-makers), so is linked with the material under the alternative heading. Some research participants had no specific comment on some issues particularly in group interviews; these are omitted.

All research participants agreed that at least some risks/issues were mitigated through design, as part of a broader system of regulation, procedures, oversight and training. For example, one research participant gave a broad answer:

> It is all taken into account one way or the other. Through the system or training. Different levels for different systems depending on different considerations. (T/O **A**)

Because research participants were working with different systems with different functions, however, not all of the issues were considered relevant by all research participants in designing or implementing a system. Further, the cost of 'regulation by design' was acknowledged as a limiting factor by one research participant, but one that did not prevent its application to critical security issues:

> [I]t's possible but it's complicated therefore it adds to the cost but no matter what advances are made in this space that you're working in there will always be a need to restrict access to data to people who really need that access, to people with a legitimate reason. (T/O **B**)

Where a specific issue was identified by a research participant as relevant in technical design, the research participant was asked how that particular issue was taken into account. Selected responses are extracted below (note that some research participants use more than one design technique for some issues):

Privacy was taken into account through:

1. Controls on access were mentioned by 8 research participants, with one research participant, the last quote (K) below, more sceptical:

> … using some sort of role-based access control. (T/T **C**)

> [Y]ou restrict access to data. All sensitive data is always restricted access. … There's also security of data in rest (encrypted – who has access to the keys – keys internally or externally generated). (T/O **D**)

> I suppose [privacy is] an extremely high consideration for us. Obviously, all the material we receive is private information and so it's very stringent for us that we manage and continue to manage the security and any risks associated with access or security or maintenance of that material. (T/O **E**)

> [T]he implementation of our security system says that I'm entitled to see certain levels of information according to my security clearance or according to the type of job that I do. I could be sitting alongside you and we're doing the same job but I can get access to [restricted information] and you can't. (T/O **F**)

> We deal with this what is communicated to whom with provenance. [Partner agencies] specify their own requirements, take and use information under their own rules. … When information is disseminated back to [another] agency, they must comply with that agency's requirements.... [There are also] security controls on access and use. (T/O **G**)

> How is it taken into account? Mostly through the fine-grained access control models. There's an ability to actually present different redactions of the same data as well. For example, you might have multiple different ways – levels of granularity for example or levels of abstraction of representing a piece of data and you might expose one in one case and a second in another. So I might expose you as a male in one case or as a completely identified male in another case depending on what's needed to complete the task. (T/T **H**)

> In our systems we have personal data. It would not be appropriate to allow anyone to read through the data. It's incumbent upon us to limit access to that data or to have audit trails of who, when and why. You cannot make the assumption that all officers have a need to know or even the ability just to change data around integrity of data. (T/O **I**)

> [We] provide the ability to have fine grained audit. We could log every single access inside the database. Everyone who logs in and every activity that they do we can log and we can retain for auditing. (T/T **J**)

> [T]he user of the tool … can say, alright this particular person can't see individual names, for example. But they still remain in the system and it's not entirely clear to me how that problem can be solved. There are clearly ways that can solve some parts of it, but that just moves the problem to somewhere else. … So the privacy is a problem for a person whose privacy is being violated and it's not at all clear to me if there's anything that they can do to fix that problem. (T/T **K**)

2. Other cybersecurity features (4 research participants)

> We've got a world-class team that does [hacking prevention]. (T/O **L**)

> We have the information security policy and security is a system requirement. (T/O **M**)

> Security of the data again comes down to both security of it in transit and security of it at rest. So that's to do with again policies, procedures, et cetera around who has access as well as technology answers like encryption and other things to keep the data secure. Also to do with the physical environments of deployment so in many cases deploying in restricted buildings, on restricted air gap networks and things like that. (T/T **N**)

> We use encryption, access, single sign on, encryption of data at rest and data in transition, only keep certain data in cloud systems, and other internal mechanisms. (T/O **O**)

3. De-identification of data (2 research participants)

> We also use some de-identification for crime stoppers data for instance … That information is in its raw form. The person may self-identify, that information doesn't go into the backend computer system. It is vetted to remove personal information – any information that identifies. With the 000 line you can only deal with data given and even if they accidently identify themselves as a neighbour, the user's privacy is still protected. (T/O **P**)

> In a lot of cases the actual personal identification isn't needed, what is needed is some kind of label to say, if one person is the same as another person. So instead of communicating names, you could communicate some random ID number that is always the same for the same person, but a second person has got a different ID so you can never see their names but you can see if data coming from two different people is from different people. (T/T **Q**)

The benefits of de-identification was also mentioned by another research participant in a different context:

> [T]he avenue of depersonalised data for analytical purposes is getting widespread use. The reality is that often to get the meaningful insights that you're looking for, you don't need to have personalised data. The insights you gain or the filter that the insight might provide you can then be applied to personalised data within the constraints of the legal permission. … [P]eople are starting to apply their minds to are there ways we can get some of the goodness out of the data without violating privacy principle (P/T **R**)

4. Deletion of old data (2 research participants)

> We are really protective with a great deal of oversight and protection for personal information. For example, when young offenders commit crimes I believe we have to expunge all data after two years. (T/O **S**)
>
> [We do] deletion when purpose expires. (T/O **T**)

5. Relying on public data (1 research participant).

> I think our tools rely on sucking data out of areas that are public. (T/O **U**)

6. Options provided to customer (1 research participant)

> [I]t's configurable but it's not turned on as a default. So the assumption is any data you put on here you want to share entirely. You want everyone to analyse it and then you go from that position towards a more secure one. … We provide a framework that allows our customer to set their own security rights and roles and privileges. (T/T **V**)

Communications confidentiality was interpreted differently by different research participants, with most linking it to protecting data moving between systems, while one participant (T/O) also linked it to the need for those with access to keep information confidential.

Five research participants included communications confidentiality as a feature of their system, giving varying levels of detail as to how this was achieved.

> There are protocols for communications between us and external agencies. (T/O **W**).
>
> We must comply with all of that. Systems are designed with these requirements in mind. Communications that are monitored are Chinese walled and there are processes around them. Ultimately data needs to be joined for analysis. (T/O **X**)
>
> Yes, highly relevant. How is that manifested? Largely through encryption and verification of end points so making sure that the channels of communication are secure both in terms of authenticating who it is that's communicating, knowing who you're actually communicating with from a system level and then encrypting that communication to ensure it can't be listened to over the wire. (T/T **Y**)
>
> Yes, it's hard to say. I'll say yes, once again it's a feature that we provide which is always taken up by most customers. So SSL connections, HGTPS between client and server, absolutely, if that's the sort of angle I'm thinking of. (T/T **Z**)
>
> There's … security of data in … transit (SSL between user and webserver, or additional tunnel, firewall rules, firewall rules to only allow certain PCs). It is very onerous. Some of the information is extremely secure. [There is a] physical cage area of data systems even although they're encrypted. I think that we're looking at [a private cloud] to avoid risk but we're not there yet. … [W]e also use external cloud providers with the same security measures and privacy measures …. Only some data could go to a private cloud. We have certain data for certain systems. We use data storage as a service with a privatised cloud as a service and we have virtualisation so we also have servers as a service. (T/O **AA**)

Two research participants felt that while communications confidentiality may be important, it was not core to their system. For example:

> I think we can do a pretty job there, there's specific technical techniques that can guarantee security and confidentiality of communications... We're not really building communication tools – having said that, I mean public key encryption systems are the standard way to go there and they work well when implemented correctly. … [O]ur systems wouldn't be aiming to communicate those images [in a

> repository of video footage] with anyone, they're going to do analysis and to keep analysis within a secure system. Secured both, probably physically in that case as well as normal network security. … The privacy and personal information problems occur when you're communicating that system or that information from one system to another. In both those cases the important thing to do is to only communicate the bare minimum that needs to be done for whatever the purpose is. So you don't go and grab all the details that can possibly be grabbed when you only need a specific thing. (T/T **AB**)
>
> All new systems have the confidentiality spiel as soon as you try to access the system, 'please note that your access to your system will be audited and all data is to remain confidential'. Confidentiality is not directly built into the system but some systems are audited constantly. Subversion of confidentiality is so easy – take photo of screen. We mostly do this by warning messages and auditing. (T/O **AC**)

One research participant suggested that communications confidentiality was an area of concern:

> [W]e have secure means for obtaining the data and ensuring that we maintain it off-site until we have that material over a secure mechanism on-site and then our same mechanisms for maintaining security and privacy of that. For the surveillance device material or certain material that we get, a lot of systems that we look at and have obtained that gather private information legally have quite weak security in how they store and deliver that material and as an organisation we're quite stringent on that. So there's a number of corporations where we've been quite unhappy with their procedures and we've actually had to pay a lot of money to change the way that they store and deliver material to increase the security of that sensitive information which is quite – these are companies that should know - that deal with private information on a day-to-day basis and should've had better security mechanisms in place. Some of the experiences that we find; some of industry security and privacy over their data holdings – security for their data holdings has been quite weak. (T/O **AD**)

Data integrity. Those who stated that data integrity was taken into account provided varying levels of detail on how this was done or might be done in future. Specific techniques referred to include checking transmission and upload integrity (including parity checks, checksums, hash algorithms) (4), flags or tools for inconsistencies and duplicate entities (3), automation (2), provenance tracking (2), audit (1), and database normalisation (1). Two research participants used the word 'trustworthy' in relation to the importance of data integrity.

> I'm no expert in this area, I must say, but parity checks, and checksums and all that sort of stuff. (T/T **AE**)
>
> [Data integrity is] really important to us, really important. I couldn't tell you the fine details of how it happens. … We do talk about things like Admiralty Scales where … the credibility of a piece of information [goes] from … this is absolutely factual…to 'the guy in the pub told me'. (T/O **AF**)
>
> We are trying to limit manual processing which causes time lags and errors. (T/O **AG**)
>
> We track provenance [of data], audit through its life and use this to assess integrity. We no longer do data cleaning because of the variety problem, provenance is more important. We use raw data. Flags in the system for bad data is at a macro level, can identify multiple entities that should be merged. Much is left to the analyst to make a decision. … [Avoiding unintended consequences] is really about decision-making. It

requires transparency around what is the information, how reliable is it, should it be used. We need to give decision makers what they need to make a decision. It is related to the risks … of automated decision-making. The potential is very high for unintended consequences – these are the sorts of things that keep me awake at night. (T/O **AH**)

We have some and we're working on some. We don't do any data cleaning. We do some normalisation of data. But being an evidentiary environment, we have to ensure that it's documented and repeatable whatever we do. … Currently we've got some very primitive ways of flagging unreliable delivery of data and for possible corrupted data but we're currently building systems to try and do that at a much higher level because the integrity of some of the data we receive is a bit questionable from time to time but we don't have automated systems currently to the level that we would like so we're in the process of trying to develop those. (T/O **AI**)

Once data is in a system there are technical techniques you use to make sure that it hasn't been changed within the system. Things like checksums. When you're moving data into and out of a system there are some degree of checking that you can do to see how accurate it looks. For example if you've got data that indicates a person married another person at a particular date, you can check to see whether both of those people were alive at that date. If they're not it seems like there's some kind of problem there with the data you're seeing. … We do substantial amounts of both accuracy checking and sort of rules around that type of accuracy when we're looking at that type of data, as well as check-summing for data when it's coming in and leaving our systems. (T/T **AJ**)

We have capabilities within our product suites that will allow a customer to ensure the integrity of the data … data quality tools which will weed out duplicates, resolve addresses which are very similar, matching names, spell errors, checks and all that. So that's a data quality component which we can integrate into as well. (T/T **AK**)

The other thing that I think complicates it or that is part of this from a product perspective is a very robust mechanism for making sure that there is a clearly visible and understandable sense of where any particular piece of data comes from. Because that has a huge influence on how much trust, how much authority a human should place in that data coming down to issues of accuracy, of timeliness, of recency and other things that can very deeply influence how much or how someone interprets that particular piece of information. … Our products basically approach [issues of inconsistency] by allowing there to exist inconsistent information surfacing the sources of that data allowing analysts the opportunity to correct and reference corrections as to why one believes – why a user may believe one piece of data to be more accurate or more timely or more something else than another…. In general ... we strive to just leave the data as it is, to present the data as it has been collected and to allow the humans, who are the only real people who can make judgments on correctness or otherwise, to resolve any ambiguity. … I guess the answer here is being as transparent as possible about everything that you know about the data within the bounds and constraints of whatever security models require you to constrain that. (T/T **AL**)

We use one way hash algorithms SHA256 to ensure that what was uploaded into the system … is forensically identical to what was uploaded in the system. At minimum it would be MD5 but more modern systems use SHA256. MD5 is a one way hash algorithm with 32 character in length whereas SHA256 is 64 character hash output.

> It’s like digital fingerprints. For example, if a video has been altered or shortened we should be able to test if for example the video was chopped. (T/O **AM**)

As two research participants observed, data integrity may be low for reasons beyond the control of the system designers:

> Part of the challenge of data quality is data migrations can override all the things you’ve actually built into your system. So it comes down to how well that was done and also how well it was maintained and that’s not necessarily done by any of us. So there are a few factors of data quality beyond just a system build. (T/T **AN**)
>
> We have treasure trove of hidden databases that we cannot access, and don’t get updated unless manually. (T/O **AO**)

Regulatory compliance. All research participants with technical roles agreed that design needed to accord with any applicable regulations, sometimes with the assistance of legal departments or independent oversight agencies.

> [I]t probably comes down to appropriate designs, and design reviews and testing frameworks to ensure that you’re adhering to these regulatory guidelines. (T/T **AP**)
>
> Generally you have to if there are regulations that you need to design around. (T/T **AQ**)
>
> Yes [regulatory compliance is] built in from the start and maintained when there are changes to legislation and regulations … (T/O **AR**)
>
> Every system that we make or purchase has to suit or be customised to meet our regulatory compliance requirements that we currently have. (T/O **AS**)
>
> We involve the legal department to help us in the design. (T/O **AT**)
>
> The system takes into account lots of different information from different places. Security controls are related to provenance. … Output information is … restricted based on provenance of the underlying inputs – [there are] only certain places it can go. (T/O **AU**)
>
> [Regulatory compliance is] highly relevant, something that we definitely butt up against. I think a big part of this is how do we support that? A lot of it is through being able to walk through and explain how compliance is realised in any particular case. So rather than talking very fuzzily, take for example the compliance requirements around data that’s collected under a particular type of warrant that has constraints over how long that data might be held, has constraints in terms of what one has to do if there is an overrun of collection of data or over-collection of data outside the bounds of the warrant unintentionally or issues like that. Historically we have done that with our customers by directly being involved in the engagement with people like ombudsmen or oversight mechanisms in organisations and to walk them through very, very concretely what does it look like when this data is included in our system? What kind of safeguards are in place to make sure that it is very clear? The type of data that this is. What type of safeguards are put in place to restrict access to this type of data if necessary depending on its nature? What types of mechanisms? How do we actually deal with situations like needing to redact or remove data in the event of over-collection or redact or remove data in the event that it is no longer required or permitted to be held by that agency? So how do we do that? There’s obviously a lot of features within the product that are specifically targeted at that in terms of being able to drill down to data, to be able to delete data, to be able to soft delete and hard delete data. So to soft delete it, make it inaccessible to any user other than an administrator or hard delete it to remove all

> trace that the data ever existed – and there can be some nuances there about do you need to capture, audit that that event has happened or does it actually require you to also go back and redact audit logs that that data ever existed because the agency should never have had it? It can depend on the circumstances. You can get down beyond that as well. There's complexity in how that works but we are very focused on being able to support all of those different modes of operation recognising that these things are all parts of the world that these organisations live in. So the products in terms of how we deal with that. Product features coupled with direct and transparent communication with the oversight agencies that are responsible for that. … We fundamentally have to rely on the interpretation of those rules by our customers. In many cases there are specific acts for those organisations. They generally have internal legal teams and we would defer to them in terms of interpretation. Now we do have our own legal staff as well within our organisation and there are cases where there have been inconsistent interpretations of the same legislation across different customers. In that case we actually engage in a legal conversation to try and understand and unpick why there is an inconsistent interpretation, why one thing that is true in that organisation is not true in an organisation that's constrained by the same legislation. Things are not always rational. Things do not always fall out in the same way but we do attempt to apply an engineering mindset and a rationality to it and try and understand why that is the case. But ultimately we defer to the customers' interpretation of their remit. (T/T **AV**)

A slightly different take was given by one research participant:

> Regulatory would be more the application than the configuration and that comes back to security in a lot of ways. (T/T **AW**)

Testing and evaluation (see Lens 5.1.5). Most research participants did at least some testing and evaluation of systems, with some taking this process very seriously.

> We do user acceptability testing, load testing, etc (T/O **AX**)

> [We are] always testing the system and looking for better ways to do things. (T/O **AY**)

> I look at [testing] from a project management perspective as a stage that you do to actually ensure your configuration is built correctly. (T/T **AZ**)

> We have our traditional testing platforms … so customers will test the function to its nth degree and then deploy that into production as well. (T/T **BA**)

> For our main corporate systems, we make sure that we have a test and quality assurance system in place for us. … I suppose the security of [data management system] is tested from time to time for accreditation. Our system for bringing our data in has an accreditation process that it's gone through to allow it to be at a certain security level. From time to time that is re-evaluated. … Currently we've got very limited quality assurance on the product but again we're looking to develop systems to do that better. … [W]e have quite a stringent reporting regime for any integrity issues or loss of data issues and so whenever that happens we put in place different strategies and procedures to ensure that future occurrences are limited. Our management are quite stringent on any of those issues being reported up and that we continue to follow up on implementation and solutions or procedures to limit any reoccurrences. (T/O **BB**)

> We do [testing and evaluation], we're quite pedantic about that. (T/O **BC**)

> [We] test both to build reliable systems but also in the sense of we build … academic based evaluations of how well our systems perform against various benchmarks. … We can build systems that benchmark that, so if you have a large data collection and you're looking for a particular person within it, if you know in advance how many instances they are in, then you can look at how often your system finds it and benchmark how it well it does compared to a perfect system. … [I]f you have a large number of people from different backgrounds who look at the same problem, it does tend to minimise unexpected things. (T/T **BD**)

> Security is always a bit of a hard-core deal here. [My organisation's] security are very strict on what they allow. They need to verify that what you're implementing be what they determine to be best practice for security. You can't just release something. For example, a technology or system would need to be pen tested by external company and even depending on the data that's being held there might be additional requirements on how much encryption exists between the user and the webserver. … [W]e test and evaluate all new systems. It is done reasonably well but it depends on who drives the system in the first place. … [P]roper testers will use boundary testing to try and break system rather than use it for its intended purposes. (T/O **BE**)

> We approach [testing and evaluation] in a number of ways. Obviously there's testing at a software level where we're testing the capabilities and functionality of the product. … There's then very much testing and evaluation in situ with any particular organisation and their data. So for any installation of [our] products there is almost always what we would call a staging or a quality assurance replica of that system, complete end-to-end replica of the production system that exists. That is there to allow us to quality check, to evaluate, to test any changes to data feeds, to ingestion, to modelling of data, to access controls on data. Anything that we might actually roll out to a production system is tested with real users in a real environment against real data with end-to-end replica environment of what's going to happen in a real production system. … [T]here's a pragmatic response here which is that it's very, very hard to be perfect about that but we do the best we can by working with that real environment and making it as real as possible to get real people working through real workflows. … Usually there is some form of expert set of users who are the ones who dedicate some time to testing any new functionality, new data, who understand how that data looks or how it should be used or what they do with it and generally have good domain expertise to be able to inform and detect things that are not quite right. (T/T **BF**)

Comprehensibility to decision-makers. Some research participants pointed out that it was not possible to make all data analytic tools comprehensible to decision-makers (T/T), that it was hard to predict how outputs would be interpreted (T/O), or that this aspect of a system was client-driven and thus external (T/T). Other research participants, however, gave some insight into how they improved comprehensibility for different types of users:

> They can approach us to help them interpret the data. (T/O **BG**)

> Systems have to be better, [we] have to be responsible to start building systems that don't just spit out an answer but also why. (T/O **BH**)

> For any new systems we bring the end users on board … we've developed a working group of end users to have a trial of the systems that we're getting and people from various parts of the organisation have experience in those data sets. (T/O **BI**)

> I think that there's different levels of data that needs to be presented to different people. So an analyst who is interested in very detailed analysis will want to see very

> deep level of details about the individual items of data that you're seeing. Whereas a decision maker is more likely to just want to see the overall big picture view of what the data is telling rather than the details of why the system thinks that. So it's important to have both levels, though it does depend on the system a bit. If you're building something that's designed to be used at those high levels then you should be using visualisation tools that are appropriate for that. (T/T **BJ**)

> [U]ltimately we're there to try and help influence decisions and to drive better decision-making. If you can't do that you may as well go home. How does that manifest? It's about explicitly thinking about the fact that there are different ways that data needs to be surfaced and different levels of synthesis and granularity that the data needs to be surfaced at. So different products. For example, a dashboard might be a much more effective way to communicate the same underlying data or trends in the same underlying data to a decision-maker who is not an analyst as opposed to giving them the ability to interrogate that data and visually build graphs and maps and other things. Still make it interactive so if they're curious or they want to know they can drill back down into the data. So it's important that it's actually backed by that underlying data but levels of abstraction in the way that you summarise and present data is probably the primary way that we would tackle that. … [Avoiding unintended consequences] mostly comes back to transparency so this is about making sure that analysts understand what it is that they are looking at and what it is that they are building the case or building their understanding and interpretation of the world based on. We cannot hope and we shouldn't aim to second guess what that is in specifics. What we should do is just make sure that it is as clear as possible to the analyst what it is that they are basing their interpretation on and that comes down to data sources, reliability, et cetera, et cetera, … making that visible through the interfaces that you expose the data. (T/T **BK**)

Avoiding discrimination. We asked research participants whether there was anything built into their system to avoid discrimination (for example as to race, national origin). Despite the literature on this issue identified in Chapter 2, most research participants did not feel this was a problem, at least not from a system design perspective. In particular, six research participants felt that this was not a system issue, but a question for analysts and decision-makers:

> That's pretty easy to avoid when you're talking data. Data is 1s and 0s. By its very nature it goes past discriminatory lines. As a technical person, I don't implement something that's discriminatory. The interpretation of that data may be discriminatory. (T/O **BL**)

> It is about avoiding analytical bias, we don't talk about discrimination, it isn't an issue for us. We rely on the analyst rather than building it into a tool – it is part of the training process. (T/O **BM**)

> There is a Catch 22 – analytics is good because it is unbiased, just numbers and facts so can help avoid analyst bias. But how one selects features for use in systems can introduce bias. It is a risk. It is important. Really, it is about education. (T/O **BN**)

> From our side, we just purely would deal with the actual data itself and not make any other sorts of association. (T/O **BO**)

> No we don't discriminate so we don't need to avoid it. … The data is separate to the system a lot of the times. As an organisation we don't really touch the data, we supply the environments that hold the data and does the analytics on the data. … It's very challenging in that space [profiling based on national origin based on observed facts] because it's not about discriminating against individuals or nations.

However if you come from the Golden Triangle region then you've got more chance that you're carrying drugs because that's where a lot of it comes from. … Those groups, they will run them on [our system] but it's not [our system] that's doing the discrimination in the system itself. (T/T **BP**)

I guess we are fairly agnostic … because that comes down to specific values of data that you might contain in the system. So is it possible for someone to discriminate on the basis of targeting all their intention on a particular race of people in the system? Yes. How would we tackle that? Right now that would be through the auditing capability. So how do you actually hold people accountable for the way that they're prosecuting their job? How do you hold people accountable for the data that they are or indeed are not looking at as part of that role that they should be? (T/T **BQ**)

Three research participants felt that in some contexts, discrimination (in its broad sense) was a feature of data analytics rather than something to be avoided:

[B]y their very definition, classification algorithms are designed to discriminate. (T/T **BR**)

I think it could be defensible discrimination for lack of a better word. (T/T **BS**, in relation to profiling based on observed facts)

[W]e see problems in … all these criminal gangs, these criminal groupings, we see them within ethnic groups. … It's probably more than a correlation, it's probably - yeah it's probably a direct connection, we're not making an assumption here, you know, you're Japanese therefore you are Yakuza … (T/O **BT**)

One research participant was concerned about the potential for discrimination, but observed that discrimination was in principle detectable, and thus preferable to decision-making by (potentially) biased humans:

I think that's a risk and it's something that you have to be careful of. But at the same time, it's fairly easy to detect that, because the systems are computational and you can actually look at what the parameters are and you can go, oh it is looking at the gender of a person to project what their outcome is going to be. … As opposed to a human based system where you can't tell what the biases are. (T/T **BU**)

Re-identification of de-identified data. Much has been written on the potential for data analytics to be used to re-identify what had previously been described as de-identified data.[77] We asked research participants whether their system was built to avoid or mitigate this risk. Three research participants stated that their systems were not designed for de-identified data or to de-identify data, and so the issue was not relevant to them, although one mentioned a tie-in with an external product that could do this. One research participant stated that it was difficult to design around this risk while maintaining a useful system. Another research participant (T/O) noted that 'it is a genuine concern but it's not just for [my organisation]. I think it's a society concern.' Two research participants did think that this issue was important, and did have a system to deal with it, particularly where data was shared:

It's definitely an issue. … We deal with it mostly by providing mechanisms for redacting data when it comes to sharing. So giving analysts visual tools to be able to be very selective on the basis of classifications of types of data, types of properties or attributes about that data, particular values of data that they might want to exclude when filtering down some set of data that they need to share to get it to an

[77] See for example the discussions introduced in Chapter 2.

acceptable set of data that they are willing to then share with the partner agencies. So that's an example of where I guess we deal with – it's not quite de-identification but it's redaction of data in a similar way that you don't want to allow someone to re-infer things that you've taken out of that data set. So it's about giving people good visual tools, being able to very explicitly see what's there and then having … completely reliable auditable parallels that go along with that to allow the regulatory functions to begin to validate and verify what's about to go out to a different agency. (T/T **BV**)

In some systems where we retract or vet the information we cannot bring that back. … This might entail getting subpoenas to the defence, taking out informants name. If the defendant is a bikie gang member where the informant's life is in danger we need to ensure that what we provide to the defence is vetted in a way that they cannot find out what that name would be and will not go into details. We use custom tools because of importance of keeping information secure. (T/O **BW**)

One research participant commented on the risk of re-identification in a different context:

[I]t does get mentioned as one of the big concerns, that while you can de-identify, de-personalise individual data sets, could you use it to then triangulate to re-identify the data? That really comes down to the sophistication of the technical processes you use to de-identify the data. If you simply remove the name of the person, then you're leaving lots of data there that allows, by triangulation, to get back to who that person is. If however you use more sophisticated statistical processes like perturbation and those sorts of techniques to actually fuzzy the data slightly so that it - it's not possible to re-identify it, but it doesn't change it enough to alter the output, if you know what I mean, then – so it really comes down to how sophisticated those processes are as to how reliably they are de-identified. (P/T **BX**)

Agency inter-operability (see Lens 5.1.1). Research participants were asked about whether they designed systems capable of inter-operability between agencies. This was omitted from the table above, because the answers did not fit neatly into a Yes/No framework.

Four research participants saw agency inter-operability as a goal rather than a current fact, where the challenges were not technical.

At a technical level, yes, it's trivial to design around that. The problem is that there's no central way of enforcing those design decisions and each agency makes decisions that are in their own interest but those decisions don't necessarily promote compatibility between agencies. (T/T **BY**)

That's per system based right now. Obviously we could have a much better and faster standardised approach to sharing information if we had a large collection but right now it's per system. (T/O **BZ**)

It could be done. It's not done at the moment, at all well, because agencies tend to work on the exchange of narratives. Some exchange of raw data, but generally exchange of a written report, which is quite hard to enforce. I think one of the key things we'd like to see out of the [D2DCRC] integrated policing project, is systems enable rigorous exchange of data under some sort of mechanism or MoU. (T/T **CA**)

We have a concept … that technically allows us to query into databases and data sources of other agencies. So in theory yes, the capability's there technically. The policy and agreements in place are typically not. … So we provide that query … capability which is I guess the infrastructure and the software that allows agencies to have that interoperability at a technical level. (T/T **CB**)

One research participant went into some detail on how systems interact in practice, describing a manual, human-centred process:

> So [agency inter-operability] is a bit of an issue within our environments because most law enforcement agencies within Australia have completely different ways of dealing with data and formatting and storing information. Even when it comes to vendor-based systems, so commercial systems, it's quite a spread of different commercial systems. So inter-agency share or cooperation with data sets is very difficult for us to do. … [I]t's something that needs to be addressed more at a national level but it's something that's not necessarily easy to address because all organisations are doing their own sort of things and using their own commercial systems. So without there being more of a single body looking after data for all of law enforcement that normalises data or processes it in one central place, it's going to be always a challenge to have data accessible between different agencies. For us, we are an organisation where we work in partnership with [other Australian] organisations so the way we get around that is by having people seconded … and giving them access to the systems that we have. With some organisations, having our systems available within that organisation, so that if it's an operation happening out of a separate organisation, the data holdings we have can be accessed by certain people within that organisation or by our officers. … So there are lots of joint counterterrorism teams in each state and they all have access to each other's systems in a special facility and that might be housed in one or the other's organisations but everyone has access to the different systems and data sets. But technically they are isolated and so it's through the investigators themselves that the associations are drawn between them. It's more manual, or human interaction between them. (T/O **CC**)

Another research participant (T/O) explained that their entire system was to facilitate exchange of data between different organisations, but again the system itself was partly manual, where requests for data would take 'a few days'.

Two research participants described standards/systems to facilitate exchange of data between agencies:

> We have made a decision to move away from [Criminal Intelligence Database (ACID) using Standard Information Exchange Format (SIEF)] to a new system based on the national/international NIEM standard (National Information Exchange Model) that began in the US. ACID will be replaced in the next 5 years. Many agencies are moving, but some not immediately, rather on a replacement schedule. (T/O **CD**)

> What we aim to do is to take the technology out of the way as an inhibitor of sharing and to actually make it an enabler of systematic auditable and also policy driven sharing so that you actually are confident about what's going out across the wire between any two different agencies or indeed a disk in many cases … It deals with then the ability to, having shared data from system A to system B, have system B make changes to that data, have system A simultaneously make changes to that data and to then keep that data in synchronisation across those two different instances. So to continually be able to keep a single consistent view assuming they continue sharing. There's obviously a requirement to keep moving … information backwards and forwards about that data. But to allow then two agencies to sort of jointly keep developing that data. … [T]here needs to be more made of that capability. There is technology out there that can do a lot more than is being done… (T/T **CE**)

One research participant believed agency inter-operability was not an issue in practice for them because '[g]enerally we've got the skills to be able to transfer information and receive information in what you would consider to be electronic forms, standard interchange.' (T/O)

Cost was, unsurprisingly, identified as relevant by all research participants who addressed this question specifically. There was specific mention by those working inside operational agencies of budgetary issues. For example, those research participants referred to a 'very limited budget', the fact of design being 'tightly budgeted', the need for 'value for money', and the need to find products that were 'cost-effective to the limited budget that we have' but also the importance of 'cost saving long term' to allow for the fact that a 'Big Data solution may be expensive but would be operationally beneficial'. Even a research participant who had spoken of a more generous budget referred to cost in discussing system design.

Those working for private-sector technology companies (designing systems for agency use) recognised the importance of cost (for example, one research participant stated it 'absolutely impacts the way you design a system') but also emphasised that better systems sometimes cost more:

> I'd relate cost to outcomes. (T/T **CF**)
>
> So you can certainly design systems to different cost levels. The capabilities of those are probably somewhat related to the amount of money that is spent on them, but it's about prioritisation and deciding what needs to be done … (P/T **CG**)
>
> Cost is important. It shouldn't be very important though because the costs that you talk about when it comes to technology like this is fairly immaterial compared to the cost of not tackling the problems effectively. How do we deal with cost in our products? Look, our products are incredibly good value for money … (T/T **CH**)

Summary and implications

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). 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, cyber-security 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 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.

2.6. Values and Big Data

As reflected above [in 7.5.4], much of the debate about law reform comes down to questions of attitudes and values. In particular, different people can have different views on the role of consent of data subjects, on the importance of privacy and particularly whether it ought to 'give way' to security, and on the need for and importance of transparency in operational contexts. We thus asked research participants with policy roles a series of questions seeking to understand their position in these debates, as well as the sources of their views and understandings, the extent to which they perceived their views as in conflict with others and how they would address any such conflict. Selected questions were also addressed to research participants with primarily operational roles.

2.6.1. Protections where individual consents to use or sharing of their data (see Lens 5.1.2)

The Policy group were asked specifically for their views on an important policy question, namely 'what protections, if any, should remain in place in circumstances where an individual consents to the use or sharing of their data?' [P13] Three research participants did not wish to answer this question. The remainder expressed a broad range of views.

Consent must be meaningful, informed and freely given. Six research participants commented on the importance of consent being substantive, often commenting unfavourably where consent involves merely ticking or clicking 'I agree'. For example:

> I think it's unfair to expect people to be subject to these contractual arrangements that are obviously a fall-back to hard copy days but they've just been applied to the digital world. (O-P/O **A**)
>
> So [consent to end user license agreements or consent via notice on a sign] is not an effective mechanism to engage in serious questions. (P/P **B**)
>
> In some contexts there's little choice but to consent in order to engage or have the service or whatever it may be. (P/P **C**)
>
> Bundled consent has … problems. (P/P **D**)

Data must be used for a proper purpose. Five research participants referred to the need to use data only for a proper purpose despite the existence of consent. For example:

> There should be no use put which is alien to a purpose. [This is] mandated ultimately by parliament, so either expressly in a statute or permitted under a statute and therefore you'll always be able to get the judiciary involved one way or the other. (P/P **E**)
>
> [Using] any information you get in the course of your duties for something that doesn't relate to your duties … that's a criminal offence. … [Information given to police] needs to be protected so that people can't keep digging on that, particularly media. (O-P/O **F**)
>
> The individual should be contacted again if whoever is handling the data wants to use if for a purpose that they have not originally consented to. (P/P **G**)
>
> Information must be relevant for the purpose of collection and Big Data often grabs any information without a specific purpose. (P/P **H**)

However, one participant expressed some scepticism about the proper purpose requirement:

> The orthodox approach is to describe purposes and seek authorisation upfront. Whether this is still necessary is a society wide question. (P/P **I**)

Expiry and revocation. Two research participants referred to the need for consent to be revocable while another suggested consent could be formulated so that it 'cannot be revoked'. One research participant also referred to the need for consent to expire at some point while another stated it should be 'current'.

Some limits. One research participant pointed out the need for some limits at a very general level, stating that 'some things are not a good idea', giving the example of spying on civil servants.

Consent by victims and families of missing persons. One research participant noted that consent was frequently given by victims of crime and those reporting missing persons, and that in these situations:

> I should be able to say oh yes … I consent to [the police] accessing all my telecommunications data to try and figure out who broke into my house. … I think in this space, consent given in an informed way to the police to do these sorts of missing persons and victims stuff is good. (P/P **J**)

Data security. One research participant referred to the continuing need to ensure that data was securely stored.

Parental consent. One research participant mentioned the importance of involving a parent, guardian or trusted adult to help young people understand the risks of giving such consent or providing information.

Consent versus knowledge. One research participant pointed out that the *Telecommunications (Interception and Access) Act* did not require consent, but rather that knowledge was often sufficient.

Two research participants queried whether consent should be required at all. One commented on changing social expectations as to what was implicitly permitted, including the need to confine purposes and use up-front. The other expressed the view that citizens who seek assistance from government in an area or provide information to government to pay taxes have lost the right to privacy over the data provided to secure that assistance.

Summary and implications

Research participants in the Policy group 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.

2.6.2. Attitudes to privacy (see Lens 5.1.2)

Attitudes to privacy, particularly relative to other values, was raised by research participants in a number of contexts. For example, even though the Technical group was not asked to express their views on privacy directly, one research participant astutely stated in response to a question about future issues for Big Data, 'I think the ownership of data and the privacy issues around that are the real problem.' (T/T). Those with policy roles were asked to comment on the extent to which considerations such as privacy should give way in the face of serious, imminent threats such as child kidnapping, child sexual abuse or terrorism [P16]. Table 2-17 summarises their responses.

Table 2-17: Policy participants' attitudes to privacy (n=15)

	Research/NGO/ Private	Independent	Government	Total
Privacy not important in the face of such threats	0	1	1	**2**
Privacy should give way in the face of such threats	2	1	1	**4**
Need to find balance in circumstances	3	2	2 (both O-P/O)	**7**
It is primarily a question for legislation or political/ public debate	1 (P/T)	1	1	**3**
Other	1	0	0	**1**

*Responses in the fourth row can be coded in addition to responses in other rows. All respondents are P/P, except where noted in brackets.

Two research participants did not think that **privacy should be a factor at all**, in one case because they did not value privacy and in the other because they didn't see information used solely within an investigation as a privacy issue:

> I don't accept the first premise that it's broadly undesirable or undesirable at all to be having full access to any information which is capable of being accessed. … [Law enforcement] do the obvious, sensible, honourable and decent thing, is they use every informational resource they can within the law to help in preventing the atrocity, and it's not a question of leeway, it's a question of diligence in my view. (P/P **A**, who elsewhere described privacy as 'one of the complete myths of our time' and opined that privacy legislation 'has been grossly overdone and … has impeded lots of sensible things')

> I would say ''No. A crime has being committed. A wide analytical technique that accesses confidential data are legitimate investigative techniques.'' What is not legitimate is the publication of data used in investigation. … So long as it is in the course of an investigation, privacy is not implicated so long as data stays with the investigation. (P/P **B**)

Four research participants felt that privacy was a factor, but that **privacy should give way** in the face of serious threats. For example:

> I think many people would agree that imminent threats to live are really a special case where we should be setting aside the rules, doing the thing and coming back to it later on. (P/P **C**)

> I think we have to give them every opportunity to find the child [who is kidnapped]. For us, it comes back to the child. (P/P **D**)

> … privacy law understands that certain situations require privacy to give way to public safety and good public policy objectives. (P/P **E**)

The search for **balance that takes into account the specific circumstances** was expressed by seven research participants.

> You need to balance people's right to live in a safe and secure society against their ability to live their lives in a way that they feel comfortable with. … [M]y fear is that you use stories about eight year olds being kidnapped and terrorism suspects

[example from interviewer] in order to justify things that are not necessary to capture those instances and then may unduly invade upon the public's privacy. (P/P **F**)

Striking the right balance is very important and also not being too carried away with moral panics around terrorism and serious crimes. … [W]e do need a more sensible and rational debate around what is effective and what is not - proper evidence based policy. (P/P **G**, who also expressed a 'deep concern about privacy and about individual autonomy' as well concern for maintaining procedural justice and the presumption of innocence)

It's always a balance between what law enforcement needs to do its job and what the community expects in terms of what it needs to give up for that to be done. In these sorts of emergency situations really I think privacy falls to a second or third level issue. (O-P/O **H**)

… the kinds of things that should be thought about[:] is it necessary, is it proportionate, are there other means that can be used that are less intrusive? Or is the situation such that … there may be a more privacy intrusive mechanism that is more effective and efficient in the circumstances. (P/P **I**; See Lens 5.1.2)

It would depend on the depth to which they could probe the Big Data. So if you were going to just probe public sources or just probe metadata that might be of a different order than a hundred people's telephone conversations' contents or the contents of their emails. … I can see it would make sense in some cases but it's about the depth to which you probe that. (P/P **J**)

So the challenge, the overarching challenge, is to strike the balance between security, or better security analytical techniques and privacy. The challenge within that challenge of course is the expectations of privacy of individuals is changing. (O-P/O **K**, in response to a different question)

Some research participants felt it was a **political question or a question for the public** but expressed a range of positions on the chances that it would be resolved satisfactorily.

… [o]n the one hand, citizens expect the governments to protect them against the Lindt Café … event, and other terrorist attacks. At the same time they want all their privacy respected. … The fact is you can't have it both ways. That's a big political problem, is how do you marry that up? How do you meet both of those expectations? My biggest concern is that the level of political dialogue in this country is so simplistic, that no politician wants to actually broach the subject and have an intelligent conversation about this. So I don't hold a great deal of optimism in that issue being resolved easily. (P/T **L**)

I guess again these are policy questions for the public to nut out. This would be a very interesting survey to put to a thousand people to see what they think. (P/P **M**)

Research participants with operational roles were asked how they felt the law should strike a balance between privacy and individual rights and 'public concerns such as national security, terrorism and serious crimes'. Some research participants in that group did not answer directly, either:

- stating that the question was too hard,
- stating that it was an issue to be determined by policy experts, by reference to international best practice, or as a result of public debate,
- stating that it was a government decision based on measuring what precisely would be lost in terms of privacy and what the community impact would be, or
- stating that it was a question for the legislature to find the appropriate balance.

In a similar vein, one research participant referred to the need to understand and manage community expectations while another referred to the need for 'political leadership' to properly inform the public so that 'they can decide what is the impact if access is continually restricted'. Two of those who expressed a substantive view also emphasised that it was ultimately a political question to be determined in public debate.

Of those who responded substantively, research participants in this group were **primarily concerned about the need for access to data**, although research participants also referred to the need for audit, safeguards or protections:

> … I think all agencies should be able to … have access to the information that sits publicly within government databases but we've just got to properly record when that data is accessed. … I think everybody should hold their own databases but … everybody should be able to have access to it but that needs to be audit -trailed and what that information was used for. (O-P/O **N**)
>
> I think the laws need revision. I think if the broader Australian community knew that I couldn't access tax data to undertake a [counterterrorism] investigation they'd be flabbergasted. … The information … is only collected for a particular purpose and then there needs to be safeguards again as to how that's then shared.… [P]otentially people's privacy needs to give a little bit so that the overall national security benefit can be realised (O/O **O**, commenting specifically on the current heightened threat environment)
>
> I think there are situations where the use of data can actually be for the greater good and for the individual good. In situations like that I think my sense is the majority of people would say that's an appropriate use. Where information is used to breach people's rights to privacy, to be used against them from a legal perspective where they don't have any recourse to correct it or to be used against them inappropriately … that's when I think it's inappropriate and there needs to be some protections in place. (T/O **P**, stating also that protective regulation should focus on how data is used and what recourse is available, rather than who can access data)
>
> … I think personally that privacy is … a crock. … we've got great examples of where privacy has gone mad. [Gives an example from US context] … I think you see the same kind of logic in the Australian context. There's this notion that privacy is actually a right and that as a right it trumps safety. Or privacy is a right and it trumps security. … Then … almost by a sort of logical absurdism, you've won the argument because you say … what if the Australian government went mad and started to try and destroy entire populations and became a totalitarian state? So you put these checks in place and you call it privacy, and you privilege privacy over other principles or … sources of expectation. … We police by consent. You get something like privacy put up as a stonewall but generally I think our settings are pretty good. Because we can still generally get through that when and as needs, although I think that sometimes … the decision maker [for a warrant] is someone outside of the criminal justice system generally … they don't necessary see the extreme or the depth or the extent of criminality and therefore the legitimacy of the tools that are sought to be used. So … privacy and other principles of constraint perhaps are sometimes not balanced against the actual targets we go up against. … I think sometimes there's a degree to which … one hand is tied behind the back in an effort to try and balance out the fight between the state and the individual in some of these instances. … You'll often have a technical capability that's available to an individual but not available to government agencies necessarily. (O/O **Q**)

Two research participants referred to the **need for checks and balances**, or simply balance, in enhancing operational capacity while providing appropriate protections:

> … there needs to be checks and balances in the system. I think what we need to do is look at the effectiveness of those checks and balances in the system rather than talking about the actual capability of what we should or shouldn't be doing. … [W]hat we need to do is not limit capability but work really hard on making sure that oversight controls … [exist] in a very public forum. (O/O **R**)

> We need to protect people from crime and from privacy threats. The state has to do both. … Privacy is something to be cherished. … I want to protect kids from crime and protect their privacy … But the balance is hard. [It is] never going to be easy and nor should it be. (T/O **S**)

One research participant linked this question to media-driven perceptions that reducing privacy for some groups (such as the Muslim community) would make people safer. That research participant pointed out that interference with individuals ('raided, searched, detained') was ultimately 'at the expense of the Muslim community or whatever community it is'. (P/P)

Summary and implications

> There was a wide spectrum of views among 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.

2.6.3. Privacy versus Security: A scenario (see Lens 5.1.2)

In order to gain greater insight into the ways in which research participants with policy roles believed that concerns around privacy (including surveillance) do or ought to interact with concerns around security, we presented research participants in that group with a scenario. The scenario varied slightly over the course of the interviews (removing extraneous and irrelevant material such as how much time had passed, which tended to distract rather than focus the issue), but the core of the scenario was as follows:

> *Lucy is an 8 year old girl who has been kidnapped from her home in Lane Cove in Sydney. All avenues of traditional physical surveillance and canvassing of the area so far haven't produced any leads. How do you feel about the immediate and expeditious use of Big Data tools in these circumstances? **[P15]***

As one research participant noted:

> It's an interesting example, because from a public perspective as well, an eight year old girl, emotion would come into it. I often wonder, … people who may have raved about privacy and protection of privacy previously, when it comes to that sort of circumstance do they change their view on that? Or would they keep insisting that privacy [is inviolate] and you shouldn't be using data to find the perpetrators or find the girl. (P/T **A**)

This was essentially what this question set out to test. After an initial response to this scenario, and in order to further test where research participants would draw lines, research participants were asked a series of more specific questions, in particular their response to:

a) A metadata search of all known kidnappers with previous arrests in the area matched against CCTV footage from public and private sources in Lane Cove on the day of the kidnapping
b) Collection of data and monitoring of all known kidnappers including known addresses, registered telephonic devices, social media accounts and email accounts
c) Facial recognition deployed on CCTV footage across all Sydney and surrounding areas, and multiple social media networks, in an attempt to identify Lucy
d) Metadata from all devices of all family members of Lucy, her neighbours, and people seen visiting the house that day (including a postal worker, package delivery service, water meter inspector).

Research participants where then asked whether two changes would alter their response. In particular, they were asked whether it would make a difference if there was a suspicion of paedophilia and whether it would make a difference if there was a suspicion that the kidnapping was linked to terrorist activity (for example, an intent to blow Lucy up in a public place).

Table 2-18: Responses to general kidnapping scenario and specific prompts

	Agree to use tool	**Agree to use tool with caveats**	**Reluctant to use tool**	**Other**
Initial response	**8** (6 P/P; 2 O-P/O)	**5** (1 P/T; 3 P/P; 1 O-P/O)	**0**	**3** (3 P/P)
Prompt (a)	**7** (4 P/P; 2 O-P/O; 1 P/T)	**6** (5 P/P; 1 O-P/O)	**2** (2 P/P)	**1** (1 P/P)
Prompt (b)	**5** (3 P/P; 2 O-P/O)	**5** (3 P/P; 1 P/T; 1 O-P/O)	**5** (5 P/P)	**1** (1 P/P)
Prompt (c)	**9** (6 P/P; 2 O-P/O; 1 P/T)	**3** (3 P/P; 1 O-P/O)	**2** (2 P/P)	**2** (2 P/P)
Prompt (d)	**5** (3 P/P; 2 O-P/O)	**8** (7 P/P; 1 O-P/O)	**0**	**2** (1 P/P; 1 P/T)

* Some respondents mentioned general caveats in giving a positive response initially. Where these were repeated in relation to specific prompts (including by reference), the research participant was placed in the 'agree to use tool with caveats' column. However, where the research participant did not mention the earlier general caveat but gave an unconditional positive response to the prompt, they were put into the 'agree to use tool' column.

In their initial responses, all research participants who responded were generally positive about the use of Big Data tools in this scenario. Three research participants did not substantively respond until further prompts were provided. One research participant put it in strong terms:

> This information is ours [citizens as a group]. It's our resources, like the roads are our resource, and I wouldn't want the police to apologise and drive slowly on the

> road to the scene of the abduction, nor do I want them to apologise and only gingerly get into Big Data. (P/P **B**)

Some respondents suggested specific techniques including mapping entity relationships and networks, checking family court records, checking DOCS data, analysing transportation through motorway records or public transport cards, exploring financial data such as credit cards and GPS data for people of interest, using CCTV footage possibly with facial recognition, using local cell site data, geolocation of suspects, tracking Lucy's mobile phone, and cross referencing some of the above data sets against police intelligence nationally. There were also some caveats that some research participants felt ought to apply generally including:

- the need to comply with legal requirements (O-P/O),
- the importance of independent oversight mechanisms (P/T),
- the need for transparency (discussed in more depth in the following section) (P/P),
- the need to minimise privacy impact on non-suspects (P/P),
- the need to limit who can see the data (P/P),
- the importance of interpreting results carefully (P/P), and
- the need to draw boundaries, such as recognising distinctions between a young child and an older teenager who may go missing for different reasons (P/P).

Note that these caveats are not repeated in full below where proposed by the same research participant in relation to a specific prompt.

One research participant noted that the *Privacy Act* deals with this kind of situation sensibly:

> [W]hen I spoke before about an appropriate balance in the *Privacy Act*, there are exceptions that allow data to be used and disclosed … firstly where it's authorised or required by law, or if it's required for law enforcement purposes – but also where there's a serious threat to the health or well-being of an individual. So sometimes there can be a lack of understanding of how the *Privacy Act* applies in certain circumstances. It can be held up as an impediment or a blocker to information freely flowing, whereas in fact there are very practical exceptions that permit that. An example is under the *Privacy Act* … the Privacy Commissioner can make rules and has made rules in relation to the location of missing persons, so on tap with this. They were developed in consultation with the police and Red Cross and those who are all involved in locating missing persons. So a framework that's practical and that works for those entities has been developed up and provides guidance around how to appropriately handle personal information in those very serious situations. (P/P **C**)

Another research participant was disinclined to express a view on the specific prompts but stated generally:

> … I would say is the kinds of things that should be thought about is that idea of is it necessary, is it proportionate, are there other means that can be used that are less intrusive? … Right through from the development of legislation and the compatibility of human rights statements that have to be associated with that, that those things have been thought through. (P/P **D**; see Lens 5.1.2)

In response to the **probe (a)**, there were some specific caveats suggested:

- No repurposing of data (P/P)
- No harassment of former offenders who have not committed this crime (P/P)

- Limiting ‘known kidnappers’ to those whose past offence involved a stranger rather than family member (P/P) or after some other ‘pairing down’ process (P/P)
- Requirement to obtain warrant (P/P)
- Data must be available only to police (P/P)

One research participant gave a detailed response here, both on the current law and the policy settings that ought to apply:

> Probably not lawful under the [*Telecommunications (Interception and Access) Act*] – currently – because you’d have to get an authorisation to access Joe Bloggs’, the kidnapper’s, data. So you’d have to say I think that accessing Joe Bloggs’ … data is reasonably necessary for the purpose of enforcing the criminal law. If I have literally no traditional physical surveillance that has produced any lead connecting Joe Bloggs … to the disappearance of Lucy, it’s very hard for me to sign off on that authorisation to access Joe Bloggs’ … data. So under the current legal paradigm, probably not a thing you could do. The next question is, from a policy perspective, would it be justified to access Joe Bloggs’ … data to see whether or not there was any connection. … If I was Joe Bloggs the kidnapper I would rather the police access my metadata, saw that I was sitting at home watching Netflix all day and then didn’t knock on my door. …. But - I don’t know. Maybe the public would say better that the police overtly and with consent knock on the door and then Joe Bloggs the kidnapper gives consent for his metadata to be accessed so that Joe Bloggs’ privacy is not infringed. (P/P **E**)

Two research participants (P/P) had reservations here. One was concerned that it was ‘not based on any real intelligence’ and ‘once someone has served their time, that’s it’. The other felt that it was ‘too intrusive’ to a person who may have a prior record and been in the area at the time but was not the one who committed the crime, and that metadata was ‘too simple’ to be used.

In response to **probe (b)**, the suggested caveats were:

- No repurposing of data (P/P)
- Independent oversight (P/P)
- Requirement for a warrant (P/P)
- Limitation to situations analogous to the scenario:

  > My concern is always around, for want of a better expression, the use of those capabilities in peace time. In other words when you don’t have this example of a kidnapping in a real situation, how do you prevent policemen just coming, stand[ing] over people, by harassing people and snooping around when there’s no cause. (P/T **F**)

Five research participants expressed reluctance here:

> That seems pretty extreme. (P/P **G**)
>
> This is not a proportionate response. (P/P **H**; see Lens 5.1.2)
>
> I don’t know if we should be just speculatively intercepting the phones of a whole bunch of people … Under the current law there’s just no way that if you went to … a legislative issuing authority and said I’d like to have a thousand interception warrants for all of these people, the judge is just going to laugh you out of the room. In fact, one of the things we have in our data is that very few warrants get rejected. So when people go to issuing authorities, the issuing authorities in 99.99 per cent of

> instances issue the warrant. People say these issuing authorities are a sham. They just issue – always issue warrants. But the truth is that police are professionals and they know when they can and can't win the argument. So the police just know that that warrant would never be issued and just never ask for it, which is why that dataset looks weird. (P/P **I**)

> I think it would have to be more than just the fact that they've been kidnappers. There would have to be some more suspicion that they were somehow involved. Probably some of them … could be ruled out of investigations. (P/P **J**)

> It's like 1984 … I don't think the state should be doing stuff like that. (P/P **K)**

In response to **probe (c)**, there was only one suggested caveat:

- No repurposing of data and destruction of data when no longer required (P/P **L**)

While two research participant were more positive about probe (c) than probe (b):

> [In probe (b)] you're going to start targeting particular people who may have absolutely nothing to do with this, whereas if you're using data about the child it's more likely to turn up somebody who's got something to do with her. (P/P **M**)

> I react badly to you intercepting my phone and listening to what I am saying but I don't react so badly to that surveillance camera scanning my face for an analysis purpose. … What is it that makes me think … one is a private thing and one of them isn't a private thing. … I don't know what the paradigm here is. But for whatever reason, people react very differently to these two things and one of them is lawful and one of them is not because of that difference in public reaction. The diagnosis of that, a very interesting question I think. (P/P **N**)

another research participant was more concerned about probe (c):

> I would think that would be actually far too much information that it's not even helpful and also disproportionate to the aim, because that way you would be interfering with the privacy or data privacy of many people who have got nothing to do with the case. … (P/P **O**; see Lens 5.1.2)

One research participant (P/P) was equally concerned about probes (b) and (c).

One research participant (P/P), despite expressing an opinion, did not give a final view noting it was 'a question of values for the public to decide'.

For **probe (d)**, the suggested caveats were:

- Very narrow remit for searching metadata (P/P), for example around narrow time frame related to disappearance (P/P)
- No repurposing of metadata; destruction of metadata when no longer required (2 P/P)
- Only for those seen at Lucy's house, not people connected to those people or further degrees out (P/P)
- Only if reasonable suspicion following police questioning (P/P)
- Only if judicial warrant issued (P/P)
- Only if authorised by internal investigator who certifies it is relevant to the investigation (P/P)

Two research participants (P/T, P/P) were not asked this probe.

Another research participant would have gone further than the probe in looking at metadata:

> I'd go for more than that. I'd go for the cell sites that are nearby … that will be thousands of people in Lane Cove, including people that are going down through the tunnel and all that sort of stuff. So it's a fair bit of data but if you've got a lot of data there you can quickly analyse that against other known databases and that's where you need your good analytical tools. (O-P/P **P**).

Only one research participant (P/P) felt that **changing the context to paedophilia** made a substantial difference to their response. In that case, the reason for the distinction was the established nature of the sex offenders list compared to the concept of 'known kidnappers', thus changing the response for probe (a) and probe (b) from reluctance to agreeing to the use of the tool with caveats (that the use of data be sufficiently targeted). One research participant (O-P/O) suggested that they would 'be going in harder and faster' and that additional data may be relevant depending on the context. Another research participant (P/P) believed that 'it adds a sense of immediacy and certainly heightens the implication of wrongdoing' but did not change any substantive response. Most research participants, however, dismissed the idea that it should make a difference, pointing out that all both contexts were sufficiently serious.

On the other hand, six research participants felt that **changing the context to terrorism** made a substantial difference to their response. One research participant (P/P) would be willing to extend the range of people whose data could be examined depending on the depth to which their data would be probed and provided there was sufficient public transparency. Another research participant (P/P) would put in the same requirement for a judicial warrant but believed it was more likely to be granted. One research participant (O-P/O) noted that different actors would be involved if the context shifted to terrorism because it would become a federal, and possibly a defence, issue.

Another research participant expanded on this in explaining why:

> So legally here you switch gear very drastically as a matter of law because you move from the *AFP Act* to the *ASIO Act* and you move to a whole different part of the *TIA Act* about access for the purposes of the *ASIO Act*. So this is a very different legal paradigm. You can definitely do … more under the purposes of the *ASIO Act* than you can do under the serious offence provisions for the police. It's not exponentially more. It's another step up but it's not a whole different paradigm. (P/P **Q**)

This research participant was thus more comfortable collecting and analysing metadata and surveilling known terrorists compared to known kidnappers.

One research participant made a more general point about the different categories:

> Always paedophilia and terrorism are the two examples. The difference in a way regarding terrorists is that it may include people who have never been tried whereas paedophiles would have been. For terrorists one would look at people under suspicion, I assume that law enforcement agencies have a list of such. (P/P **R**)

Another research participant gave a mixed response:

> I'm not sure that from a law enforcement perspective the priority would change. [T]he resources may be outside the Big Data sort of scope that would be available to respond because in terms of the risk to the public the risk here is immediately to Lucy in this one. If you throw in counterterrorism and you throw an improvised explosive device or some other device into that you're talking about more people getting hurt than just Lucy. So that would actually have a different sort of scale. (O-P/O **S**)

The remaining research participants stated that the terrorism context would not affect their response. One research participant argued vehemently against there being a difference:

> I have lived with terrorism now for all those years and I am utterly impatient of the idea that it has a qualitative difference that could justify a greater … invasion of so-called privacy than other offences, ... [like] ordinary murder. … [I] do not distinguish in the social urgency of … getting information, and it is nonsense, in my view, to say that the supposed motivation of the perpetrator could tell you anything about the appropriate limits or controls of the resort we have to information in order to either prevent if you're being hopelessly optimistic or to investigate and punish. (P/P **T**)

Summary and implications

The scenario presented an opportunity for more fine grained analysis of how research participants 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, 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.

2.6.4. What transparency is required (see Lens 5.1.8)

We asked research participants with policy roles (and one T/O who expressed an interest in policy matters) to comment on the extent to which there should be transparency about the nature of data collected or the algorithms employed in analysis, both within an agency and more broadly [P18]. The results are shown in Table 2-19.

While some research participants noted that transparency offers clear benefits in an open democracy and increases the likelihood that errors or biases will be picked up, others pointed out challenges. In particular, there are benefits in preserving secrecy as concerns operational capabilities. Most research participants concerned about preserving operational secrecy argued against full disclosure of algorithms. On the other hand, no research participant expressed the view that the data sets being accessed should remain entirely confidential. A number of research participants expressed an intermediate position as to data or algorithm disclosure (or both), arguing either that the 'envelope' within which government should operate should be transparent or else that a balanced approach was required.

Table 2-19: Views of research participants with policy roles on transparency of data and algorithms

	Data should be transparent	**Data envelope / some information about data should be transparent**	**No comment re data**
Algorithms should be transparent	**4**	**0**	
Algorithm envelope / some information about algorithms should be transparent	**2** (1 O-P/O)	**3** (1 O-P/O)	
Algorithms should not be transparent	**4** (1 P/T)	3 (1 O-P/O; 1 T/O)	**1** (O-P/O)
No comment re algorithms	**1**	**0**	

* No multiple coding. All respondents are P/P, except where noted.

A number of research participants referred generally to the **advantages of transparency.** For example:

> It's very important it's transparent to the public because it's got to match community values. (P/P **A**)
>
> Being open and transparent [as to] what data sets governments are matching … can be a deterrent. (P/T **B**)
>
> We need transparency as to what they can do and do do in data matching – such transparency is a healthy mechanism to avoid abuse. There are always edge cases in the grey zone. If no one knows what is going on, then the risk of entering the black zone is a lot higher. Agencies have a natural tendency, which is not to talk because they are worried about the grey zone. But in the long run from society's perspective, that is dangerous. (P/P **C**)
>
> Accountability is a good thing, no hiding behind confidentiality and privacy as a barrier. … There should be reports to the public about the use of Big Data, need for external review and public reporting: when certain mechanisms have been used, number of times, how many effective results, how many breaches, and were the breaches notified. (P/P **D**)
>
> [I]f it's anything other than transparency it just feels like a police state. (P/P **E**)

On the other hand, there are some **risks of transparency**, particularly for algorithms, as agencies do not wish to disclose their operational capacity:

> [I]f you told them what the algorithm was that was being applied to a particular data set, you might as well not do anything because they'll work it out and work around it. (P/T **F**)
>
> … capability protection … is absolutely important because these capabilities are massively expensive to develop. … If you can do something that people think you can't do, it's massively valuable. (P/P **G**, who went on to discuss the example of the Allies in WWII who hid their ability to break the Enigma code)
>
> … it's about capability and every time you disclose capability you weaken the effect of that capability. (O-P/O **H**)
>
> … we would be concerned about losing our operational capability and our operational advantage. (O-P/O **I**)

> In the stock exchange world, every exchange holds rules closely because they don't want people to work just outside the bounds. This is similar. (T/O **J**)

> … there's going to be reverse engineering and preventive approaches. … So no agency should ever be required to publish its analytical approaches. (P/P **K**)

> [The reason that] you don't want to publicise them is that you open up exposure and the other reason is that it can reveal a law enforcement investigative technique so therefore there is secrecy as it might compromise an investigation or investigative method. (O-P/O **L**)

While most of these arguments against transparency focussed on algorithms and analytic capacity, the same argument was applied by one research participant to information about which data are accessed:

> If criminals know what is collected, they will avoid leaving a trail … We don't want criminals to know where we are looking. (T/O **M**)

Many of the views expressed were **balanced**, suggesting that what ought to be disclosed needed to be carefully defined:

> … to explain the examples [as to the uses of telecommunications metadata for intelligence and law enforcement] is to show what capabilities they use and then our adversaries, … people with criminal intent will be able to undermine those capabilities. … But now … as an Australian person – we have a right to know what's happening. Within limits. We can't expect to know all the secrets otherwise we couldn't protect our secrets and we couldn't protect our interests. But I do think, and I do think the Australian Government and other governments are going to have to be more open in what they're doing, how they're doing it, and most importantly how they regulate and oversee their law enforcement and intelligence agencies capabilities. … If there's no risk of exposing the law enforcement or intelligence capabilities then those techniques could be made public. But … if exposing those capabilities nullified the capability then of course you wouldn't expose them. (O-P/O **N**)

> There should be more transparency but operational methods need to be protected to retain utility. It is a balance. Unless it causes issues, the default should be disclosure. (P/P **O**)

> There should be those characteristics that you could say … our algorithms meet this industry standard or … whatever the appropriate mechanism was, that's the sort of assurance or transparency I think we should have on it. (O-P/O **P**)

> I … completely understand that there … cannot be total transparency. It may jeopardise some Law Enforcement activities. … I think before [data access for law enforcement agencies] is expanded [we need to have] a clear and transparent picture of what's going on – bearing in mind the risks to Law Enforcement that too much transparency can cause. … I do think there should be transparency around … how [the algorithms are] being used … It's very important that we ensure that there's accuracy and they're robust, especially if the consequences of their use at least partially can be very severe for people. (P/P **Q**)

A particular middle ground position expressed by one research participant was that the data and algorithms not be transparent, but that it was important that the envelope in which agencies could operate be transparent:

> I think the data collectable, disclose. The analytics that could be run in principle, disclose. The actual data collected, protected. The actual analytics run, protected. So

> let's tell people about the envelope. … But let's not tell people which of those datasets we actually pulled and what we ran against what for what purpose. Let's keep that to ourselves. (P/P **R**)

Those who were concerned about maintaining secrecy vis a vis the public often stressed the **importance of transparency for users within government, and also for independent oversight officers and agencies** such as those identified above (ombudsman, IGIS, Privacy Commissioner etc). For example:

> Should there be so-called blinded researchers? No. It's not a game … there should be continuous improvement, technically … you can't continuously improve something without understanding (P/P **S**)

> [W]ithin the agency it's very important that people understand what's collected, how it's analysed and how it's reported and what can be reported. They must understand that. … generally speaking in the interests of good governance and in the interest of transparency and oversight, yeah, they need to be known internally. (O-P/O **T**)

> … they need to be able to understand the quality at that stage of the information that they're actually making a decision on. So if we were going to make a decision to take a particular course of action, execute a search warrant, seek a surveillance device, those sorts of things, we'd want to know that we were meeting the standards for an affidavit because we're swearing that. (O-P/O **U**)

> I think sharing within or between government agencies, having some transparency there, I think could be appropriate at times. I think transparency certainly towards the Privacy Commissioner, for him to satisfy himself that no rights are being violated, I think is important. (P/T **V**)

> … it's okay to have a bit of a black box going on inside these agencies and saying here's the legislative provisions that we work inside. Here's the ombudsman who confirms to you in a public report that we indeed operate inside the legislative provisions. Here's the [Inspector General for Intelligence and Security] that confirms that we operate inside those provisions. … You kind of want the person advising government about what the paradigm ought to be to have some kind of good understanding about what the actual challenges these people are facing are. (P/P **W**)

On the other hand, it was recognised that there were **limits for even intra-government transparency**, both in terms of technical comprehension of users and in order to protect operational capabilities from potential leaks:

> The end customer won't understand all the inputs and mechanisms. There is an element of black-boxing … (T/O **X**)

> … they need an understanding of the potential for error – that is false positives and false negatives. I am not sure that every investigator needs to understand the full science. (P/P **Y**)

> Obviously every person in the agency's not going to understand every aspect of it because it can be highly technical. Sometimes in the interests of maintaining the integrity of a capability not all people in an agency will know about a capability. (O-P/O **Z**)

> It's all on a need to know basis. (P/P **AA**)

> The flipside of this of course is if you tell everyone about your capability then your chances of a damaging leak is increased …. So you do need to protect your

> capabilities internally as well as externally. … You need to navigate that just on a factual basis about how much information do people need to know – to be able to make good decisions of the decisions that their jobs require them to make. (P/P **AB**)
>
> It's the sort of thing that you do need to compartmentalise. All others in the agency need to know is what is produced not how it's produced. … any opportunity for capability to be exposed diminishes its value. (O-P/O **AC**)

Summary and implications

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 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.

2.6.5. How views align with others

Research participants with policy roles (and one T/O who expressed an interest in policy matters) were asked to comment on how their views about the design and regulation of Big Data aligned with the views of other stakeholders [P19]. Research participants generally agreed that there was a divergence among up to four sectors: rights-based NGOs (and some community groups), victim-aligned NGOs, industry groups and government agencies, with themselves located at one of those points:

> Well I think that it's a very, very wide spectrum of stakeholders. We certainly align with a lot of them because I sit on teleconferences with them and we are at one. Those range from just tech NGOs and industry groups to human rights NGOs and privacy NGOs and associations. Cleary they don't align with the intelligence agencies and law enforcement who would have … a very different view about what tools. It's not unreasonable in that most people who do their job day in and day out would rather have tools that make their job easier and faster to do. It's just that uniquely law enforcement and intelligence in having those tools has the capacity to kind of rip open the lives of the micro citizen. So things that slow them down or at least put some checks or balances on them doing that are kind of important. Annoying I am sure, but important. (P/P **A**)
>
> My views are probably not aligned with those of Law Enforcement. On the civil society side then at least from the perspective of communications groups, Australian Privacy Foundation …, digital rights groups and human rights groups I'd say my views

> … would probably align. Perhaps some kind of child protection groups, … groups for the victims of crime…there might be some more divergence on the civil society side. (P/P **B**)
>
> My views align with … those people … concerned with the rights of individuals. (P/P **C**, who also compared position with 'gung-ho law enforcement people who want DNA taken at birth, everyone has an ID card at birth')
>
> The only ones I know of are the views of the intelligence agencies – we would just talk about where the balance lies. Our views are close rather than far or at the margins … With the agencies, sometimes we agree to differ. Tensions do not need to be resolved. (P/P **D**)
>
> … I am dealing with … the telecommunications industry. … My colleague … had to understand from an enforcement agency perspective. I don't think either of us are close to the civil society perspective on it, it is largely parliament who has to reflect on that. (P/P **E**)
>
> I think we're pretty consistent, certainly in the law enforcement space. We're not necessarily consistent with those in the privacy space. (O-P/O **F**)
>
> [We] probably don't align with the privacy advocates but there may be greater common ground that we think but that's just bitter experience on other issues where we want to access the information. I guess we probably align on the information quality and accessibility type issues at an agency level with other agencies. (O-P/O **G**)

Some research participants put themselves in a middle or moderate position within the debate:

> I think if I can characterise my views they're probably middle of the road. … I have privileged knowledge about how these things work in the intelligence and law enforcement communities and I also know the importance of applying Big Data analytical techniques in Australians' interests. But I'm also … very concerned about the intrusiveness, the power, of those capabilities … I can understand why we need them but … the more intrusive those powers are the more rigorous the oversight has to be and the more we need to know about that oversight. (O-P/O **F**).
>
> So one axis is the parliament and the public. The other balancing act … is the agencies …, their mandate is to want more. If your job is to protect national security, if a bomb goes off in a café it's a terrible day for you. You want to do everything you can do …. Then the other side of this is the [telecommunications] industry itself … [they] want to do the right thing but conversely they don't want to have to bear millions of dollars of capability lost to benefit the agencies. … So I suppose these people's views don't align. … The parliament here is just wedged between the special interest group of industry, the agencies … [and] the parliament has the constituents in the public. (P/P **G**)
>
> I think [my views] are broadly aligned with stakeholders. … there's a healthy debate around whether or not privacy principles are appropriate in a Big Data context. … [The conversation at and around the Asia Pacific Privacy Authorities meeting] is leading both sides to reflect on … elements of each other's arguments as to how they in fact both could be accommodated. (P/P **H**)

As noted in 2.6.2, one important difference among research participants was their attitude to privacy. Two research participants characterised divergence in views on this basis, rather than based on sector:

> … I really do deeply disagree with a privacy-oriented approach to Big Data. I deeply disagree … this weird ultra-right wing libertarian anti-government approach. I can't stand it. It's deeply unintelligent and deeply unfriendly among people. It's anti-communitarian. They're only too happy to get the benefit of social cooperate and then to slag off at the means by which it's actually accomplished. … I think that it's quite likely that my position will be travestied by people or caricatured by people … as showing that I've been duchessed by the agencies. (P/P **I**)

> I think the only opposition we have are from those who have expressed concerns around privacy and how [metadata retention] will all be managed. (P/P **J**)

Some research participants felt that particular viewpoints were often omitted or marginalised in the public debate, for example the views of children and young people (P/P).

Differences in views were often linked by research participants to (sometimes necessary) public ignorance, for example:

> I have a better insight so a better understanding of why certain information needs to be accessed (P/P **K**).

> The interesting thing is … it's not that they're not anti-law enforcement, I actually think that sometimes there is a lot of information about what we actually do do with [data]. I just get sick and tired of reading in the newspaper the things that apparently we can do, or apparently that we're doing with all this information. I know, because I've been doing this for 30 years, I know what we can do and what we can't do and what we're going to do and what we're not going to do. … It muddies the waters. Like this whole argument that we had recently about metadata being kept for two years, telecommunications metadata. The ridiculous argument that was put through the press around we'll have access now to journalist's sources and therefore no-one is going to talk to journalists or politicians and we're going to continue to access their information. We've been able to do that since 1979 and in the last two years we've only accessed three journalists. Out of all the investigations we do, out of the 56,000 requests that we made three were for journalists and yet they got a separate section made for them in the Act because it's a squeaky wheel and they made a lot of noise. They think we're just going to listen to everybody. We don't have the … inclination to do that. I couldn't care less who they're talking to but I do care about catching terrorists and so on. (O-P/O **L**)

> Most don't understand (T/O **M**).

> The general population take their lead on what they see on the TV. It's not [an] informed view that they have. (T/O **N**)

> So from a privacy side, our ability to access and what we can do with data is highly regulated but the public perception is that we have more open slather to data and a bit of a disregard for privacy. But I suppose that's not the case. Some of the risks for us, I suppose that's a bit of a spin-off from that maybe is that public perception of our requirements and our oversight and our access to data is far from the reality. (T/O **O**, in response to another question)

Ignorance could also be linked with alignment, rather than divergence, of views:

> I think there's a high level of ignorance about what's actually possible, or what … greater use of data that agencies and organisations could make. I think a result of that is often a greater alignment between various stakeholders saying 'yep that's a great idea', 'yeah we should do that', and 'that would be really valuable'. (P/T **P**)

Summary and implications

Research participants 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 views: 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 discussed in 2.6.4, 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.

2.6.6. Resolving conflicts in values

Those who expressed the view that there were a diversity of views were asked how that conflict might be resolved [P19]. The suggestions broadly fell into four categories:

1. reducing the information gap between relevant agencies and those outside, including the general public – mentioned by **7** research participants;
2. facilitating conversations, debates or discussions (with a diversity of views on who should be involved) – mentioned by **6** research participants;
3. finding the middle ground in the debate between national security/law enforcement and those concerned about privacy and oversight (with a diversity of views on where the middle ground lay) – mentioned favourably by **4** research participants and opposed by **1**; and
4. enhancing trust in the relevant agencies - – mentioned by **2** research participants.

Reducing the information gap (see Lens 5.1.8). Seven research participants felt that the information gap between the agencies and others, including the general public, needed to be addressed and that this would lead to a greater alignment of views. The challenge is that identified in 2.6.4 above, namely the need to balance transparency against the need for operational secrecy.

> For civil society, there is a dilemma. I realise why I appear to lack credibility given that I cannot give reasons. It is a real dilemma. … There could be a perception that oversight is weak. Oversight is better than can be explained publicly. (P/P **A**)
>
> The problem with the regulatory and oversight mechanisms is that their implementation is not seen by Australia's public on a day to day basis for obvious reasons. There's high level information out there for the Australian public to see in relation to the oversight but because the detail is not there it's right for people to be sceptical about that. If we didn't have a sceptical public we'd be in trouble (O-P/O **B**, in response to a different question)

There were, however, some suggestions for enhanced transparency in order to facilitate public understanding of the need for enhanced collection of, access to and/or use of data as well as the protections that are in place:

> It goes back to transparency – some people are mightily aggrieved by data retention laws. That degree of grievance might drop away if there is more transparency about how often, for what purpose and how is it done. If the powers are abused, they will say that we were all right and you cannot trust them. (P/P **C**)

I think people have to be really clear about what it is, why government will need it. … Why they would need it, and then how they would use it. Who knows about it once they've got it, as well, the dispersion of that information and how far it goes. (P/P **D**)

Education is key. Also among the community generally, not just policymakers. People think that we can do things that we can't. So some transparency is good but we must balance that against the risk that we expose our methodology. (T/O **E**)

[These kinds of conflicts can be resolved] sometimes by more information around what we actually do. Public examples like we've got about how we use metadata and things like that. … [T]hat people know why we're using it for is important. It's the how that's the bit that you need to keep secret. (O-P/O **F**)

I really do think it should be the subject of much better information in terms of civics education. People need to know that these things exist. (P/P **G**)

[People have to know] how individuals are protected, for anyone abusing that type of information. … I think that there is that fear that Big Brother will happen. That's a huge risk. So I think … we need to ensure that … [the scope is defined]. (P/P **H**)

One research participant suggested that ignorance was not only an issue for the general public, but could also exist within government:

There seems to be a lot of folklore and myth about what you're allowed to do and not allowed to do. Often when you actually say no show me the legislation, it's actually quite different to what people had assumed it to be. So there's a lot of hubris around what the constraints are. They're often not nearly as strict as what people are led to believe. (P/T **I**, in response to a different question)

Conversations (see Lens 5.1.7). Six research participants in the Policy group discussed the possibility that conflicts could be resolved through conversations, discussions or debates, either among specific stakeholders or more broadly. The quotation in 7.3.1D is also relevant here.

I actually think you should take a set of people from civil society and I don't mean the soft pleasant ones in Australia and lock them in a room with a set of intelligence agents and law enforcement and spend about two days role playing a set of scenarios. They should be real scenarios that law enforcement and intelligence come across. Potentially they should use some of the real analytic tools that these guys use maybe not necessarily the real data but they could populate a faux database similar to real data. At the end of that two days tell them they can't come out of the room until they agree on some core principles and functional structures for how to do it, for how to resolve this. I actually think it could work. You can't put them all in one room at one time because you might have some homicides on your hands but you could potentially do it in four or five clusters. (P/P **J**)

I think [the way to] to resolve that is to ensure that there is collaboration in the development of these types of legislations and policies…. (P/P **K**)

These are big debates that have to happen. Big and important debates, and they have to happen in an open environment. (P/P **L**)

One research participant pointed out that in any such debate, the views of groups with different experiences (such as young people) should not be ignored:

[Young people] tend to use technologies more often and in different ways. [They should be involved in the creation of any policy in this area. They should be given some special consideration. (P/P **M**)

One research participant made the point that 'stakeholders' should not have privileged access to the debate:

> Stakeholders worry me. … [O]ne of my positions is that this is all equally everyone's concern. I don't acknowledge that there are specialties or special responsibilities that privilege anyone's views. The only privilege that should be given to views is on the merits. That is knowledgeable and thoughtful and that can come from inside or outside so-called specialists. (P/P **N**)

Two research participants identified practical challenges in facilitating such a conversation:

> [W]e've been talking at crossed purposes and we've been talking across people, across each other. We don't resile from what our role is and what we need to do our role. We'll live by … the way the rules are set but we'll play hard and similarly they don't agree fundamentally with what we do. I don't know whether it's an issue about explaining to them the actual nature of the risk or the threats that we're dealing with that how valuable particular sorts of information can be and why it actually justifies the derogation of a privacy right or whatever it is that they're concerned about. Because when you come to policy debates or legislative debates in the media and in the parliament there's too much pressure around time, there's too much pressure around sensationalism and sort of drama that you can't actually have a decent conversation. The confidentiality around cabinet processes and things like that is an impediment to that as well, so it's hard. (O-P/O **O**)

> I'm just not funded for that conversation. If you want to change the entire public paradigm around surveillance and privacy, this is going to be a $100 million endeavour to do that. … [T]here's a big conversation to do - this is a massive task. (P/P **P**, in response to a different question)

Finding the middle ground (see Lens 5.1.2). Four research participants believed that there was a middle ground that could be found and that the debate needed to shift from one of polarising views to identifying a middle path.

> [T]he debate tends to get stifled because the issues are polarised. …[T]hey become binary. The nature of the debate in the public unfortunately tends to get drawn to either of those poles. But I would characterise my views on this as sitting right in the middle of both those poles. I know how intrusive these powers can be and therefore I know that they need to be managed capably by our government. The thing that frustrates me is that polarisation. … [T]he views expressed in the mainstream media tend to be polarised. But when you read some of the comments to news articles … you see that there can be a lot of balance there. That people who have absolutely no experience whatsoever in law enforcement or intelligence can actually understand the need to do this. But by the same token they show a mature degree of concern that the oversight is there. (O-P/O **Q**)

However, there were of course differences on the appropriate balance. For example, while one research participant favoured stronger data protection laws, another identified the 'silent majority' as preferring greater law enforcement access to data, while a third was concerned that sometimes bad trade-offs were made in an attempt to satisfy diverse interests.

> I think that more robust accountability and oversight mechanisms around the use of data, not even just Big Data, by Law Enforcement would get some of the sceptics more on board or be something of a compromise with people who are more sceptical about it. … [P]erhaps more robust data protection laws with more robust enforcement as well. (P/P **R**)

> [T]he single interest groups have got the loudest voice in this argument sometimes. The silent majority out there would be more than happy I think for the law enforcement agencies to have access to our information. (O/P **S**)

> You've got to come up with some sort of balance … . Resolving conflict is something that you have to do … on a case by case basis every time you try and do anything at all …. So for data retention, this is a new capability for the agencies which is great. But to keep the public happy, a whole bunch of agencies [are] having their access to data cut so that the pool of agencies that can access is being narrowed, which is a privacy boon for the public people who think this is good. But it might not be because suddenly some agency – like the RSPCA's access to data has been taken away currently. … If someone tortures a koala, the RSPCA investigates this because they're the people who can assess whether a dog has been tortured or not. So … I kind of want koala torturers to go to gaol. I think these are bad people and they should be investigated, prosected and sent to gaol. But … well, the public thinks that data access should be narrower so koalas are going to get tortured. This is an awkward balance. The industry is having $128.4 million thrown at them from an appropriation to grease the wheels on building this capability. So this is a lot of money that is going out of the public's purse into the pockets of industry just to make them complain less about a thing. So there's a huge amount of giving and taking going to find the balance that gets data retention through the parliament. So there's people taking wins and losses here to come up with something. Certainly the dataset inside data retention is not the dataset that the agencies would have wanted. It doesn't include a whole bunch of that rich data that they'd like to have in their dataset because you can't include location at all times in a data retention dataset because the public are going to say no, this is just live tracking of every person in Australia. This is unacceptable, which - fair enough. So - and this is how you end up with this noisy landscape we were talking about because every time you want to do something you've got to balance the interests of all these stakeholders that are conflicting and that balance falls in a slightly different place each time. Then you end up with a landscape that's just a massive mess. (P/P **T**)

One research participant expressed the view that the argument should be won rather than compromised.

There's no compromise. One should take no step towards people who want to take the benefits of organised society without contributing to it. You can't compromise with them. … I would deprecate taking a compromise approach, that is saying that these are differences of view that lend themselves to a compromise. No, I think one or other needs to prevail. … The way to live with different political views is not to have some Pollyanna view that we should all somehow sing Kumbaya and agree, I'll give up part of my view if you give up part of your view. No, no, no, just be happy, go to lunch with each other, you don't kill each other about it, you have different views. If they lend themselves to electoral politics, you will vote differently every three or four years. That's fine. That's how you reconcile it … These are not matters of mere expediency. There are values, serious values that lie not so far underneath the surface. Many of them are well and truly above the surface of these controversies. Value differences don't lend themselves - except when somebody changes their mind, which people do, by the way - they don't lend themselves, it seems to me, to compromise without sacrificing what's important and why we call them values. They're not just preferences. … I think that's why we have argument. (P/P **U**)

Enhancing trust (see Lens 5.1.5). The importance of enhancing public trust in relevant agencies was identified as crucial by two research participants.

> The PEW Centre in the US showed that people will share your information if there is trust in your organisation – if people don't trust you they don't provide accurate information (P/P **V**).

> It really is that trust. It's a big trust – it's offering a lot to law enforcement, offering a lot of trust to a government institution … That's … got to be done carefully and for a really good solid authentic reason that the community can … understand and back. (P/P **W**)

Summary and implications

Any conflict in values is unlikely to be fully resolved, particularly as it relates to underlying differences in attitudes towards privacy. However, research participants 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.

2.6.7. Source of views

Having asked research participants with policy roles (and one T/O with an interest in policy) about their views on various issues, as elaborated in this section, we asked them to identify the sources of the views, in particular the extent to which they were shaped by internal or personal experience as opposed to external sources (such as blogs, watch groups and media) [P20].

As Table 2-20 indicates, the most common sources of views were professional (11) and personal (6) experience. A few respondents identified other sources, such as contact with people who have lived under surveillance overseas, media and blogs as well as evidence and academic sources.

Table 2-20: Sources of views of Policy group

	Private/ Research/ NGO	**Independent**	**Government**	**Total**
Professional experience, knowledge	**3** (1 P/T)	**4** (1 O-P/O)	**4** (2 O-P/O)	**11**
Personal experience	**4**	**1**	**2** (1 O-P/O)	**7**
Contact with people who have lived under surveillance overseas	**2**			**2**
Media/blogs	**1**	**1**		**2**
Evidence / Academic papers		**1**	**1** (T/O)	**2**

* Multiple responses can be coded for each research participant. All are P/P except where specified.

Six research participants (including those who were not asked this question directly) expressed particular scepticism towards the media and blogs as a source of information, believing such sources to be unreliable and inaccurate:

> As far as media and the blogosphere and all that goes, I'm a sceptic. I think invariably people that get on there, while they may have some valid points at times, it's personal motivations for a position they take. Until you understand those I think you have to be a bit wary of what's being said. I'm a very factual person so I try and take the emotion out of it and just focus on what outcomes can be delivered. (P/T **A**)

> The general population take their lead on what they see on the TV. It's not the informed view that they have. (T/O **B**)

> I guess I haven't seen particularly constructive contributions on issues - not specific Big Data but similar sorts of issues from those sources … They may well be there but I just haven't seen them. (O-P/O **C**)

> [My views are] very influenced by what I know because I know more than what the bloggers that write know. (O-P/O **D**)

> The things that I say to people often end up in the media. So someone from industry or someone from a special interest group will come and say [name], what's the answer to this question? I will answer the question and this will get forwarded to some media person and then published as the views of [my agency], a comment by government or the views of the agency that I gave the information to. So … the end result [is] the article that's published in [particular media source] is just an embarrassingly different thing from the actual truth. The quality and accuracy of the media in this space is just so partisan it's ridiculous. … I'd be concerned about anyone who was [influenced by the media] because they're being influenced by something that is not the truth of the matter. So I think that this is one of these problems with the public discourse … [T]his is the kind of … indescribable nonsense that you read when you try and learn about these matters. So it would just be impossible for a member of the public going into the public sources on these kinds of conversations to walk away with a useful view because you've got just incomprehensibly wrong things coming out of people like [particular journalists] … [I]t's unfair to a member of the public relying on external sources to form a fair view. There's just - you have no chance. (P/P **E**)

> We can see through it whereas other people don't see through it. (P/P **F**)

Summary and implications

Research participants 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. The 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.

3. BIG DATA, LAW ENFORCEMENT AND NATIONAL SECURITY: THE LEGAL ENVIRONMENT IN AUSTRALIA

This chapter discusses features of the Australian legal framework relevant to Big Data, law enforcement and national security.

The chapter is divided into eight sections that reflect the lines of inquiry introduced in Chapter 5 of the *Methodology Report*, generally referred to as the 'lens' in this discussion. The sections therefore address aspects of the regulatory framework relating to the following questions:

1. Is access for data mining enabled?
2. Are legal controls comprehensive and proportional?
3. Are legal rules clear, principle-based, consistent and instructive?
4. Is integrity of data and analysis supported?
5. Are data and systems protected?
6. Is accountability maintained?
7. Are principles and rules regularly reviewed?
8. Is there a sufficient measure of transparency?

While the 'lens' is used to structure this discussion, it is important to emphasise that it is only used to inform the lines of inquiry, and not as a tool to assess the current framework. It is used to focus the inquiry on key elements which, if collectively present, would be indicative of a framework that:

- supports the effective use of advanced analytics and large data sets for law enforcement and national security purposes,
- while respecting the rights and interests of all stakeholders (including data subjects and the broader community and economy);
- reflects proportionality and evidence-based justification and decision-taking; and
- ensures comprehensive identification and management of risk and opportunities.

The indicators are not presented as a comprehensive or final list. While they provide structure to the analysis it is not meant to restrict the broader inquiry or the ongoing debate about an appropriate framework.

The legal environment regarding data is highly complex and detailed. The objective of this chapter is not to capture the detail or to comprehensively map access rules and exchange mechanisms but rather to trace the broader features and contours of the framework that are of particular relevance to this study.

The study focuses on information that is publicly available. It is clear that many aspects relevant to this investigation are set out in internal policies and procedures as well as confidential agreements. As the study is concerned with an appropriate public law framework that balances public and private interests, it is confined to sources that the public can access, assess and debate.

This chapter refers to quotations of interviewees in Chapter 2. Each quotation in that chapter is assigned a letter (in bold). So, for example, 2.6.1E refers to the quotation marked "E" in section 2.6.1 of the report.

The study reflects the law as at 31 March 2016, except where important developments necessitated minor updates.

3.1. Is access for data mining enabled?

The first line of inquiry addresses collection, use and disclosure of data, subject to the governance and control mechanisms set out in 3.2–3.8 below, for purposes of analysis using

Big Data techniques. It considers whether the framework enables access, subject to those mechanisms, 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.

The discussion in this section considers the parameters for this type of access, while the discussion in 3.2, addressing controls that are imposed on access, use and other dealings with data, considers features of the legal nature of some of the controls, and the degree to which these require the question of proportionality to be taken fully into account.

In Australia information has been traditionally available for law enforcement purposes on the strength of warrants, such as specific-purpose search and seizure warrants, or orders setting out particulars of the information, location, time, circumstances and things (including electronic devices) that were allowed to be seized and accessed.[78] The principles are reflected in legislation, rules of court and procedure for such orders. Big Data tools, on the other hand, are accompanied by new approaches to access to data, with a technological preference for as direct access as possible to as many, and as large, data sets as possible,[79] and a tendency to deprecate traditional restricted, purpose-specific data stores as unnecessary 'silos' preventing information flows.[80] Such access to data may be through system-level or similar direct access[81] to distributed data sources, or to a single, combined data holding. Statutory models governing this type of access can be different from models based on prior articulation and oversight of the specific purpose and scope of particular access requests. The statutory landscape of access rules are therefore reviewed with needs such as these in mind.

This discussion now focuses briefly on access to each of the four types of data holdings noted above:

- government-held data,
- 'open source' data,
- privately held data, and
- data held by foreign governments.

3.1.1. Access to government-held data

'Government-held data' refers to information stored by all levels of government (federal, state and local) in data systems.

---

[78] For instance, see s 62 *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW). A warrant has to contain the information set out in ss (1)–(2A) including the nature of the searchable offence, and the issuer has to consider the factors in ss (3), and for covert searches (4), including necessity, relevance to the offence, reliability of the information, and impact on the privacy of those not believed to be knowingly concerned in the commission of the searchable offence. For a specific example, see the *Protocol* and *Guidelines* for the execution of search warrants on barrister's chambers, Bar Association of NSW and NSW Police Force, 21 January 2013 <http://www.police.nsw.gov.au/__data/assets/file/0009/254619/Guidlines_for_Execution_of_Search_Warrants_on_Barristers_Chambers.pdf>.

[79] See for example Chapter 2, 2.2 on assumptions about desirability of more and bigger direct access].

[80] See for example Chapter 2, 2.4.1, 2.4.5 re silos.

[81] Concepts such as 'direct access', 'API (Application Programming Interface) level access', and 'system level queries' have been used to describe an approach which seeks to enable software-mediated queries over a data set rather than delivery of small sets of records output as a result of individual searches by operators.

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.[82]

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 authorised/permitted.

As a result, access to government-held data is governed by general exceptions and specific statutory or delegated authorisations, including those detailed in public and confidential Memoranda of Understanding,[83] as well as by other general mechanisms such as Rules or Guidelines issued by the Privacy Commissioner for particular scenarios. This means that access rules are located in a complex combination of statutes, guidelines and inter-agency agreements, some of which may not be public documents.

Three agencies with critical but different roles in relation to criminal intelligence were selected to serve as examples of data collection, use and arrangements:

- **AUSTRAC**, that collects financial transactional data that can be accessed by a range of bodies and agencies;
- **CrimTrac**, which provides a crucial information sharing mechanism for police services; and
- **Australian Crime Commission** (ACC), the national crime intelligence agency.

While CrimTrac and the ACC provide valuable agency perspectives they are also significant as the two key agencies that will merge to form a 'super' Australian crime intelligence and information agency, the Australian Criminal Intelligence Commission.[84]

AUSTRAC

The Australian Transaction Reports and Analysis Centre (AUSTRAC) was established under the *Financial Transaction Reports Act 1988*, amended and complemented by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), as a statutory authority within the Attorney-General's portfolio. Read jointly, the two laws structure AUSTRAC as a financial intelligence unit and as a regulator for anti-money laundering and counter terrorist financing (AML/CTF). AUSTRAC is bound by the *Privacy Act 1988*.

Receipt and analysis of data

AUSTRAC collects transactional data from approximately 14,000 regulated institutions. Regulated institutions have a range of statutory AML/CTF obligations including customer identification, record keeping, and customer monitoring. These institutions are required to

---

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

[83] 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.

[84] Minister for Justice, 'New Super Agency to Tackle Emerging Threats' (Media release, 5 November 2015); Minister for Justice, 'Australian Criminal Intelligence Commission to Combat Criminal and National Security Threats' (Media release, 7 May 2016).

report an array of reportable transactions to AUSTRAC, ranging from large cash transactions and cross-border electronic transactions to reports of unusual or suspicious matters. A significant number of reports are received, for example nearly 85 million international funds transfer instruction reports, more than 5 million threshold and significant cash transactions reports and more than 60,000 suspicious transaction and suspicious matter reports were filed in 2013/2015.[85]

AUSTRAC's Transaction Reports Analysis and Query (TRAQ) database receives, stores and analyses the reported data and related information. AUSTRAC can also request additional information and access data held by some other agencies. AUSTRAC, for example, has indirect access to information held by the AFP. This information may be entered manually as single records into TRAQ to be used for purposes of analysis.[86] AUSTRAC developed an automated monitoring system called TargIT to monitor the large volume of transactional data housed within its TRAQ system. TargIT is described as 'a rules based system that uses 'clauses' (financial profiles) to identify particular types of suspicious financial activity'.[87] AUSTRAC has been investing in significant upgrades to its intelligence data systems as part of its Enhanced Analytical Capability (EAC) project. AUSTRAC is currently in the process of replacing the TargIT system with its own *AUSTRAC Intelligence* (AI) system. This replacement process commenced in 2013-2014.[88]

Disclosure of data

Under its legislation, AUSTRAC may disclose data to four categories of recipient:

(1) the ATO,
(2) designated Australian agencies (below)
(3) government authorities other than the ATO and designated agencies, and
(4) foreign counterparts.[89]

Different rules regulate disclosure to the four groups. The ATO and its officials, for example, are entitled to access AUSTRAC data[90] while designated non-ATO agencies and their officials are not generally entitled to access AUSTRAC data. The AUSTRAC CEO may, however, authorise specified officials, or a specified class of officials, of a specified designated agency to have access to AUSTRAC information for agency purposes. The *AML/CTF Act* sets out a range of 'designated agencies' including:

- the national security agencies,
- AFP and state and territory law enforcement agencies,
- regulators such as Australian Prudential Regulation Authority and Clean Energy Regulator,

---

85 AUSTRAC, *Annual Report 2013–14* (October 2014) 32–3 <http://www.austrac.gov.au/austrac-annual-report-2013-14.

86 FATF, Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia – Mutual Evaluation Report Anti-money laundering and counter-terrorist financing measures: Australia – Mutual evaluation report (2015) [3.7].

87 ANAO, AUSTRAC's Administration of its Financial Intelligence Function Audit Report No.47 2012–13 [1.10]. See the ANAO discussion in 3.6 below.

88 AUSTRAC, *Annual Report 2013–14* (October 2014) 58 <http://www.austrac.gov.au/austrac-annual-report-2013-14.

89 AUSTRAC, *Communication of AUSTRAC information to a foreign country* <http://www.austrac.gov.au/about-us/policies/communication-austrac-information-foreign-country>.

90 S 125 Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

- independent oversight bodies such as Inspector General of Intelligence Services (IGIS), and
- integrity and anti-corruption bodies.[91]

Individual access by authorised officials to AUSTRAC data records is a common means of access. Access to bulk data is possible on request by an agency. This is discussed in greater detail below.

In 2014-2015, AUSTRAC trialled its new AI system with NSW Crime Commission, NSW Police and the ATO. AI system will be available to its other partner agencies upon signing a new Memorandum of Understanding (MOU). The MOUs will reflect the system's enhanced capability and include strengthened provisions regarding data access and usage.[92]

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions.[93] FATF reported as follows on agency access to AUSTRAC data:

> 'Authorised partner agencies' access the AUSTRAC database directly online through the TRAQ Enquiry System (TES) – based on MOUs concluded with each partner agency. The MOUs govern the number of personnel from each agency permitted to use TES and the level of access granted to each user. The 41 agencies include all major federal, State and Territory law enforcement bodies. In 2012/13, these agencies had a total of approximately 3,200 personnel with access to TES. All use of the AUSTRAC information can be audited for security reasons. In each of the previous five years, over 2 million manual searches (more than 7,000 each day of the year) have been conducted in the AUSTRAC database.

Other access is role-based (different agency staff with different levels of security or operational responsibility have differing levels of access to the AUSTRAC system). Some agencies, such as the AFP, have full online access to all data held by AUSTRAC. Other agencies, such as ATO, automatically receive copies of all Suspicious Matter Reports (SMRs) [3.12]. AUSTRAC also automatically forwards potential 'high risk' reports, such as some SMRs, to certain partner agencies within an hour of receipt, based on dynamic red flags that are set in coordination with each partner agency. Other flagged reports are made available within 24 hours. AUSTRAC refers and sends these SMRs to partner agencies based on the nature of the alleged offence, risk or other material fact.[94]

At 30 June 2015, 3,364 registered partner agency personnel had online access to TES. These users logged onto TES to access financial information on 197,360 occasions, 'conducting a total of 1,825,041 TES activities.'[95]

---

[91] S 5 Anti-Money Laundering and Counter-Terrorism Financing Act 2006 ('designated agency').
[92] AUSTRAC Annual Report 2014–2015 (2015) 44.
[93] The 'objectives of FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a 'policy-making body' which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas': 'About us,' FATF web site, 2015 <http://www.fatf-gafi.org/about/>. While FATF proposes benchmarks and assesses country compliance with them, these do not have the status of ISO standards and are not based on a treaty triggering national legislative obligations. FATF criteria do not appear to include proportionality factors.
[94] FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia – Mutual Evaluation Report* (2015) [3.11]–[3.12].
[95] AUSTRAC, *Annual Report 2014-–2015* (2015) 44.

AUSTRAC's policy document on sharing of bulk data with Australian agencies[96] notes that the AUSTRAC CEO will provide an ATO official with downloads of bulk AUSTRAC information upon written request. This is being done in line with the process outlined in the MOU between AUSTRAC and the ATO and subject to guidance regarding bulk access issued by AUSTRAC. Designated agencies, on the other hand, are subject to restrictions on the amount and type of AUSTRAC information they can access. Their access is generally regulated by the Act, read together with their respective written authorisations under section 126(1) of the Act as included and detailed in the MOU between AUSTRAC and the designated agency.

The AUSTRAC CEO considers written requests for bulk AUSTRAC information from an authorised officer of a designated agency on a case-by-case basis in accordance with the bulk access guidance issued by AUSTRAC.[97] A requesting designated agency must demonstrate a 'justifiable need' to access bulk data to fulfil its statutory purposes, and will also need to satisfy the AUSTRAC CEO regarding its measures to protect the integrity, security and privacy of the requested bulk AUSTRAC information, once received. The CEO may also impose conditions regarding the use, protection, recording, storage, disclosure and destruction of the bulk AUSTRAC information.[98]

In addition, AUSTRAC can assist an agency by matching data held by the agency with bulk AUSTRAC information and disclosing the results to the agency.[99]

AUSTRAC can also disclose data to federal non-designated agencies.[100] Section 129 of the *AML/CTF Act* empowers the AUSTRAC CEO to exercise discretion to authorise access to AUSTRAC information by officials from Commonwealth non-designated agencies. AUSTRAC is, however, not allowed to disclose information to non-designated State and Territory agencies.

Section 129 allows for an application for access to be made for the purposes of an investigation or proposed investigation of a possible breach of a law of the Commonwealth. Where access is allowed, the type or class of AUSTRAC information that may be accessed must be stated. This access is therefore tightly controlled. The Act also allows the ATO or a designated agency to share AUSTRAC information with a non-designated Commonwealth agency for the purpose of an investigation or proposed investigation.[101] However, they may not share information regarding Suspicious Matter Reports or Suspect Transaction Reports.

---

96 AUSTRAC, *Dissemination of bulk AUSTRAC information to the Australian Taxation Office and designated agencies* (2013) <http://www.austrac.gov.au/about-us/policies/dissemination-bulk-austrac-information-ato-and-designated-agencies>.
97 AUSTRAC, *Dissemination of bulk AUSTRAC information to the Australian Taxation Office and designated agencies* (2013) <http://www.austrac.gov.au/about-us/policies/dissemination-bulk-austrac-information-ato-and-designated-agencies>.
98 AUSTRAC, *Dissemination of bulk AUSTRAC information to the Australian Taxation Office and designated agencies* (2013) <http://www.austrac.gov.au/about-us/policies/dissemination-bulk-austrac-information-ato-and-designated-agencies>.
99 This process, referred to by AUSTRAC as 'Autosearching', is 'a process of matching names, addresses, account numbers or identification numbers contained within AUSTRAC information against similar information held by an authorised agency. AUSTRAC Autosearching output provides a detailed summary of the information held by AUSTRAC on each of the names, addresses, account numbers or identification numbers provided by the authorised user agency.' See AUSTRAC, *Generic program protocol – Autosearching* (January 2007) <http://www.austrac.gov.au/generic-program-protocol-autosearching>.
100 AUSTRAC, *Access to AUSTRAC information by non-designated Commonwealth agencies.*
101 S 128(8) of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

AUSTRAC also has MOUs in place with 79 foreign countries governing disclosure and exchange of information.[102] A policy on communication of information to a foreign country underpins such MOUs.[103] The terms of this policy appear to limit responses to requests for personal information so as to generally exclude disclosure of 'personal information relating to a third party incidental to the request', and thus supports a relevant-record based approach rather than a bulk access approach.

AUSTRAC, which is subject to the *Privacy Act 1988* also maintains a Privacy Consultative Committee. This committee is tasked with advising the AUSTRAC CEO on privacy, civil liberties and freedom of information matters. The committee comprises representatives of privacy, civil liberties and consumer groups, as well as representatives from AUSTRAC partner agencies and the office of the Australian Information Commissioner.

CrimTrac

CrimTrac is the national information sharing service for Australia's police, law enforcement and national security agencies. It was established in 2000 by means of an Inter-Governmental Agreement signed by the Australian Federal Government and State and Territory Police Ministers.[104] CrimTrac is an Executive Agency within the Commonwealth Attorney-General's portfolio.

CrimTrac is responsible for developing and maintaining national information-sharing services between state, territory and federal law enforcement agencies. CrimTrac's services and capabilities include:[105] 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 operates databases such as the following:

- National Automated Fingerprint Identification System;
- National Criminal Investigation DNA Database;
- National Child Offender System;
- National Police Reference System;
- National Police Checking Service; and
- National Firearm Licence and Registration System.

CrimTrac has been expanding with the addition of services such as a missing person and victim system, and an online cybercrime reporting network.

CrimTrac is bound by the *Privacy Act 1988*.[106] CrimTrac does not generally collect personal information directly from individuals, except for purposes such as National Police Checking

---

[102] AUSTRAC, *Exchange Instruments List*, AUSTRAC web site <http://www.austrac.gov.au/about-us/international-engagement/exchange-instruments-list>. The countries include the 5 Eyes, much of Europe, and other countries as diverse as Russia, Bahrain and Egypt.

[103] AUSTRAC, *Communication of AUSTRAC information to a foreign country*, AUSTRAC web site, undated <http://www.austrac.gov.au/files/austrac_info_to_foreign_gov_policy.pdf>.

[104] 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.

[105] CrimTrac, Annual Report 2013–2014 11.

[106] CrimTrac, Privacy policy, CrimTrac web site <https://www.crimtrac.gov.au/privacy>.

Service (NPCS) reports,[107] and internal administrative functions, including its own human resource functions. 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 via CrimTrac, the minimum set of data they will provide, and who is authorised to access or receive the data.[108] Police agencies either input information directly into CrimTrac systems, or upload it through automated system uploads.

Access to CrimTrac systems is restricted to authorised officials, such as police officers, who may access them for authorised purposes. CrimTrac facilitates 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.

In 2014, the National Commission of Audit recommended that CrimTrac be merged into the Australian Crime Commission to better harness their collective resources.[109] On 5 November 2015, the Minister for Justice announced that an agreement that will give effect to a merger was reached between CrimTrac and the Australian Crime Commission.[110] ACC is also in the process of merging with the Australian Institute of Criminology.[111] 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.[112]

Australian Crime Commission (ACC)

The Australian Crime Commission (ACC), Australia's national criminal intelligence agency, was established under the *Australian Crime Commission Act of 2002 (Cth)*.[113] 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,

---

[107] 3.7m reports were produced in 2013–2014, requiring individuals to provide consent and personal information to CrimTrac. CrimTrac, *National police checks* <https://www.crimtrac.gov.au/national-police-checks>.
[108] CrimTrac, Information Publication Scheme, CrimTrac web site <https://www.crimtrac.gov.au/information-publication-scheme>.
[109] National Commission of Audit *Towards Responsible Government The Report of the National Commission of Audit – Phase One* (2014) Recommendation 52; David Connery 'Investing wisely Spending political capital on Australia's criminal intelligence capabilities' Special Report, Australian Strategic Policy Institute (August 2014).
[110] Minister for Justice, 'New Super Agency to Tackle Emerging Threats' (Media release, 5 November 2015).
[111] 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.
[112] 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).
[113] S 7A(a) Australian Crime Commission Act 2002 (Cth) ('ACC Act').

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.[114]

Unlike AUSTRAC and CrimTrac, the ACC is not bound by the *Privacy Act 1988* and nor does it have its own set of forma privacy principles.[115] This exemption appears to have been based on special powers of the National Crime Authority (NCA), one of the bodies it replaced.[116] NCA's coercive powers were 'unique to Commonwealth law enforcement, which allowed the collection of personal information of a speculative and untested nature.'[117] However much of the information held by the merged ACC came – and still comes – from agencies such as the AFP, AUSTRAC, ASIC that are covered by the *Privacy Act*. This information appears to be exempt when in ACC hands, or in records originating from or received from ACC by other bodies subject to the *Privacy Act*.[118] The Law Council of Australia in 2012 reported advice from the Attorney General's Department that 'ACC voluntarily complies with the [then] Information Privacy Principles under the *Privacy Act* as far as possible,' but maintained its view that the Government should develop information handling guidelines for the ACC, as recommended by the ALRC in 2008 as an alternative to bringing the ACC under the *Privacy Act*.[119]

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.[120] The Parliamentary Joint Committee on Law Enforcement noted that:

---

[114] *Australian Crime Commission Act 2002* (Cth) s 59AA.
[115] See *Privacy Act 1988* (Cth) s 7(1)(a)(iv). Although ACC is an 'agency' under the Privacy Act, its acts and practices are excluded from the reference to 'an act or practice' in the Act. With the exemption from the TFN provisions in s 7(2), ACC is completely exempt from the operation of the Act.
[116] The other bodies were the Australian Bureau of Criminal Intelligence (ABCI) and Office of Strategic Crime Assessments (OSCA).
[117] Office of the Privacy Commissioner, Submission to ALRC 108, PR 215, 28 February 2007, cited in *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) 2008 [37.25]. The ACC's special coercive powers, which can only be exercised by an ACC examiner in the context of a special operation or investigation approved by the ACC Board, include the capacity to compel a person to produce documents, to attend an examination and to answer questions.
[118] See *Privacy Act 1988* (Cth) s 7(1)(h).
[119] LCA, Inquiry into the gathering and use of criminal intelligence, submission to Parliamentary Joint Committee on Law Enforcement, 1 August 2012 [68]. See *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) 2008 recommendation 37–1.
[120] 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 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

> Fusion co-locates investigators, analysts and technical experts to maximise the use of public and private sector data and facilitate real-time intelligence sharing and analysis. Fusion brings together capabilities from Commonwealth agencies including the AFP, Department of Immigration and Citizenship, ASIC, AUSTRAC, ATO, Department of Human Services, ACBPS, the national intelligence community and state and territory law enforcement authorities. It collects and receives intelligence from the Australian Intelligence Community (AIC) and other stakeholders including Commonwealth law enforcement, regulatory and policy agencies, state/territory police agencies and crime commissions, foreign law enforcement agencies supported by the AFP and private sector organisations.[121]

According to the government the National Criminal Intelligence Fusion Capability could be classified as an 'intelligence generating system'.[122]

> It provides technical analytical tools combined with a diverse and ongoing feed of bulk data and targeted new information, as well as secondees from participating agencies (currently 19 partners) and agreements to share data. This enables the ACC to compile and analyse large volumes of information and intelligence from multiple sources, which generates new insights (via monitoring and discovery activity) into serious and organised crime. Palantir is a core analytical tool provided by Fusion for ACC analysts to analyse information and generate intelligence. Fusion also provides the ACC a gateway to interface with international partner networks and forums. It should be remembered however that ultimately a human element is always required to evaluate, assess and make judgements and recommendations in relation to the information and intelligence.

The ACC maintains the Australian Criminal Intelligence Database (ACID) that includes ACC intelligence as well as intelligence uploaded by its partners. ACID is accessed by 24 Commonwealth, state and territory law enforcement agencies and other regulatory authorities. ACID provides the ability to securely share, collate and analyse criminal information and intelligence.[123]

The ACC also manages the Australian Law Enforcement Intelligence Network (ALEIN). This is a secure extranet that enables partners to access ACID and other data holdings of the ACC.

The ACID framework is 30 years old and the ACC is in the process of replacing ACID and ALEIN with the National Criminal Intelligence System (NCIS). NCIS will be a federated national law enforcement capability, which will facilitate real-time collaboration and intelligence sharing.[124] It will operate within a framework of common principles and standards, aligned to the Australian Criminal Intelligence Model (ACIM) developed by the

---

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.'

121 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the gathering and use of criminal intelligence* (2013) [4.80} <http://www.aph.gov.au/~/media/wopapub/senate/committee/le_ctte/completed_inquiries/2010-13/criminal_intelligence/report/report.ashx>

122 Senate Standing Committee on Legal and Constitutional Affairs Hearing, *Australian Crime Commission* (Question No. 86 by Senator Brandis, 12 February 2013). The answer continued: 'The ACC also generates intelligence through: coercive powers, cyber intelligence capabilities, covert human source capabilities,
research and analysis capabilities (open source and specialised information sources), traditional investigations, surveillance and telephone interception activities, (and) joint taskforces, joint operations and joint forums. ACC intelligence is therefore both generated internally and through joint activities with state and territory police and Commonwealth law enforcement partners.'

123 Australian Crime Commission *Annual Report 2013–14 (*2014) 94.

124 Australian Crime Commission *Annual Report 2013–14 (*2014) 95.

ACC and partner bodies and agencies.[125] ACIM is a model that aims to minimise the restrictions on flow of intelligence across the policing, law enforcement, law compliance and national security environments.[126]

The Parliamentary Joint Committee on Law Enforcement considered some of the key challenges to establishing the ACIM and published a report in 2013 with recommendations to improve the collection and use of criminal intelligence.[127] Importantly the committee supported the ACIM and endorsed efforts underway to develop it.

'Silos' and controls on access

AUSTRAC and the ACC have their own governing legislation, which largely determines how information can be collected, used and disclosed to partner agencies. AUSTRAC and CrimTrac are subject to the *Privacy Act*, which operates alongside any specific legal or contractual arrangements in the case of personal information. Each of the three agencies therefore has an own set of applicable disclosure rules regulating the disclosure of data to their own sets of partner agencies. The Parliamentary Joint Committee on Law Enforcement captured it as follows in the 2013 report on the gathering on use of criminal intelligence:[128]

> 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.

The most prevalent form of 'data sharing' is providing individual officials with the ability to browse for particular information held in another agency. Little information is publicly available on bulk sharing by the ACC and as facilitated by CrimTrac. Only AUSTRAC has a public policy on bulk data sharing.[129] Also, not much information is available on data matching done by CrimTrac and the ACC. CrimTrac holds DNA and fingerprint data for data matching purposes but AUSTRAC is the only agency of the three that has a public policy on its bulk data matching services, called 'auto-searching'.[130]

The discussion thus far has touched briefly on the framework of information sharing between government agencies. It is important to bear in mind that different officers of an agency are generally entitled to different levels of access to shared information. This is the basis of the security and auditing functions discussed below in topics 3.5 and 3.6. The Australian Government Security Classification System provides guidance regarding the

---

125 Australian Criminal Intelligence Management Strategy 2012–15. The partner bodies include the AFP, ASIO, ATO, CrimTrac and State and Territory police forces.

126 Australian Criminal Intelligence Management Strategy 2012–15. Strategic Objective 6 of the ACIM includes the identification and resolution (where possible) 'of legal and policy impediments to the dissemination of intelligence when using technical and security architectures.'

127 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the gathering and use of criminal intelligence* (2013).

128 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the gathering and use of criminal intelligence* (2013) [4.10].

129 AUSTRAC Dissemination of bulk AUSTRAC information to the Australian Taxation Office and designated agencies (2013).

130 AUSTRAC Generic program protocol – Autosearching (January 2007).

grading of confidentiality requirements of official information, and how levels of access are set.[131]

The Australian government is concerned about the current data access challenges and various steps have been taken to address them.[132] The formation of the Australian Criminal Intelligence Commission should be viewed in that light.

3.1.2. Access to 'open source' or publicly accessible data

Access to 'open source' data offers the potential to collect and analyse information relating to a very large number of people, often with apparently few controls other than those found in contractual agreements or where privacy legislation applies. Access to most 'open source' data may be on an individual, specific search or streaming feed basis, which may complicate its application for Big Data purposes.[133] This may apply to both public and non-'public' parts of the data, particularly where it is held off-shore. It should be noted that there is an absence of clear legal guidelines in this area and one could reasonably expect to see test cases emerging around the collection, use and disclosure of such data in relevant jurisdictions, including UK and Europe. Under the *Privacy Act*, if information is collected for inclusion in a record, government agencies may need to comply with APP 3 in relation to collection and APP 6 in relation to use and disclosure. In addition to the basic requirement that agencies only solicit and collect personal information that is reasonably necessary for or directly related to one or more of their functions and activities, the collection of sensitive information requires the individual's consent unless an exception is available. Obligations to collect by fair means (APP 3.5) and only collecting from the individual concerned (unless an exception applies) are likely to be relevant in the national security and law enforcement context. Use of data once collected, as well as retention and archiving requirements, were also issues raised by research participants (see 2.5.4 'Online data as evidence').

'Open source' data includes:

- Data held in open-access online databases, publications and directories like the Australian Business Name lookup,[134] a source of both personal information, to the extent it is held in such sources, and of a much broader range of other information, such as informal commercial transactions on eBay.
- Communications such as the voluminous streams from messaging services like Twitter, or the posts and links on social media services like Facebook which have been posted or uploaded with limited, ambiguous or no access restrictions.[135]

---

[131] Australian Government Australian Government information security management guidelines – Australian Government security classification system (2014, as revised in 2015).
[132] See for example the steps discussed in The Parliamentary Joint Committee on Law Enforcement *Inquiry into the gathering and use of criminal intelligence* (2013) par 3.22–3.31.
[133] Streaming, although potentially a high 'velocity' source, only lets one sip from the 'hose' of new data accumulate it, but not search the 'lake' of existing data. So it does offer some Big Data features.
[134] See <http://abr.business.gov.au/>.
[135] 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,

This data may be held in public hands, particularly where government data sets are released as 'open data'; or in private hands, particularly social media. In most cases not all of a service's data is 'open'. The unrestricted or 'open' part is typically accessible to everyone by online search, or by subscription to streaming 'feeds'. Over time and with automated tools, this may enable collection of or access to substantial volumes of data.

There is often additional data accessible only to a sub-set of users under restricted access technical controls. This would not be considered 'open source'.

Direct system-level access to their data store is also typically not openly available. Some services experiment with more direct forms of access, for instance, the Twitter 'fire hose'.[136]

There do not appear to be any statutory rules regulating access to 'open source' information by federal or state law enforcement or national security intelligence agencies.[137] In the absence of such provisions it appears such 'open' data can be accessed, collected, used and disclosed.[138] Further, government agencies may acquire information via private sector data brokers rather than through direct access to the 'open source'.

The absence of statutory rules regulating access does not, however, imply that agencies enjoy unrestricted or unlimited access. Access to the repository at system level, or 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. The fact that social media data centres are typically out of the jurisdiction would be a challenge for agencies where they seek access to data not openly available to the public.[139]

Copenhagen, June 2015; <http://www.pearlsinpolicing.com/wp-content/uploads/2014/07/Pearls-in-Policing-2015.pdf>.

136 Twitter appears to be one of the few services willing to enable bulk access to a stream of its public messages for third parties on a commercial basis. This has been wound back recently. Presumably this would exclude, without further arrangements, inter-personal communications not directed to the public stream.

137 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.

138 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>. Other agencies have been interested in social media for this purpose, including through the international Pearls in Policing forum. Pearls in Policing is a Dutch-inspired international think tank conference on policing issues. Andrew Scipione (NSW Police Force Commissioner), 'Challenges and opportunities for policing of social media', presentation, Pearls in Policing 2010. See also David Vaile, 'Social networking challenges for policing', presentation, Pearls In Policing, Brisbane, 2011; and the diagram of the potential for 'Big Brother policing' in a 'soft policing' mode in the Working Group 2 presentation the 2015 event in Denmark <http://www.pearlsinpolicing.com/wp-content/uploads/2014/07/Presentaties-pearls2015.zip>.

139 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; 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

The Victorian Commissioner for Law Enforcement Data Security in 2013 noted difficulties in getting access to social media information located offshore (presumably the non-public aspects, or system level access).[140] Their office has to go through Mutual Assistance treaties, and via the Commonwealth to the relevant federal agency in that country, e.g. FBI, where data is held in the US.[141]

This challenge is evident in the statement of one research participant that it takes '6 or even 18 months for getting an authorised record from Facebook that is admissible in court'.[142]

Encryption is also posing an increasing challenge for agencies. Major US communications service providers like Apple are responding to changing perceptions about the boundaries between public and private, implementing strong encryption measures to deter system level access to the latter.[143]

Why 'open data' may be sensitive

Some publicly accessible material may be sensitive. It is unclear the degree to which users of particular services are aware of increasingly ambitious law enforcement and intelligence collection of their data, or the implications of communications intended for their intimate circle or family being available for such collection.

It is also unclear whether any of the users of the dominant social network Facebook are aware of the implications of its repeated downgrading of default privacy settings that increase 'public' access to their social media data, which they may have intended to be private or for an intimate circle.[144] The result is that data uploaded into what was, or was

---

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).

[140] Also, where social media data is used as evidence (which is largely out of scope for this report), it needs to be verified by the provider in some circumstances. One research participant raised this as another circumstance in which they had to go the long route, even though data was publicly accessible (7.2.3).

[141] See 4.3.3 in 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>. See also See also *Commonwealth Mutual Assistance in Criminal Matters (United States of America) Regulations 1999*.

[142] See 2.2.3.

[143] See for example Tim Cook, CEO of Apple, on encryption. Matthew Panzarino, 'Apple's Tim Cook Delivers Blistering Speech on Encryption, Privacy,' *TechCrunch* (online) 2 June 2015 <http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/>. Mr Cook made further comments in a letter to customers February 2016 in respect of an FBI request to assist it in sidestepping iPhone encryption. 'A message to our customers', Apple Computer, 16 February 2016 < http://www.apple.com/customer-letter/

[144] See Matt McKeon, 'The Evolution of Privacy on Facebook', web page, 2010 <http://mattmckeon.com/facebook-privacy/>. Eleven parameters of access control show all defaults repeatedly made less protective over 2005–2010. Data uploaded into a private, non-'open' zone is later exposed to increasingly wide access without user input. This has continued since 2010. Snapchat promoted 'disappearing' photo messages that can't be viewed once opened promising 'delete is our default', but now exposes data for commercial exploitation. Sally French, 'Snapchat's new "scary"

thought to be, a private, non-'open' zone may be later exposed to increasingly wide access without user input. It may appear as if it was intended to be 'open' by the external observer, unless they have tracked this gradual degradation of default security controls.

There have also recently been proposals to harvest photographs from Facebook for law enforcement biometric purposes.[145] Photographs contain personal information, typically of individuals other than those who have taken the image or posted it. Facebook has shown little interest in encouraging caution about the potential consequences of, or seeking permission from the subjects for, uploading such images.[146] A biometric harvesting exercise would potentially use information and images that may not have been disclosed in contemplation of conversion to a biometric, or with a full appreciation of the inherent sensitivity and risks of such functionality applied to one's family and friends without their knowledge or consent.

A lack of knowledge about the operation, instability and implications of the complex access controls may undermine arguments that data subjects or users gave informed consent to or 'reasonably expected' such disclosure.[147]

---

privacy policy has left users outraged,' *MarketWatch*, 29 October 2015 <http://www.marketwatch.com/story/snapchats-new-scary-privacy-policy-has-left-users-outraged-2015-10-29>.

[145] Shalailah Medhora, 'Facebook photos could be taken for use in national biometric database – officials,' *The Guardian* (online), 21 October 2015 <http://www.theguardian.com/australia-news/2015/oct/21/facebook-photos-could-be-taken-for-use-in-national-biometric-database-officials>. This highlights a conflict between different models of 'security', either supporting the security of personal information (by warnings about global publication of photographs which could be used for biometric harvesting by any sophisticated entity), or exploiting public ignorance and a weak security stance (encouraged by Facebook) to harvest such data. Facebook is respondent in a class action under the *Illinois Biometrics Information Privacy Act* for failure to get written consent for its harvesting of photo imagery for biometrics: Cale Weissman, 'Facebook is being sued for amassing the largest facial recognition data stash in the world,' *Business Insider*, 7 April 2015 <http://www.businessinsider.com.au/facebook-biometric-program-2015-4>.

[146] For instance, Facebook privacy page <https://www.facebook.com/about/privacy/> notes that others may 'share' information about you to third parties, but does not alert to your role as a publisher of information about others or raise the issue of consent or the subject's wishes, and suggests only an after the fact take-down reporting pathway rather than a 'prior informed consent' approach.

[147] *Privacy Act 1988* s 16 excludes application of the APPs to dealings with personal information by an individual for the sole 'purpose of, or in connection with, his or her personal, family or household affairs,' but while this may exempt an individual's use of Facebook for such purposes, the operator who collects and discloses the personal information of the user and others on a user's behalf does not benefit from this exemption. Where the APPs apply, APP 6.1(a) disclosure permitted on the basis of 'consent' may not apply to disclosure of information about others, who have typically not been asked for permission); this would also apply to APP 6.2(a) as the 'reasonable expectation' is that of the poster, not of a third party whose information is posted. Inadequate understanding of the ambiguous access controls may also cast doubt on the degree to which APP 6.1(a) consent is properly informed. Note that APP 6.2(e) would apply to permit disclosure to agencies where 'reasonably necessary' for many law enforcement purposes, but only where the operator is disclosing directly to agencies for this purpose; it would not cover publication on the generic interface.

3.1.3. Access to privately-held data

A significant source of data for government agencies is data held by private corporations. There are many different types of data sets in this category. We consider two examples in this study: financial data and telecommunications data.

Financial data includes financial data held by financial institutions, relevant for tax enforcement as well as anti-money laundering and combating of terrorist financing purposes. (Aspects of access to financial data were discussed earlier in relation to AUSTRAC.)

Telecommunications data is also held or dealt with by private carriers, carriages service providers or other telecommunications intermediaries. The importance of telecommunications data is highlighted in the policy debates around the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth).

Telecommunications information

Telecommunications data (both 'traffic' and 'content') has long been accessible for law enforcement and national security purposes. Traditionally, either a warrant or court order was required for a law enforcement agency to access such data.

Types of telecommunications data of interest include:

- Digital telecommunications content[148]
- Digital telecommunications traffic or metadata[149]
- 'Over the Top' (OTT) application content[150]
- 'Over the top' application traffic or metadata[151]
- Traditional wired, microwave, optical and radiofrequency communications channels[152]

Such data may be held in private databases or stores, whether in Australia or in other jurisdictions, and on devices.[153]

---

[148] This includes the audio of telephone calls, the text of SMS messages and perhaps of email messages.

[149] These are of increasing interest, as communication channels move from those built in at the CSP level like traditional telephony and SMS to those integrated into 'apps' which communicate by TCP/IP channels in the ISO application layer.

[150] See Jaan Murphy and M Biddington, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015*, Bills Digest, 89, 2014–15, Parliamentary Library, Canberra, 26 March 2015 <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A"legislation%2Fbillsdgs%2F3733407">. Intermediaries and carriers would not have to store such content data, and thus could not provide access to it. It may however be stored in the systems of the operators (who may be Internet Content Hosts under the *Broadcasting Services Act*.)

[151] OTT application data appears exempt from the data retention regime and need not be kept, so may not be available for access through the data retention scheme: Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015. It is likely to be held by the OTT operator, in many cases in another country. It may be accessible through a warrant, court order or MLAT-related process, if it has been retained.

[152] These are less useful in the aftermath of digitisation and Internet Protocol packet-switched networking.

[153] These may require a warrant or court order to access if it is a traditional document system with confidentiality or privacy conditions. Some data may have no such conditions applying and may be accessible by informal request or arrangement. Foreign data may be accessible through the terms of MLATs and the assistance of foreign agencies.

The *Telecommunications (Interception and Access) Act 1979* (Cth) provides agencies the means 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. [154] Warrants are required where access to content is sought,[155] 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).[156]

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 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.

3.1.4. Access to information by, and from, foreign governments

We turn briefly to information access arrangements with 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*[157] (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 (2.1.5E). 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.[158] These services have been interpreted as including information exchange.[159] 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.[160]

[154] *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.
[155] *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.'
[156] *Telecommunications (Interception and Access) Act 1979* (Cth) Parts 4-1, ss 175 and 176 for ASIO, ss 178–180 for law enforcement agencies.
[157] 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>
[158] S 8(1)(bf) of the *Australian Federal Police Act 1979*.
[159] FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia – Mutual Evaluation Report* (2015) 191.
[160] See <http://www.afp.gov.au/policing/international-liaison/international-network>.

AUSTRAC also actively exchanges information with its financial intelligence counterparts in other countries. AML/CTF-related exchange arrangements of AUSTRAC, ASIC and APRA were described as follows by FATF:[161]

> AUSTRAC had 67 exchange instruments with counterpart foreign financial intelligence units (FIUs) effective in 2014. AUSTRAC uses Egmont's secure web as the primary channel for international exchange. ASIC has a clear and secured gateway for foreign requests; a dedicated email address is available on the ASIC's website. ASIC plans to improve the level of security of the information exchanged with foreign counterparts in 2015, through for example enhanced encryption. Section 127 of the *ASIC Act* provides that information received from foreign regulators, including their requests, is treated as confidential information. ASIC complies with the requirements of the Protective Security Policy Framework (PSPF). APRA also communicates and exchanges information with foreign counterparts using encryption tools.

The Council of Europe *Convention on Cybercrime* was ratified in 2012 by Australia. Key provisions are in Chapter III, Articles 23 and 25, including expedited search, seizure and real-time interception of content. The terms of Convention also facilitate or, in some cases, require disclosure.[162] Australian ratification of the Convention builds on the *Mutual Legal Assistance Treaty* between Australia and the US, and strengthens the basis for disclosure with the other signatories.

AFP reports disclosing stored telecommunications data, sourced from private sector carriers and carriage service providers (as discussed below), to 14 other countries.[163] In 2013-14, AFP made 19 data authorisation requests to 'enforce the criminal law of a foreign country', disclosing (presumably) telecommunications data 17 times to 14 foreign countries.[164] Information regarding the scale of each of these disclosures is not available, nor whether the AFP facilitates access to or disclosure of bulk telecommunications data from private entities.

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.[165] That allows ASD and perhaps

---

[161] FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia – Mutual Evaluation Report* (2015) 188.
[162] Council of Europe, *Convention on Cybercrime*, CETS No. 185 <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>. Article 23 covers general principles relating to international co-operation, and Article 25 is on general principles relating to mutual assistance.
[163] Allie Coyne, 'AFP reports data sharing with Russia, China,' *IT News* (online), 18 June 2015 <http://www.itnews.com.au/news/afp-reports-data-sharing-with-russia-china-405403>, citing AGD, *TIAA Annual Report 2013–14* (2015) <http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/Telecommunications-Interception-and-Access-Act-1979-Annual-Report.pdf>.
[164] The countries were France, Germany, Greece, Hong Kong (The Special Administrative Region of the People's Republic of China), Hungary, India, Italy, Japan, Lithuania, Norway, Poland, Russia, Sri Lanka and Singapore. *TIA Annual Report 2013–14*, 2015, 54 <http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/Telecommunications-Interception-and-Access-Act-1979-Annual-Report.pdf>.
[165] 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*

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 Five Eyes Law Enforcement Group.[166] Research participants in Ch 2 also refer to these arrangements.

Observations

> Australia has a complex framework of data access, collection, use and disclosure rules. In principle, law enforcement and intelligence agencies have access to relevant open source and privately-held data, when appropriate. The picture regarding access to government-held data is more complex. This complexity stems from the federal structure of Australia, the nature of privacy protection in Australia, and the incremental and fragmented development of legislative powers, controls and exceptions to general principles..[167]

3.2. Are legal controls comprehensive and proportional?

Having introduced some of the parameters around access to data for data mining and other Big Data purposes, we now turn to consider the key legal mechanisms that control access and other dealings with Big Data systems. This is not intended to be a comprehensive survey of such controls. In view of the focus of this report, we use examples to illustrate how the current regulatory framework balances law enforcement and national security purposes with the protection of the interests of third parties, including those subject to investigation, those not subject to investigation whose data is intentionally or inadvertently dealt with, and those affected in other ways, such as private data hosts or service providers.

This section applies the test of 'proportionality' as the essential aspect of the legality principle. It examines the extent to which criteria for a robust assessment of proportionality are embedded in the current legal controls of decisions as to whether data should be accessed or collected, as well as in the design, operation and management of (a) data mining and analysis, (b) data retention and deletion, and (c) disclosure (domestically and, where required, internationally).

Apart from the controls embedded in the formal management, governance and oversight structure of agencies,[168] we also look to Guidelines, internal policies and procedures, Memoranda of Understanding (MOU) and other inter-agency agreements to add depth and

(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%20Wide%20Open%20v1.pdf>.

[166] ACC <https://www.crimecommission.gov.au/5-capability-and-development>.

[167] While complexity and inconsistency are proper subjects for remedial simplification and improved coherence, it should perhaps be noted that some 'complexity' in the *Privacy Act* arises because of a history of resolving particular use or disclosure issues by way of a limited exception rather than a blanket roll-back of restriction. Simplicity has obvious merit, but may not support such nuanced tailoring to special cases.

[168] Independent oversight, for instance by the Inspector-General of Intelligence and Security (IGIS) <http://www.igis.gov.au/> in relation to activities of ASIO, ISIS, DIO, AGO, ASD, and ONA is discussed in 3.6.

detail to the operation of the legislative framework.[169] However, many of the internal policies and MOUs are not publicly accessible, and therefore will not be analysed here.

The discussion below will examine provisions contained in national security and law enforcement legislation which 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. This approach is for example embedded in APP 3.1 that states that an agency must not collect personal information (other than sensitive information) unless the information is reasonably necessary for or directly related to the agency's functions or activities.

In the process of deciding this question, the relevant considerations include the scope and objectives of the collector and the purposes of the collection; the seriousness of the matter for which the measure or action is to be deployed; evidence about its effectiveness for the purpose; and the availability of less intrusive, costly or risky alternative measures to achieve similar ends.

Some of these provisions create obligations to weigh law enforcement and national security considerations in the particular circumstance of the case against such countervailing factors as interference fundamental rights and freedoms, which include:

> freedom from trespass by police officers on private property; procedural fairness; … vested property interests. … rights of access to the courts; rights to a fair trial; … freedom from arbitrary arrest or search; … the liberty of the individual; freedom of speech; legal professional privilege... [170]

Other considerations that feature in proportionality tests in the context of this study include privacy, personal information security and confidentiality; effectiveness and alternatives; natural justice; cost and risk, including their projection onto third parties; and other commercial interests.

Where they are present, application of the control provisions is essential in circumstances involving foreseeable risk that information about persons subject to investigation (via warrant or other forms of authorisation) may be intermingled with third parties' data, which, in turn, may lead to adverse inferences, decisions or other detrimental effects for these third parties. A further risk arises when the agency intends to disclose or communicate such information to other entities, including organisations outside Australia.

State/Territory and Federal powers

A range of constitutional controls and rules about data arise from Australia's federal structure. These are evident in the respective constitutional powers of Commonwealth (federal) agencies and State and Territory agencies.

Commonwealth law enforcement agencies, for example, are governed by federal law and are bound by constitutional restrictions on their scope and powers. Within the federal constitutional structure, the Commonwealth has power in relation to 'the influx of criminals' under s 51(xxviii) but it does not have a discrete head of power with respect to criminal law in general. States, in have inherent, residual powers[171] over criminal law enforcement. As a

---

[169] In Ch 2.1.3, a law enforcement research participant describes how MoUs affect the granularity of practical controls (2.1.3G).

[170] In *Momcilovic v The Queen* [2011] HCA 34; 245 CLR 1 at [43] per French CJ.

[171] Under the Constitution, 'residual powers' are powers not included in section 51; they remain within legislative competence of the States.

result, powers over State police and powers over the Commonwealth police (Australian Federal Police) are limited to their particular jurisdictional boundaries. However, these boundaries are blurred when State police officers are involved in the administration and enforcement of federal as well as State criminal law.[172]

The powers of Federal Parliament are subject to restrictions, for example explicit[173] or implied constitutional guarantees;[174] and the common law principle of legality; an important aspect of which is embodied in the following statutory definition of human rights included in the *Human Rights (Parliamentary Scrutiny) Act 2011*:

> the rights and freedoms recognised or declared by … international instruments, including the International Covenant on Civil and Political Rights [ICCPR].[175]

In turn, Article 17(1) 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.

Thus, regulations governing federal agencies that access, collect, use, store or disclose personal information obtained from third party data sets need to comply with Article 17(1). The Parliamentary Joint Committee on Human Rights[176] and the High Court of Australia adopted the criteria of reasonable necessity (in the circumstance of the case) and

---

[172] In *Coleman v Power* [2004] HCA 39; 220 CLR 1 at [80], McHugh J observed that *Crimes Act 1914* (Cth) Part IAA, Divs 2-4 'empowers State police officers to execute search warrants and to make searches'. State police are also included in the definition of 'investigating official'; they can investigate and bring charges against those who threaten national security. David Connery, in 'Essential and underappreciated: The contribution of law enforcement to national Security,' Special Report, Australian Strategic Law Institute, March 2014, 2–3, notes that there is a 'continuum of activities that link' community law enforcement elements with strategic (national security) law enforcement elements <http://apo.org.au/creator/david-connery>.

[173] For example, freedom of religion and the guarantee of obtaining property by the Commonwealth Government on 'just terms' under s 116 and s 51(xxxi) respectively of the *Constitution*.

[174] For example, freedom of political communication, see Australian Capital Television v Commonwealth (1992) 177 CLR 106; Lange v Australian Broadcasting Corporation (1997) 189 CLR 520; APLA Ltd v Legal Services Commissioner (NSW) (2005) 224 CLR 322; Unions NSW v State of New South Wales (2013) 88 ALJR 227.

[175] *Human Rights (Parliamentary Scrutiny) Act 2011*, s 3. Other instruments listed in s 3 are: the International Convention on the Elimination of all Forms of Racial Discrimination done at New York on 21 December 1965 ([1975] ATS 40); the International Covenant on Economic, Social and Cultural Rights done at New York on 16 December 1966 ([1976] ATS 5); the Convention on the Elimination of All Forms of Discrimination Against Women done at New York on 18 December 1979 ([1983] ATS 9); the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment done at New York on 10 December 1984 ([1989] ATS 21); the Convention on the Rights of the Child done at New York on 20 November 1989 ([1991] ATS 4); the Convention on the Rights of Persons with Disabilities done at New York on 13 December 2006 ([2008] ATS 12).

[176] 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'.

proportionality[177] as the test for determining whether interference with someone's privacy is 'unlawful' or 'arbitrary'. Elements of the proportionality test are discussed below.

Although in Australia, privacy is not a constitutionally recognised right.[178] Article 17 of the ICCPR guarantees the right to privacy. The *Privacy Act 1988*provides individuals certain protections against interference with their personal information. Consequently, there is a presumption that Australians have a right to privacy, which under the principle of legality can only be infringed on the ground of reasonable necessity and then, it needs to accord with a proportionality test.

This principle is embedded in legislation governing agencies exempted from the operation of the *Privacy Act*, either in statutory provisions or under legislation[179] requiring either mandatory or voluntary privacy guidelines (see 3.2.2). Hence, to paraphrase Crennan J, while some legislative restriction on the right to privacy is permissible, 'a test of the limits of legislative power is necessary in order to ensure that the … [privacy] is not so limited as to be lost'.[180]

The restrictions in the form of the legality principle also impact the powers that Federal legislation can grant to Federal agencies, including powers to access and disclose data.

---

177 The High Court in its analysis has referred also to the European Convention on Human Rights (ECHR) Article 8.2, which prohibits 'interference by a public authority with the exercise of … [the right to privacy] 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 wellbeing of the 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'' Though ECHR is not listed in Human Rights (Parliamentary Scrutiny) Act 2011, s 3, Art 8.2 has been very influential. While neither ICCPR Art 17(1) nor ECHR Art 8.2 refer to proportionality, both provisions have been construed as imposing a test of proportionality and necessity.

178 Unlike the United States, where by analogy with trespass to land and trespass to chattels, courts are extending common law remedies for wrongful intentional interference with electronic networks, unauthorized access to websites, and use of website information without licence or permission (see for example *Ebay, Inc v Bidder's Edge* 100 F Supp 2d 1058 (ND Cal 2000), *Theofel v Farey-Jones*, 359 F3d 1066, 2003 US App (9th Cir Cal 2004), the High Court of Australia is yet to develop a general remedy for violation of privacy (Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (Lenah) [2001] HCA 63).

179 *Intelligence Services Act 2001*, s 15: 'Rules to protect privacy of Australians: (1) The responsible Minister in relation to ASIS, the responsible Minister in relation to AGO and the responsible Minister in relation to ASD, must make written rules regulating the communication and retention by the relevant agency of intelligence information concerning Australian persons. (2) In making the rules, the Minister must have regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by the agencies of their functions. Note: For 'Australian person' see section 3. (3) Before making the rules, the Minister must consult with: (a) in the case of ASIS – the Director-General; and (ab) in the case of AGO – the Director of AGO; and (b) in the case of ASD – the Director of ASD; and (c) in any case – the Inspector-General of Intelligence and Security and the Attorney-General. (4) For the purpose of consultations under paragraph (3)(c), the Minister must provide a copy of the rules the Minister is proposing to make to the Inspector-General of Intelligence and Security and to the Attorney-General. (5) The agencies must not communicate intelligence information concerning Australian persons, except in accordance with the rules. (6) The Inspector-General of Intelligence and Security must brief the Committee on the content and effect of the rules if: (a) the Committee requests the Inspector-General of Intelligence and Security to do so; or (b) the rules change. Note: For '*Committee*' see s 3(7) Rules made under subsection (1) are not legislative instruments.

180 *Maloney v The Queen* [2013] HCA 28 at [166] per Crennan J.

The governance of State police and their law enforcement 'assets', including data, on the other hand, comes within broad terms of the States' legislative powers.[181] The exercise of the legislative powers conferred upon the State Parliaments is limited only by the federal structure,[182] though it may include some restrictions 'which are not spelled out in the constitutional text'.[183] In particular, the High Court is yet to determine the scope of the inhibitions on State legislative power in relation to fundamental principles of human rights.[184] Until this question is determined, State Parliaments, with the exception of the Victorian legislature,[185] can choose, but are not compelled, to incorporate human rights considerations into control mechanisms for access, collection, management and disclosure of data-sets relating to purely local crimes. Where these activities involve the *Crimes Act 1914* (Cth), however, they are probably bound by the same obligations and controls as Federal Agencies.[186]

The legal picture is intricate and unclear, but it is relevant to intergovernmental data-sharing between State and Federal Agencies. For example, the proposed scheme to create a nation-wide facial recognition database, 'which would match faces to images on passports, visas and driver's licences'[187] by sharing and matching information held by State and Federal law

---

[181] Confirmed by s 2 of the *Australia Act 1986.* For example, *Constitution Act 1975* (Vic), s 16 provides that 'The Parliament shall have power to make laws in and for Victoria in all cases whatsoever.' See also *Constitution Act 1902* (NSW), s 5 Parliament has the power to make laws 'for the peace, welfare, and good government of New South Wales'.

[182] States laws enacted under their inherent, residual and concurrent powers continue in force by virtue of sections 106 and 107 of the *Constitution*, except to the extent that the concurrent Federal Constitutional laws are inconsistent with those of the States (section 109 of the *Constitution*).

[183] *Durham Holdings Pty Ltd v New South Wales* [2001] HCA 7; 205 CLR 399 at [14] per Gaudron, McHugh, Gummow and Hayne JJ citing *Kable v Director of Public Prosecutions* (NSW) [1996] HCA 24; (1996) 189 CLR 51; *Lange v Australian Broadcasting Corporation* [1997] HCA 25; (1997) 189 CLR 520 at 567–568.

[184] According to the plurality in *Durham Holdings Pty Ltd v New South Wales* [2001] HCA 7; 205 CLR 399. See also *Union Steamship Pty Ltd v King* [1988] HCA 55; (1988) 166 CLR 1 at 10: 'Just as the courts of the United Kingdom cannot invalidate laws made by the Parliament of the United Kingdom on the ground that they do not secure the welfare and the public interest, so the exercise of its legislative power by the Parliament of New South Wales is not susceptible to judicial review on that score. Whether the exercise of that legislative power is subject to some restraints by reference to rights deeply rooted in our democratic system of government and the common law, a view which Lord Reid firmly rejected in *Pickin v British Railways Board* [1974] UKHL 1; [1974] AC 765 at 782, is another question which we need not explore.'

[185] *Charter of Human Rights and Responsibilities Act 2006* (Vic).

[186] *Kable v Director of Public Prosecutions* (NSW) [1996] HCA 24; (1996) 189 CLR 51.

[187] Allie Coyne, 'Aussie facial recognition database to land next year' *itNews* 27 August 2015 <http://www.itnews.com.au/news/aussie-facial-recognition-database-to-land-next-year-408471>. Apparently the national facial recognition system will share images that may include stills from licence plate cameras or CCTV. See also AGD, *National Organised Crime Response Plan 2015–18* at 18 <http://www.ag.gov.au/CrimeAndCorruption/OrganisedCrime/Documents/NationalOrganisedCrimeResponsePlan2015-18.pdf>.

enforcement Agencies, National Security Agencies, and road authorities[188] will have to tackle its constitutional law implications.[189]

The Test of Proportionality as a Legal Control Mechanism

This section discusses the application and effectiveness of a proportionality test as a legal control mechanism. As noted earlier, in the law enforcement and national security context, authorisation to collect information in electronic form may have a practical effect of infringing certain freedoms and privileges of Australian persons. The precise criterion to be applied in the proportionality analysis involves 'a test of the legitimacy and proportionality of a legislative restriction of a freedom or right which is constitutionally, or ordinarily, protected.'[190]

A case concerning access to, or management of, Big Data by law enforcement or national security agencies has not yet come before the High Court. If this matter were to be litigated, the case of *Thomas v Mowbray* provides a clear example of the way proportionality test would be applied. The case concerned constitutional validity of the power vested in issuing courts under s 104.4(c) of the *Criminal Code* (Cth) to make an interim control order.[191] In a phrase not dissimilar to requirement for issuing telecommunication access warrants, the court has to be 'satisfied on the balance of probabilities: (i) that making the order would substantially assist in preventing a terrorist act …'[192]

The full High Court by majority (Kirby J dissenting) upheld the constitutional validity of interim control orders on the ground that an interim control order could not be made unless it was '*reasonably necessary and reasonably appropriate and adapted for the purpose'* of protecting the public from a terrorist act.[193] The High Court held that as expressed, these statutory criteria were in accordance with the test of proportionality and thus fell within the principle of legality.

In general, the test of the practice or measure having to be '*reasonably necessary and reasonably appropriate and adapted for the purpose*' can be adapted to other contexts, including the analysis of statutory provisions which authorise (not necessarily by way of a warrant) agencies to access large data sets. For example, the acts and practices of ASIO, ASIS

---

[188] 'The Department of Foreign Affairs, Immigration, the federal police, the Australian Security Intelligence Organisation, Defence, and the Attorney-General's Department will be able to access the platform' Allie Coyne, 'Aussie facial recognition database to land next year' *itNews* 27 August 2015 <http://www.itnews.com.au/news/aussie-facial-recognition-database-to-land-next-year-408471>.
[189] One way of alleviating the problem would be through inter-governmental agreements or through referral of powers under s s51(xxxvii) of the *Constitution*.
[190] *Maloney v The Queen* [2013] HCA 28 at [130] per Crennan J. Her Honour referred to *Betfair Pty Ltd v Western Australia* [2008] HCA 11; (2008) 234 CLR 418 at 477 [102]–[103]; [2008] HCA 11; to *Thomas v Mowbray* [2007] HCA 33; (2007) 233 CLR 307 at 331–333 [20]–[26] per Gleeson CJ; [2007] HCA 33.
[191] Interim order imposes on individuals affected several obligations, prohibitions and restrictions enumerated in s 105(3).
[192] Furthermore, s 104.4 (d) required that the issuing court must be 'satisfied on the balance of probabilities that each of the obligations, prohibitions and restrictions to be imposed on the person by the order is reasonably necessary, and reasonably appropriate and adapted, for the purpose of: (i) protecting the public from a terrorist act; or (ii) preventing the provision of support for or the facilitation of a terrorist act; or (iii) preventing the provision of support for or the facilitation of the engagement in a hostile activity in a foreign country.'
[193] See also *Attorney-General (NT) v Emmerson* [2014] HCA 13; 253 CLR 393 at [19] per French CJ, Hayne, Crennan, Kiefel, Bell and Keane J.

and the ONA have historically been exempt from the operation of the *Privacy Act 1988*.[194] Also exempted from the operation of the *Privacy Act* are any records that originate with, or have been received from these agencies,[195] as is disclosure of personal information to ASIO or ASIS.[196] Likewise, the three units of the Defence Intelligence Group (ASD, DIGO and DIO) 'are exempt from the operation of the *Privacy Act 1988* where their acts and practices relate to their activities'.[197] The exemption encompasses 'records that have originated with, or have been received from, these agencies' as well as disclosure of personal information to the ASD.[198]

However, where the *Privacy Act 1988* does not apply, fundamental rights and privileges of Australians are still protected through the principle of legality, which is based on the test of proportionality as control mechanism. In the framework of law enforcement and national security agencies, the proportionality test is embedded, to a lesser or greater degree, in provisions that set out conditions for decision-making in relation to access warrants, collecting, maintaining, disclosure and destruction of data.

As noted above the common law notion of proportionality is based on the notion of 'reasonable necessity'.[199] It involves two steps:

1. evaluation of whether the proposed measure, for example data access warrant/authorisation, is reasonably necessary and appropriate to fulfil the statutory purpose of protecting the public; and
2. if it is, whether this factor – protection of the public – should prevail over fundamental[200] individual rights not only of the party whose data is being accessed, but also of those whose information becomes available as an unintended consequence of the authorised access.

The High Court's notion of 'reasonableness' provides an overarching standard for the test of proportionality. In *Minister for Immigration and Citizenship v Li*[201] Gageler J, having noted 'reasonableness is a concept deeply rooted in the common law', cited with approval the statement of the Supreme Court of Canada in *Dunsmuir v New Brunswick*[202] that the

---

194 *Privacy Act 1988* s 7(1)(a)(i)(B), (2)(a). See also the discussion on exemption of agencies by the ALRC from 2008, prior to the change of name to ASD <http://www.alrc.gov.au/publications/34.%20Intelligence%20and%20Defence%20Intelligence%20Agencies/defence-and-defence-intelligence-age>.

195 *Privacy Act 1988* s 7(1)(f).

196 s 7(1A)(a), (b).

197 *Privacy Act 1988* (Cth) s 7(1)(ca).

198 s 7(1)(g); s 7(1A)(c).

199 In *Thomas v Mowbray* [2007] HCA 33; 233 CLR 307, discussed above, at [310] Kirby J in his dissenting judgment noted that the phrase in *Criminal Code* (Cth), Pt 5.3, Divs 104, 'the measures … are reasonably necessary, and reasonably appropriate and adapted, for the purpose of protecting the public' directs attention away from the actual subjects of the measures while focusing reasonable necessity and appropriateness of the measures vis á vis the general purpose. Referring to the 'control order' in this section, his Honour noted at [322] that the criterion of 'reasonable necessity' to protect the public is the only factor that is to be balanced against 'against the individual rights of the person subjected to the order'.

200 In *Momcilovic v The Queen* [2011] HCA 34; 245 CLR 1 at [43] French CJ, having noted difficulties with his designation has suggested that the adjective 'fundamental' be discarded in the context of the legality principle. However, other members of the High Court continue to refer to 'fundamental' rights and privileges.

201 [2013] HCA 18 at [105].

202 [2008] 1 SCR 190 at 220–221 [47].

standard reasonableness 'is concerned mostly with the existence of justification, transparency and intelligibility within the decision making process and with whether the decision falls within a range of possible, acceptable outcomes which are defensible in respect of the facts and the law'. [203]

The test of proportionality involves balancing conflicting considerations (that may or may not be listed in the relevant provisions) to decide whether a particular practice or measure is justified in the circumstances of its use. However, it does not necessarily lead to 'all or nothing' result; rather, where conflicting considerations are evenly balanced, the test directs the decision-maker to consider alternative ways of achieving the statutory purpose.

Space does not allow for a comprehensive analysis of all instances where the relevant legislation and other instruments impose the obligation to apply a proportionality test on decision-makers. We offer some representative examples, and observations about assumptions made generally or implied in particular controls. Specific criteria and factors to be considered in the application of the proportionality assessment are discussed in turn.

The test of 'reasonable necessity' is applicable to enabling legislation, for example, to the *Intelligence Services Act 2001* [ISA].[204] Although the term 'proportionality' does not appear in ISA, the regime for authorisations of activities or series of activities relating to producing intelligence on Australians[205] incorporates the necessity criterion in s 9(1), which provides that:

> 'Before a Minister gives an authorisation, the Minister must be satisfied that:
>
> (a) any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned; and
>
> (b) there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency; and
>
> (c) there are satisfactory arrangements in place to ensure that 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'.[206]

This statutory wording is in harmony with Kiefel J's formulation of the test *in Maloney v The Queen* as:

> 'The inquiry undertaken to determine whether a law is proportionate is directed to the relationship between a valid legislative object and the means adopted for its

---

[203] *Dunsmuir v New Brunswick* [2008] 1 SCR 190 at 220–221 [47]; the case involved application of natural justice (procedural fairness) principles in the decision to dismiss a public office holder.
[204] See Chapter 1. ISA governs Australian Secret Intelligence Service (ASIS), Australian Geospatial-Intelligence Organisation (AGO), and Australian Signals Directorate (ASD).
[205] *Intelligence Services Act 2001*, s 8(1)(a)(i)(ia)] by ISIS, AGO or ASD. In general, under Intelligence Services Act 2001: the responsible Minister personally [s 3A] must give a direction in writing to ISIS, AGO or ASD [s 8(1)], a copy of this direction is also provided to the Inspector-General of Intelligence and Security; then 'each Agency Head 'must ensure that the agency complies with any direction given by the responsible Minister', and report on authorised activities to the responsible Minister [s 10A].
[206] *Intelligence Services Act 2001* s 9(1)(d) provides that 'an authorisation for an activity, or a series of activities, of a kind mentioned in subparagraph 8(1)(a)(ia) or (ib)', ie relating to collection of intelligence, the *Defence Minister must request 'the authorisation in writing'.* The requirement that authorisation be in writing is important for the purpose of accountability and transparency.

> attainment. *To be proportionate, a law must go no further than necessary having regard to that object*.'[207] [Emphasis added]

The second criterion of proportionality was articulated by Crennan J in *Maloney* in the following way: [208]

> 'Proportionality analysis tests a law imposing restrictions upon a guaranteed freedom by determining the reasonableness of the means employed by the statute to achieve its legitimate statutory objective.'

This criterion is also reflected in s 9, for not only does it seek to confine activities (essentially intelligence – data – gathering) to 'what is necessary for the proper performance of a function of the [relevant] agency', but also directs the Minister's attention to the reasonableness of both the nature of the proposed activity, and its consequences.

The third criterion of proportionality: consideration whether there exist 'equally as effective', 'obvious and compelling' alternative measures[209] is not explicit in the legislation; however it might be implied in the requirement of 'satisfactory arrangements'.

Since the application of the proportionality test tends to be contained in provisions focusing on Australian persons (as distinct from non-Australians), it is apposite to begin with this distinction.

3.2.2. Australian Persons and non-Australian Persons

In some national security legislation, Australian persons are vested with more protections than non-Australians.[210] The distinction is similar to the approach adopted in the USA,[211] and at least in part, based on the presumption that 'that citizens naturally have constitutional rights, whereas foreigners do not'.[212] However, like Australian citizens, permanent residents also enjoy fundamental common law rights and privileges under the principle of legality.[213]

The distinction between 'Australian persons' and 'others' is central to the *Guidelines to Protect Privacy of Australian Persons* published by some national security agencies that

---

[207] *Maloney v The Queen* [2013] HCA 28; 252 CLR 168 at [182]. Her Honour referred to *Monis v The Queen* [2013] HCA 4; (2013) 87 ALJR 340 at 396 [280], 408 [347]; 295.
[208] *Maloney v The Queen* [2013] HCA 28; 252 CLR 168 at [166].
[209] *Maloney v The Queen* [2013] HCA 28; 252 CLR 168 at [183]: 'The existence of any possible alternative is not sufficient to show that the measure chosen was not reasonably necessary according to the test. An alternative measure needs to be equally as effective, before a court can conclude that the measure is a disproportionate response [*North Eastern Dairy Co Ltd v Dairy Industry Authority of NSW* [1975] HCA 45; (1975) 134 CLR 559 at 616; *Rowe v Electoral Commissioner* (2010) 243 CLR 1 at 134 [438].] Moreover, in *Monis v The Queen*, Crennan and Bell JJ and I said that the alternative means must be obvious and compelling, having regard to the role of the courts in undertaking proportionality analysis.'
[210] These include, for example, provisions under *Intelligence Services Act 2001* s 8, s 9 and s 13B; Privacy Rules or Guidelines of intelligence agencies including those with a focus on international matters or persons outside Australia such as DIO (discussed below), ASD, ASIS, ONA and AGO, although not ASIO, which has a domestic focus; and *Migration Act 1958*, ss 257A and 258 as amended by *Migration Amendment (Strengthening Biometrics Integrity) Act 2015* regarding provision of personal biometric data identifiers. See also Technical Reference 4 and 5.
[211] *Foreign Intelligence Surveillance Act* (USA) s 702.
[212] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 *Harvard International Law Journal* 81 at 87.
[213] For a list of these rights and privileges see *Momcilovic v The Queen* [2011] HCA 34; 245 CLR 1 at [43] per French CJ.

receive, analyse and disclose information for foreign intelligence purposes, for example, the DIO.[214] The *Privacy Guidelines* distinguish 'Australian persons', defined as 'citizens and permanent residents',[215] from 'others' – visiting foreigners and persons outside Australian jurisdiction. Additionally, they contain a presumption that 'where it is not clear whether a person is an Australian person … a person within Australia shall be presumed to be an Australian person, and a person outside Australia shall be presumed to not be an Australian person'.[216]

Privacy Guidelines were adopted by the DIO and ONA and *Privacy Rules* were issued in accordance with section 15 of the *Intelligence Services Act*, for ASIS, ASD and AGO. ASIO, on the other hand, has a set of Guidelines issued by the Attorney-General (*ASIO Guidelines*).[217] While the texts of the *Privacy Guidelines* and the *Privacy Rules* are broadly consistent, the *ASIO Guidelines* differ.

The *Privacy Guidelines* and *Privacy Rules* provide an additional instrument governing agency activities beyond each agency's governing legislation (*Intelligence Services Act 2001* in the case of DIO, ASD and AGO, *Office of National Assessments Act 1977* in the case of ONA). The *Intelligence Services Act*, for example, sets out a number of requirements and restrictions that enhance privacy protections. ASD and AGO as collection agencies are, for instance, restricted in the intelligence they may gather on Australian persons and require a Ministerial authorisation before undertaking activities for the specific purpose of producing intelligence on an Australian person or that will have a direct effect on an Australian. Before making such an authorisation, the Minister must be satisfied that the activities will be necessary and reasonable.[218] The Privacy Guidelines restrictions apply in addition to this test in the legislation itself and should be considered in that context.

---

[214] The DIO 'Guidelines are intended to be broadly consistent with rules made under section 15 of the *Intelligence Services Act 2001* that apply to the Australian Geospatial-Intelligence Organisation, the Australian Secret Intelligence Service and the Australian Signals Directorate, and the guidelines developed by the Office of National Assessments'. DIO, *Guidelines to Protect the Privacy of Australian Persons,* Department of Defence web site, undated <http://www.defence.gov.au/dio/privacy-rules.shtml>. See also *ASIS Privacy Rules,* ASIS web site, 17 September 2008; <https://www.asis.gov.au/Privacy-rules.html>. See also recent moves by US to extend protection to at least European 'non-US persons', Judiciary Committee 'Goodlatte, Sensenbrenner and Conyers Praise House Passage of Legislation to Strengthen Privacy Protections for Individuals,' blog, US House of Representatives, 20 October 2015, discussed below <http://judiciary.house.gov/index.cfm/2015/10/goodlatte-sensenbrenner-and-conyers-praise-house-passage-of-legislation-to-strengthen-privacy-protections-for-individuals>.

[215] *Intelligence Services Act 2001* s 3. *Australian Security Intelligence Organisation Act 1979* s 4 does not define 'Australian person' but defines 'permanent resident' as '(a) natural person (i) who is not an Australian citizen; (ii) whose normal place of residence is situated in Australia; (iii) whose presence in Australia is not subject to any limitation as to time imposed by law; and (iv) who is not an unlawful non-citizen within the meaning of the *Migration Act 1958'*; or a body corporate '(b) in the case of a body corporate: (i) which is incorporated under a law in force in a State or Territory; and (ii) the activities of which are not controlled (whether directly or indirectly) by a foreign power'.

[216] See also ONA *Guidelines to Protect the Privacy of Australian Persons or Corporations* <https://www.ona.gov.au/sites/g/files/net341/f/privacy_guidelines.pdf>.

[217] *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* (AG ASIO Guidelines), ASIO web site, undated <https://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf>.

[218] *Intelligence Services Act 2001* s 9.

These provisions in favour of Australian persons largely reflect the jurisdictional limits of the relevant agency legislation, for example, the focus in *Intelligence Services Act 2001* (Cth) s 6(1)(a) and (e) is on 'the capabilities, intentions or activities of people or organisations outside Australia.' In essence the rules provide greater protection for Australians compared to non-Australians, including rights with respect to the legality principle. It is also evident in comments from research participants about differential treatment of data depending on whether it concerns Australians (2.5.1I, 2.5.1K).

Observations

> *Privacy Guidelines* and *Privacy Rules* of national security agencies that functios as foreign intelligence agencies distinguish between Australian persons and non-Australian persons. Given the nature and objectives of the agency and its major focus on 'preventing a terrorist attack in Australia, countering terrorist-related activity, warning of security threats and countering espionage and foreign interference against Australia',[219] ASIO's *Attorney-General's Guidelines*,[220] discussed below, do not distinguish between Australian and non-Australian persons.[221] They apply controls on the scope of ASIO activities in the interests of people generally.

3.2.3. Proportionality test as control to protect privacy

We now turn to the potential for the use of proportionality tests to protect privacy in the context of national security and law enforcement.[222]

Technical Reference 9 to this report contains details of several provisions containing variants of the proportionality test. It compares the different formulations of proportionality factors in a sample of Acts, illustrating the diversity within an Act, and between Acts. These represent significant variations among the contexts in which privacy and other potentially relevant factors may be taken into account as a form of proportionality assessment. The most common factor considered relevant is privacy, but other factors include the following (some of which are discussed in context below):

- 'the interests of law enforcement and national security'[223]
- 'the objects of the *Telecommunications (Interception and Access) Act 1979* (Cth)[224]
- The activity is 'necessary, and not beyond what is necessary, for the performance of a function of the agency'[225]

---

[219] See ASIO, 'What we do,' web page <http://www.asio.gov.au/About-ASIO/What-we-do.html>.
[220] *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* (AG ASIO Guidelines), ASIO web site, undated <https://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf>.
[221] In interviews, there were suggestions that separate rules applied to Australians and non-Australians for ASIO too. While the aim of ASIO is framed as protecting the interests of Australians, such differences in treatment of persons of interest were not obvious from the *AGs Guidelines*.
[222] 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'.
[223] *Telecommunications (Interception and Access) Act 1979* s 189(4)(a).
[224] *Telecommunications (Interception and Access) Act 1979* s 189(4)(b).
[225] *Intelligence Services Act 2001* s 9(1)(a) and (b).

- 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’[226]
- Act is done with ‘due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest’[227]
- ‘the least intrusive techniques of information collection … used before more intrusive’[228]
- ‘where a threat is … likely to develop quickly, a greater degree of intrusion’[229]
- ‘likely relevance and usefulness of the information or documents’[230]
- ‘why the disclosure or use concerned is proposed to be authorised’[231]
- ‘proportionate to the gravity of the threat posed and the probability of its occurrence’[232]
- ‘the disclosure is appropriate in all the circumstances’
- ‘to what extent methods … that do not involve the use of a stored communications warrant in relation to the person … are available’[233] and ‘how much [they] would be likely to prejudice [or assist] the investigation’
- ‘the gravity of the conduct constituting the serious contravention’[234]
- ‘any submissions made by the Victorian Public Interest Monitor’[235] (discussed below)

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. Proportionality tests often have a similar approach or core concerns, but there may be a need to tailor a test to the objective of the provisions themselves rather than simply replicating a standard formulation of a proportionality test across legislation, or within a single piece of legislation.

Notwithstanding these explanatory factors and the at times unavoidable variation due to differences of intent and context, the impact of this variation is relevant in the scheme of this review, as are potential methods for increasing the robustness of proportionality assessments.

---

[226] *Intelligence Services Act 2001* s 9(1)(c).
[227] *Attorney-General’s Guidelines for ASIO* [10.4(b)] <http://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf>.
[228] *Attorney-General’s Guidelines for ASIO* [10.4(d)].
[229] *Attorney-General’s Guidelines for ASIO* [10.4(e)].
[230] *Telecommunications (Interception and Access) Act 1979* s 180F.
[231] *Telecommunications (Interception and Access) Act 1979* s 180F.
[232] ASIO *Attorney-General’s Guidelines* [10.4].
[233] *Telecommunications (Interception and Access) Act 1979* s 116(2)(d).
[234] *Telecommunications (Interception and Access) Act 1979* s 116(2)(b).
[235] *Telecommunications (Interception and Access) Act 1979* s 46(2)(fa) and 46A(2)(fa). These say that an eligible Judge or nominated AAT member considering an application for a warrant in relation to a telecommunication service or a person shall have regard to a list of matters, including where the application is by an interception agency of Victoria, ‘any submissions made by the Victorian PIM under section 44A to the Judge or nominated AAT member.’

Observations

> While some of the variation observed in the tests 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, the inconsistency and uncertainty may nevertheless make a coherent decision-making framework somewhat more complex to develop, train for, and oversee. There is potential for consideration of whether all instances of variation are necessary or unavoidable.

Guidelines to Protect the Privacy of Australian Persons (non-ASIO)

Intelligence Agencies exempted from the purview of the *Privacy Act 1988*[236] have own codes regulating, among others, the retention and communication of intelligence information. As discussed in 3.2.2, *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 section 15 of the *Intelligence Services Act* for ASIS, ASD and AGO. The *Privacy Guidelines* are broadly consistent with the *Privacy Rules*,[237] slightly adapted to the specific functions of each agency.

The *Privacy Guidelines* and *Privacy Rules* provide an additional instrument governing agency activities beyond each agency's governing legislation (*Intelligence Services Act 2001* in the case of DIO, ASD and AGO, *Office of National Assessments Act 1977* in the case of ONA). The *Intelligence Services Act*, for example, sets out a number of requirements and restrictions that enhance privacy protections. The *Privacy Guidelines* restrictions apply in addition to any such statutory requirements and restrictions. They do, however, not have the status of legal instruments.

Attorney-General's Guidelines for ASIO

Data collection is a major function of national intelligence agencies. For example, ASIO's functions involve:

(a) collecting, including gaining access, maintaining, analysing and assessing information related to inquiries and investigations;
(b) collecting, again including access, and maintaining a comprehensive body of reference material to contextualise intelligence derived from inquiries and investigations; and
(c) maintaining a broad database, based on the above, against which information obtained in relation to a specific inquiry or investigation can be checked and assessed.[238]

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*[239] are more

---

[236] See ALRC, *For Your Information: Australian Privacy Law and Practice* (Report 108), 2008, 34. Intelligence and Defence Intelligence Agencies – Rationale for the exemption of the intelligence and defence intelligence agencies <http://www.alrc.gov.au/publications/34. Intelligence and Defence Intelligence Agencies/rationale-exemption-intelligence-and>.
[237] S 15 of the *Intelligence Services Act 2001*.
[238] ASIO *Attorney-General's Guidelines* [6.2] <http://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf>.
[239] ASIO Attorney-General's Guidelines [6.2].

comprehensive than the *PrivacyGuidelines* discussed above, and, like the *ASIO Act 1979*, seek to achieve a 'balance between individual rights and the public's collective right to security'.[240] This balance is more reflective of concepts of proportionality. Elements of the test are woven into several control mechanisms, which are imposed at different levels of decision-making.

The ASIO Director-General is responsible for determining who should be investigated by ASIO, and the investigative methods to be used.[241] 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'.[242] 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'.[243]

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;[244]

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 about individuals.[245] 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:

> (c) the more intrusive the investigative technique, the higher the level of officer that should be required to approve its use;
> (d) wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and
> (e) where a threat is assessed as likely to develop quickly, a greater degree of intrusion may be justified.[246]

[240] See <http://www.asio.gov.au/About-ASIO/Legislation.html>.
[241] ASIO *Attorney-General's Guidelines* [7.1]; [9.1].
[242] ASIO Attorney-General's Guidelines [9.1].
[243] ASIO *Attorney-General's Guidelines* [10.4].
[244] ASIO *Attorney-General's Guidelines* [10.4].
[245] ASIO is not one of the Agencies involved in the data-matching under *Data-Matching Program (Assistance and Tax) Act 1990*, see below.
[246] ASIO *Attorney-General's Guidelines* [10.4].

Observations

ASIO's *Attorney-General's Guidelines* apply in relation to both Australian and non-Australian persons. However, the scope of agency's mission implies that non-Australian persons will only be of interest where they have some relationship with Australia. The control test of proportionality 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, *Privacy Guidelines* are not legislative instruments; it weakens their legal standing and provides for amendments without the direct Parliamentary oversight.

Lack of guidance involving proportionality test for analysts

The quality and reliability of Information and data used for intelligence purposes is often, of necessity, very variable; some of the issues are explored in 3.3 below. Drawing on public information, there appears to be no test for assessment or grading of the quality and significance of the particular data (collected or analysed)[247] that requires balancing national security purpose against adverse risks to the interests of of data subjects or third parties. Neither the *ASIO Act 1979* nor the *Attorney-General's Guidelines* contain this kind of guidance for analysts. It is possible of course that non-public ASIO internal policy documents include a specific proportionality test for ASIO analysts. The decisions of analysts regarding accessing data and the analysis of the accessed data may have profound legal, reputational and commercial implications for subjects of the assessment and it is submitted that such a test as well as a public requirement to apply the test, are important to ensure public trust in the fairness of the analytical process.

Observations

From the perspective of good governance and public trust, it may be helpful for such proportionality test to be developed or, if one already exists, to incorporate it into the *Guidelines*.

A common proportionality test with a substantial set of factors for use by analysts and decision makers across all law enforcement and national security agencies may harmonise and improve both communications and comparisons of analysis undertaken within different organisations. Such a test could usefully start from the example in ASIO's *Attorney-General's Guidelines* and incorporate other factors supporting robust and quantitative balancing assessments.

3.2.4. Other aspects of the legality principle relevant to control mechanisms

Natural Justice

Predictive analytics based on unreliable data carry, among others,[248] an inherent risk of personal information being misinterpreted; assessed out of context; erroneously weighted; or unfairly dealt with in some other way. By way of analogy, adverse consequences for individuals occasioned by faulty data-matching system between VicRoads and Victorian

---

[247] The grading test known as 'Admiralty System' or 'the NATO System' is used to evaluate source reliability and validity of data for intelligence purposes. (See 8.4 below for a discussion of the grading system).

[248] Unreliable data impacts effectiveness of data analytics as predictive tool.

Police can serve as an example. In 2014, Victoria introduced data-matching number plate recognition technology linked to VicRoads, which enabled police to detect unregistered vehicles on hand-held devices. At the same time, VicRoads, while retaining the policy of expiry notifications, decided to discontinue providing evidence (windscreen stickers) to motorists that they have successfully initialled or renewed their registration. Due to system errors, including inconsistent delivery of renewal notices by VicRoads,[249] thousands of motorists whose vehicles were unregistered through no fault of their own became subject to fines of $740.[250] In this example VicRoads decided 'to investigate the accuracy of their system, above the yearly sampling and auditing which already takes place'[251] only after several months of public pressure by the affected individuals and the media. However, it is unclear whether Victoria Police (and all other agencies entitled to share its data-bases) will take the initiative to correct the erroneous information regarding individuals driving vehicles with 'unregistered' number plates in their data-sets.

The Victorian data-matching example illustrates several major points:

1. The inherent risk of data system errors that adversely impact individuals;
2. The burden of identifying the source of the adverse impact by the affected individuals: while it is relatively easy to do so where a person has been fined, the source of an adverse credit or security rating would be much more difficult to ascertain;
3. The burden of data errors rectification imposed on the affected individuals rather than the creators of the erroneous information (the agencies);
4. The virtual impossibility for the affected individual to know about and to rectify the consequences of the false or inaccurate information flowing through data-systems that have collated and/or collected that information.

Many documents of agencies under consideration are exempted from the *Freedom of Information Act 1982* as well as the *Privacy Act 1988* principles that relate to access to one's record under provisions covering national security or law enforcement.[252] As a result, data subjects are denied the right to query and correct errors in the data set. This, in turn, raises questions to whether procedural fairness to persons so affected (unfairly dealt with) is built into the legislative framework through the common law doctrine of natural justice, which, like proportionality test, is an aspect of the legality principle.[253]

---

[249] Clare Rawlinson, 'Vic Roads admits stickerless vehicle registration system 'not up to scratch', after complaints mount over missing renewal notices', ABC News (online), 7 November 2015 <http://www.abc.net.au/news/2015-11-06/vic-roads-admits-registration-systems-not-up-to-scratch/6918798>; Clare Rawlinson, ‚VicRoads to refund motorists after 'system error' led to fines for unregistered vehicles' ABC News, 12 November 2015, http://www.abc.net.au/news/2015-11-12/victorian-motorists-fined-for-unregistered-car-refunded/6933854>.

[250] As of 15 November 2015, VicRoads and Victorian Police are still in the process of determining the number of motorists who were fined because the system did not accept their change of address and/or change of ownership notifications.

[251] Clare Rawlinson, 'VicRoads to refund motorists after 'system error' led to fines for unregistered vehicles' ABC News (online), 12 November 2015 <http://www.abc.net.au/news/2015-11-12/victorian-motorists-fined-for-unregistered-car-refunded/6933854>.

[252] *Freedom of Information Act* 1982 s 7 especially subsections 2A, 2B, and 2C, and Parts I and II of Schedule 2. See also OAIC, Freedom of information – Exemptions, Fact Sheet 8, December 2010 <http://www.oaic.gov.au/freedom-of-information/foi-resources/foi-fact-sheets/foi-fact-sheet-8-exemptions>.

[253] *Momcilovic v The Queen* [2011] HCA 34; 245 CLR 1 at [43] per French CJ.

At common law a right to see one's records and to either correct or annotate them is linked to the principle of procedural fairness as criterion of natural justice, where a decision impact on legal rights of the person. As Mason J observed in *Kioa v West*:[254]

> It is a fundamental rule of *the common law doctrine of natural justice* expressed in traditional terms that, generally speaking, when an order is to be made which will deprive a person of some right or interest or the legitimate expectation of a benefit,[255] he is entitled to know the case sought to be made against him and to be given an opportunity of replying to it[256]: The reference to 'right or interest' in this formulation must be understood as relating to personal liberty, status, preservation of livelihood and reputation, as well as to proprietary rights and interests.[257]

His Honour continued:[258]

> The law has now developed to a point where it may be accepted that there is a common law duty to act fairly, in the sense of according procedural fairness, in the making of administrative decisions which affect rights, interests and legitimate expectations, subject only to the clear manifestation of a contrary statutory intention.

More recently, in *Assistant Commissioner Condon v Pompano Pty Ltd and Another*,[259] Hayne, Crennan, Kiefel and Bell JJ at [156] observed that:

> The rules of procedural fairness do not have immutably fixed content. As Gleeson CJ rightly observed[260] in the context of administrative decision-making but in terms which have more general and immediate application, [f]airness is not an abstract concept. It is essentially practical. Whether one talks in terms of procedural fairness or natural justice, the concern of the law is to avoid practical injustice.

In circumstances where risks stemming from inadequate barriers to access data sources are known or reasonably foreseeable, rules of natural justice may need to be considered when the relevant proportionality test is applied.

It is of note that *Telecommunications (Interception and Access) Act 1979* Schedule 1 has been amended:

---

[254] [1985] HCA 81; 159 CLR 550 at 583.
[255] Mason J noted at 283–284 that 'The reference to 'legitimate expectation' makes it clear that the doctrine applies in circumstances where the order will not result in the deprivation of a legal right or interest. Take, for example, an application for a renewal of a licence where the applicant, though he has no legal right or interest, may nevertheless have a legitimate expectation which will attract the rules of natural justice.'
[256] *Twist v Randwick Municipal Council* (1976) 136 CLR 106, 109; *Salemi v MacKellar* [No. 2] (1977) 137 CLR, 419; *R v. MacKellar; Ex parte Ratu* (1977) 137 CLR, 476; *Heatley v. Tasmanian Racing and Gaming Commission* (1977) 137 CLR 487, 498–499; *FAI Insurances Ltd v. Winneke* (1982) 151 CLR 342, 360, 376–377; *Annamunthodo v. Oilfields Workers' Trade Union* [1961] AC 945.
[257] See also *Kioa v West* (1985) 159 CLR 550 at 619 Brennan J noting that natural justice protection is extended to 'any interest possessed by an individual whether or not the interest amounts to a legal right or is a proprietary or financial interest or relates to reputation', expressly adopted by Gummow, Hayne, Crennan and Bell JJ in *Plaintiff S10/2011 v Minister for Immigration and Citizenship* [2012] HCA 31; 246 CLR 636 at [66].
[258] *Kioa v West* (1985) 159 CLR 550 at 585.
[259] [2013] HCA 7; 252 CLR 38.
[260] *Re Minister for Immigration and Multicultural and Indigenous Affairs; Ex parte Lam* (2003) 214 CLR 1, 14 [37].

> to make it clear that individuals have the right to access their personal telecommunications data retained by a service provider under the data retention regime. This amendment is consistent with existing policy for access to personal information under the *Privacy Act* and reinforces existing individual rights to obtain access to, correct and annotate personal information provided by the *Privacy Act*.[261]

ASIO Act contains provisions enabling the data subject to request a review of a security assessment under the *ASIO Act*, including the data that was considered in such a process. See 3.4.2 below for further discussion.

Observations

> Control mechanisms can prevent the exercise statutory power by way of access warrants/authorisations from being carried out 'in a manner that is practically unjust'.[262] This risk could be alleviated if the proportionality test were to include reference to consideration of such natural justice principles as the obligation to provide procedural fairness through notification;[263] to accord the affected person a fair hearing; and to act without bias. Any review of the limited procedural controls should address this, subject to the requirements of particular agencies.
>
> Denial of natural justice can be costly to pursue; if the risk of such litigation materialises, it may be associated with negative public perceptions relating to the fairness and trustworthiness of national security or law enforcement agencies

3.2.5. Cost as a control element in proportionality tests

Agencies are expected to pay for access to certain kinds of data,[264] and management of large data sets can be very expensive.[265] (Holders of data are also expected to pay for aspects of making data available - see Technical Reference 10.)

In the case where agencies are required to cover all or most of such costs either from their own budget or from consolidated revenue, considerations of the costs involved may introduce a de facto proportionality test: is the benefit from obtaining the information or maintaining the data-base worth the direct cost to the agency? Factoring in this question may lead to a choice of an equally effective, but less expensive, alternative measure.

There might be cases where this kind of proportionality test could demonstrate that the benefit would significantly outweigh the burden of expenditure, but an agency may not have the funds to pay for the service. That said, French CJ in *Attorney-General (SA) v Corporation of the City of Adelaide,*[266] warned that although 'The availability of an alternative mode of

---

[261] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Item 2629 amending Schedule 1 of the TIAA and also the *Privacy Act,* discussed in the first Supplementary Explanatory Memorandum at [16] and [21], and the Fifteenth Report of the 44th Parliament scrutinising Bills introduced 20-30 October 2014 (November 2014), 14.
[262] *Salemi v Mackellar* (No 2) [1977] HCA 26; (1977) 137 CLR 396 at 419 per Gibbs J.
[263] Under *Australian Security Intelligence Organisation Act 1979*, s 38A the Attorney-General must notify, within 14 days, a person whose adverse or qualified security assessment has been given to the Attorney-General in connection with certain provisions of the *Telecommunications Act 1997*. However, this obligation is strictly limited to adverse or qualified security assessments.
[264] *Telecommunications Interception and Access Act 1979* ss 206–208.
[265] Cost factors were identified as relevant in technological design by many research participants (7.5.5) and can limit the scope of data requests (7.4.5O).
[266] [2013] HCA 3; 249 CLR 1, [65].

regulation may be relevant in cases in which the question of want of reasonable proportionality is raised with respect to delegated legislation', 'counterfactual explorations' may amount to 'second-guessing' the merits of the competing claims.[267]

Observations

A proportionality test factoring in direct costs of a proposed activity or measure against its benefits may offer an efficient instrument for allocating resources between competing priorities, and may sometimes act as a restraint on expensive but low-benefit measures. However the funding of agencies by the Commonwealth and States is a matter of political, not legal judgment.

Where costs are in part borne indirectly by other parties, this effect may be reduced, particularly if the third party bears the risk of unexpected costs above an initial estimate.[268]

3.2.6. Proportionality test for data-matching

Identification of individuals is a core function of data matching.[269] As illustrated by the example of VicRoads and Victoria Police data-matching program in 3.2.3, data matching programs potentially cover a significant proportion of data analysis conducted using Big Data-type systems by national security and law enforcement agencies, and are particularly relevant to decisions that may adversely affect individuals.

The *Data Matching Program (Assistance and Tax) Act 1990* is an example of legislation mandating protocols for data matching. It was established to regulate the use of Tax File Numbers from the ATO in order to compare and cross-match personal information held by the Australian Taxation Office and 'assistance agencies',[270] including the Department of Health and Family Services; the Department of Employment, Education and Training; the Department of Social Security; the Department of Veterans' Affairs; [271] and the Human

---

[267] French CJ concluded at [65] that 'Courts are not in a position to make comparative judgments on such issues, particularly where they may involve costs and the allocation of resources upon which there may be competing claims'.

[268] There are various models for data cost sharing in the telecommunications field, including s 314 *Telecommunications Act* 1997, which applies to giving 'reasonably necessary help' under s 313(3) and (4), but not to carriers etc. 'doing their best' to prevent the commission of offences under s 313(1) and (2). It applies also to authorisations under Chapter 4 Divs 3 and 4 of *Telecommunications (Interception and Access) Act 1979*: see Note in s209. Sections 208 and 209 of the *Telecommunications (Interception and Access) Act 1979* set out a different mechanism for allocating costs for different aspects of interception between carriers and agencies. See Technical Reference 10.

[269] See Commonwealth Data Matching Working Group, *Improving the Integrity of Identity Data: Data Matching – Better Practice Guidelines*, 2009.

[270] *Data-Matching Program (Assistance and Tax) Act 1990* s 3.

[271] The Department of Veterans Affairs administers: *Defence Service Homes Act 1918*; *Military Rehabilitation and compensation Act 2004* (MRCA); *Safety, Rehabilitation and Compensation Act 1988*; *Veterans' Entitlements Act 1986* (VEA); *War Graves Act 1980*.

Services Department which administer the Centrelink,[272] Child Support Agency,[273] Australian Hearing Services,[274] and Medicare Programs.[275]

The Office of Australian Information Commissioner (OAIC) has developed two Data Matching Guidelines under *Privacy Act*:

- *Statutory Guidelines for the Conduct of Data Matching Program* under the *Data-matching Program (Assistance and Tax) Act 1990* (the *Data Matching Act*) covering data matching involving Tax File Numbers (TFNs) by prescribed agencies (*Statutory Guidelines*); and
- *Guidelines on Data Matching in Australian Government Administration* (the *Voluntary Guidelines*) under section 28(1)(a) of the *Privacy Act*, 1988.

The *Statutory Guidelines*[276] issued under *Data-Matching Program (Assistance and Tax) Act 1990* s 12 are relevant to the Agencies under consideration.[277] Their requirements import proportionality considerations, and are explored below.

Although law enforcement and national security agencies are not directly involved with the data-matching scheme under the *Data-Matching Program (Assistance and Tax) Act 1990,* it is part of their investigative functions to obtain, compile, compare and analyse data-sets about subject individuals. While law enforcement, such as the Australian Federal Police, the Director of Public Prosecutions (and presumably national security agencies) are not listed as 'assisting', 'matching' or 'source' agencies,[278] the results of the matching program may be indirectly conveyed to them.[279] Yet, there is a dearth of publicly available protocols for intra-agency or inter-agency data-matching in the law enforcement and national security domain.

---

[272] *Human Services (Centrelink) Act 1997*, which administers programs, services, facilities and 'benefits' (pensions, allowances, concessions or payments; and cards entitling its holder to a concession or a payment of any kind). Under s 6, 'designated programs Acts' include: '*A New Tax System (Family Assistance) (Administration) Act 1999; Aged Care Act 1997; Child Support (Assessment) Act 1989; Child Support (Registration and Collection) Act 1988; Dental Benefits Act 2008; Disability Services Act 1986; Health Insurance Act 1973; Medical Indemnity Act 2002; Midwife Professional Indemnity (Commonwealth Contribution) Scheme Act 2010; National Health Act 1953; Paid Parental Leave Act 2010; Private Health Insurance Act 2007; Social Security (Administration) Act 1999; Student Assistance Act 1973*; an Act specified in a legislative instrument made by the Minister for the purposes of this paragraph.' In addition there are, *Student Identifiers Act 2014; Social Services and Other Legislation Amendment (Seniors Health Card and Other Measures) Act 2014, Farm Household Support Act 2014*

[273] *Child Support (Assessment) Act 1989*; *Child Support (Registration and Collection) Act 1988*.

[274] *Australian Hearing Services Act 1991.*

[275] *Human Services (Medicare) Act* 1973; Healthcare Identifiers Act 2010 and *Personally Controlled Electronic Health Records Act 2012* (now *My Health Record Act*) would also be relevant.

[276] See <https://www.comlaw.gov.au/Details/F2009B00268>.

[277] The other two Guidelines are: voluntary *Guidelines on Data Matching in Australian Government Administration* issued under the *Privacy Act 1988*, s 28(1)(a) <http://www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/data-matching-guidelines-2014>, and mandatory guidelines under *National Health Act 1953* s 135AA regulating the storage, use, disclosure and linkage of patient claims information collected under the Pharmaceutical Benefits Scheme and the Medicare program.

[278] *Data-Matching Program (Assistance and Tax) Act 1990* s 3: the 'matching agency' is the Social Services Department; 'source agencies' are assistance agencies; or the tax agency.

[279] *Guidelines*, [6.5] provide that the 'final completion of the action' in cases 'under the control of the Australian Federal Police' occurs only 'when all investigation action, legal proceedings and repayment of debts due to the Commonwealth are finalised'; likewise in cases under the control of the Director of Public Prosecutions.

Given the comprehensive nature and sensitivity of data-matching results, the OAIC's *Data-Matching Program (Assistance and Tax) Act 1990 Guidelines* [7] prohibit linking or merging 'the information used in the program … in such a way that a new separate permanent register (or databank) of information is created about any, or all of the individuals whose information has been subject to the program.' Moreover, 'After the completion of the action in relation to an individual ..., the source agency must delete any information that relates to that action from any register'.

Under the OIAC Guidelines [3.1], matching and source agencies are required to maintain a program protocol, which, though this is not articulated, is effectively based on proportionality assessment. The agencies must:

- set out the legal basis for any collection, use or disclosure of personal information involved in the data-matching program;
- outline the objectives of the program, the procedures to be employed, the nature and frequency of the matching covered by the program, and the justifications for the program;
- explain what methods other than data-matching were available and why they were rejected;
- detail any [actual] cost/benefit analysis or other measures of effectiveness which were taken into account in deciding to initiate the program;
- outline the technical controls proposed to ensure data quality, integrity and security in the conduct of the program;
- provide an explanation for any use of identification numbers and, in particular, the tax file numbers;
- outline the nature of the action proposed to be taken in relation to the results of the program;
- indicate what form of notice, if any, of the proposed activities in relation to their personal information has been given or is intended to be given to affected individuals;
- and specify any time-limits on the conduct of the program.[280]

Significantly, the OAIC protocol requires the responsible decision-maker to '*outline the technical controls proposed to ensure* data quality, integrity and security in the conduct of the program,' a pro-active and stringent prerequisite.

A number of government data matching activities are conducted without TFNs and are not subject to the operation of the Data Matching Act. However, agencies like the ATO, DHS and AUSTRAC conduct data matching under the OAIC's *Voluntary Guidelines*, which have been adopted by a number of agencies. The *Voluntary Guidelines* reflect a number of requirements contained in the *Statutory Guidelines*, including the obligation to develop a program protocol and a technical standards report.

Agencies that have agreed to comply with the *Voluntary Guidelines* can request an exemption from complying with some parts of the guidelines. Under Guideline 10, the agency must explain the public interest grounds that justify the inconsistency. A list of exemptions granted by the Commissioner is available on the OAIC's website.

By way of contrast, the *Privacy Guidelines* [see 3.2.2] applicable to key intelligence agencies merely require that the relevant Agency 'take *reasonable steps* to ensure the intelligence information that … [the Agency] retains or communicates concerning Australian persons is

[280] *Data-Matching Program (Assistance and Tax) Act 1990 Guidelines* [3.1].

recorded or reported in a *fair and reasonable* manner'.[281] Though it is used twice in this Guidelines sentence, qualifying two different concepts, the adjective 'reasonable' is not provided with any content.

There are no publicly available protocols for intra-agency or inter-agency data-matching involving law enforcement and national security agencies. The *Data Matching Program (Assistance and Tax) Act 1990* does not apply directly to them.

Observations

> Mandatory protocol requirements in the *Data-Matching Program (Assistance and Tax) Act 1990 Guidelines* compel decision-makers to undertake a systematic and thorough examination of reasons for the proposed data-matching procedure, including benefits and burdens at societal, institutional and individual level. This is a useful proportionality assessment process.
>
> The Protocol also incorporates natural justice (notice) and fairness (time-limits) components. These aspects could contribute to a model for the design of comprehensive proportionality tests for similar programs undertaken by law enforcement and security agencies.

3.2.7. Controls indirectly protecting privacy and other rights in the form of offences

Thus far we have focussed on controls that directly protect the privacy of data subjects. There are also provisions that provide indirect protection, for example punishing individuals within agencies who communicate information about data subjects without authorisation. This provides an incentive for officers within government agencies to comply with the more direct privacy protections discussed above. The level of indirect protection is strongest where the consequences of breach are severe, for example a term of imprisonment. Such consequences were specifically mentioned by some research participants as explaining high levels of compliance with procedures within agencies (see 2.5.3).

The kinds of authorised communications are set out in the relevant agency legislation. For example, according to *ASIO Act 1979*, s 18(1), communication of intelligence on behalf of the Organisation can be made only by the Director-General, or by a person acting within the authority given by Director-General. Additionally, under s 18(3) and (4), ASIO can communicate information to Commonwealth and State authorities if it is concerns a serious offence or national interest or appears to relate' to performance of those other persons duties'. Similarly ASIO can communicate information to ASIS, ASD and AGO under s 18(4A) if it appears to relate to the performance of ASIS, ASD or AGO's functions. The Agency is also permitted to communicate information with other authorities and countries if it is cooperating with them as required by s 19 and s 19A. These permissions are subject to restrictions in the *Telecommunications (Interception and Access) Act 1979*; in particular, fulfilment of requirements under s 11A, telecommunications service warrant for collection of foreign intelligence; s 11B named person warrant for collection of foreign intelligence , and s11C foreign communications warrant for collection of foreign intelligence.

---

[281] See for example *Rules to Protect the Privacy of Australians*, as issued for ASIS <https://www.asis.gov.au/Privacy-rules.html> Rule 5.1: "ASIS is to take reasonable steps to ensure that intelligence information that ASIS retains or communicates concerning Australian persons is recorded or reported in a fair and reasonable manner.

Similarly, the *Intelligence Services Act 2001* s 11(2AA) allows ASIS, AGO and ASD to 'communicate incidentally obtained intelligence to appropriate Commonwealth or State authorities or to authorities of other countries[282] if the intelligence relates to the involvement, or likely involvement, by a person in certain activities.'[283] These agencies can also obtain intelligence and communicate it if it is relevant to serious crime to law enforcement agencies.[284]

The consequences for disclosure outside the listed exceptions are severe. Disclosure of information by an ASIO officer outside the listed exceptions and without the approval of the Director-General or a person authorised by the Director-General to give such an approval constitutes a serious offence under s 18(2) with a penalty of 10 years imprisonment. The same penalty applies for unauthorised communication of certain kinds of information under the *Intelligence Services Act 2001*.[285]

3.2.8. Controls on communication of intelligence concerning persons

There is a complex range of controls on communication of intelligence information about persons, and collecting, accessing or disclosing information for intelligence purposes. The Parliamentary Joint Committee on Law Enforcement[286] provides examples of statutory controls on communication of information concerning persons. These create a matrix of overlapping requirements that apply to different organisations in different ways.

---

[282] Approved under Intelligence Services Act 2001 s 13(1)(c).

[283] The activities listed in *Intelligence Services Act 2001* s 11(2AA) include: '(a) activities that present a significant risk to a person's safety; (b) acting for, or on behalf of, a foreign power; (c) activities that are a threat to security; (d) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the Customs (Prohibited Exports) Regulations 1958); (e) committing a serious crime.'

[284] Intelligence Services Act 2001 s 11 (2)(c).

[285] *Intelligence Services Act 2001*, s 39 (ASIS); s 39A (AGO); s 40 (ASD). Other offences include unauthorised dealing with records with penalty of 3 year imprisonment: *ASIO Act 1970*, s 18A(1) and *Intelligence Services Act 2001* 40C (ASIS); s 40E (AGO); s 40G (ASD).

[286] Parliamentary Joint Committee on Law Enforcement, 'Challenges to an Australian Criminal Intelligence Model', Chapter 6 in *Inquiry into the Gathering and Use of Criminal Intelligence by the Australian Crime Commission*, 15 May 2013, answer to Question 8 by ACC <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Completed_inquiries/2010-13/criminal_intelligence/report/c06>.

Table 3-1: Legislation affecting disclosure

Agency	Examples of legislation impacting on disclosure or 'sharing'
AFP / ACT Policing	1. s 60A *Australian Federal Police Act 1979* (Cth) 2. *Surveillance Devices Act 2004* (Cth) 3. *Telecommunications (Interception and Access) Act 1979* (Cth) 4. *Freedom of Information Act 1982* (Cth) 5. *Privacy Act 1988* (Cth)
State & Territory Police Forces	1. Individual State and Territory legislation 2. *Surveillance Devices Act 2004* (Cth) 3. *Telecommunications (Interception and Access) Act 1979* (Cth) 4. *Freedom of Information Act 1982* (Cth) 5. *Privacy Act 1988* (Cth)
ASIO	Section 17(b) and 18(3) of the *ASIO Act* are the most commonly used provisions for the communication of information to Commonwealth and state/territory law enforcement agencies
ASIC	s 127 of the *ASIC Act*
ACC	s 51 – Secrecy provisions s. 12 – for the purpose of referring a brief of evidence or POCA action ss 59(7), 59(8), 59(9), 59(11) provide the standard mechanism for sharing information with LEA, FLEA and Government agencies. s 59AA provides mechanisms to disseminate to other sectors
Australian Customs & Border Protection Service	s 16 *Customs Administration Act 1985*
ATO	ss 355-70(1)(Item 1) specifies that disclosures can be made to an authorised law enforcement agency officer, or a court or tribunal, for the purposes of: • investigating a serious offence, or • enforcing a law (the contravention of which is a serious offence), and/or • for making a (possible) proceeds of crime order. (Note: s 355-65(8) (table 7 item 2) provides details for releases to Australian Customs & Border Protection Service)

Disclosure to foreign agencies

As discussed in 3.1.4, a variety of agreements and mechanism also allow Australian agencies to access data held by foreign counterparts and to disclose data to them. Each of these mechanisms is subject to their own control mechanisms. The question of the weight to be given to the nationality or residence of data subjects, and what impact this has on any controls over dealings with their information, is relevant to the assessment of the proportionality of such dealings.

From an agency perspective 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'.[287]

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

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

information. Similar to APP 6, there are exceptions contained in APP 8.2 that support the disclosure of information for enforcement related activities.

There have been moves in the US and Europe to reconsider the applicability of privacy and related rights to persons associated with certain other countries or regions but it is unclear what impact these will have.[288]

The question of limiting controls based on location in a particular country may be of interest to the future of DIO Guidelines and similar protections for the sole benefit of 'Australian persons'.

3.2.9. Controls on Data Retention and Destruction

Keeping records or data indefinitely and without an identified purpose, while potentially appealing as Big Data,[289] can often be associated with ongoing costs and risks, and may deliver marginal benefit out of proportion with those costs and risks.[290] This section looks to examples in the telecommunications domain to help explore issues around record and data retention and destruction. (3.6 later in this chapter also considers related issues under the *Archives Act*.)

Decisions to which a proportionality test applies potentially include such retention and destruction decisions.

---

[288] This was a critical factor in the *Schrems* case, Court of Justice of the European Union (CJEU), *Maximillian Schrems v Data Protection Commissioner,* Request for a preliminary ruling from the High Court (Ireland), C-362/14, 6 October 2015 <http://curia.europa.eu/juris/document/document.jsf?>. text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=712511>. The long term implications of this case are not yet clear. In the US, 'the *Judicial Redress Act of 2015* (HR 1428) would strengthen partnerships with our allies and ensure continued law enforcement cooperation between the United States and Europe by giving covered foreign citizens the ability to seek judicial redress in U.S. courts to ensure that their privacy is protected.' Judiciary Committee 'Goodlatte, Sensenbrenner And Conyers Praise House Passage Of Legislation To Strengthen Privacy Protections For Individuals,' blog, US House of Representatives, 20 October 2015 <http://judiciary.house.gov/index.cfm/2015/10/goodlatte-sensenbrenner-and-conyers-praise-house-passage-of-legislation-to-strengthen-privacy-protections-for-individuals>. See also Glynn Moody, 'Microsoft wants US government to obey EU privacy laws,' *Ars Technica*, 21 October 2015 <http://arstechnica.com/tech-policy/2015/10/microsoft-wants-us-government-to-obey-eu-privacy-laws/>. In addition, in early 2016 a 'Privacy Shield' was announced to replace the Safe Harbor scheme for legalising otherwise unlawful transatlantic data transfers. See US Department of Commerce, 'Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework', 29 February 2016 <https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu-us_privacy_shield_fact_sheet.pdf>.

[289] See for example 7.4.5N.

[290] See for examples considerations outlined in ISO, *ISO/IEC 27001 - Information security management*, 2013 <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>. While the cost of storage per bit is reducing, volume of data is increasing, and many costs are indirect, like addressing security concerns, so there is likely to remain significant cost. While risk may reduce in the far future as matters recede into history, there remains potential risk over many decades.

Retention or preservation controls

Data retention requirements have been imposed for some telecommunications data. The *Telecommunications (Interception and Access) Act 1979* s 187AA, requires certain classes of carriers and carriage service providers to retain a set of telecommunications data.[291]

Telecommunications Act 1997 s 313(3) and (4) require preservation or retention of certain telecommunications information on request for law enforcement, national security and related purposes. It is unclear if there is any duration contemplated; there is none specified.

The vague requirement on telecommunications providers in *Telecommunications Act 1997* s 313(1) to 'do their best' to prevent the commission of offences using the telecommunications network could also conceivably be used as a basis for data retention. However, the data retention scheme under the amendments to *Telecommunications (Interception and Access) Act* has superseded such a need.

Data destruction or deletion controls

The issue of controls over deletion is significant because of the large volumes of data collected and used by Big Data operations. Large caches of sensitive or valuable data may become 'honeypots' attracting unwelcome interest from many sources. Unnecessary retention may thus result in unreasonable risk.

The recent telecommunications data retention amendment requires retention for a period, typically 24 months, but thereafter permits (although does not require) destruction by the private hosts.[292] APP 11, however, requires entities to destroy or de-identify personal information no longer required for any purpose permissible under the APPs where the entity is not required by any other law or court or tribunal order to retain the information. This requirement applies to all telecommunications data which service providers are required to retain under the *Telecommunications (Interception and Access) Act 1979.*

Controls on record, information or data deletion or destruction are likely to be contained in record keeping obligations of agencies and other entities. Deletion has long been a part of information governance policies, although it may not be applied or enforced uniformly.[293] As well as practical re-use of resources, one reason for deletion is that security is improved by not retaining information when it is no longer needed for its original purpose, especially if there are any potential sensitive or risk aspects in its continued existence. This is reflected in *ASIO Act 1979* (Cth) ss 31 and 34ZL, which require destruction of records created or obtained under a warrant.

In some cases, it may be possible to seek consent from individuals to use personal information for analytics purposes on an ongoing basis, for example by having privacy policies and collection statements under APPs which make clear the kind of uses or disclosures that will occur, and the length of time for which the data will be retained. Though more relevant for entities that collect personal information directly from individuals

---

[291] See *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) s 187AA, which lists data categories by broad function rather than particular description, leaving some uncertainty about inclusion or exclusion of the evolving data items involved in telecommunications and Internet use.

[292] s 187C *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth).

[293] Julian Gillespie, Patrick Fair, Adrian Lawrence and David Vaile, *Coping when everything is digital: Digital Documents and Issues in Document Retention*, Cyberspace Law and Policy Centre (UNSW, 2004) 8.

rather than law enforcement or security agencies obtaining personal information through other means, it could extend to law enforcement or security uses or disclosures.

Obligations regarding deletion and destruction of records for *Archives Act* purposes are discussed in 3.6.

No longer 'necessary' for a purpose

One criterion appearing in several provisions requires revocation or undertakings to delete when certain records or information is 'no longer required' for the purpose which enlivened their collection or use.[294] There may be scope for ambiguity around the issue of 'purpose' in the context of 'Big Data' paradigms.[295] The assumption behind some approaches to data mining is that data can yield useful insights that may not be foreseeable in advance. Thus data may only have a general purpose in data mining, without a specific purpose known in advance. Further, historic data can be useful for solving older cases and drawing links between historic and current cases (2.2.2F), so that data retention will always have some unknown potential at any point in time.

It is not clear whether the possibility of data mining in future means that data will always be 'necessary for a purpose'. Statutory provisions addressing this include the *Australian Privacy Principles*,[296] which base justification for use and disclosure on necessity for the purpose of collection or for closely related purposes.[297]

Observations

If the question of deletion when not necessary for a relevant purpose is dealt with explicitly, this can avoid generalisations, assumptions or technical affordances having greater influence than is appropriate. Risks associated with retention when it no longer serves the original purpose may increase over time, including risk of security breach, the decrease of accuracy, currency, completeness or relevance over time, and also the potential for other entities to be attracted to the 'honeypot' to seek access for unrelated (and perhaps unjustified) purposes. The scale of these ongoing risks may become disproportionate to the benefits associated with retention of certain classes of records or data past a particular date. There may be other reasons for setting tight and strict deletion parameters, including the need for auditing and transparency.

These considerations appear to be lacking from the general formulations of data controls and proportionality tests at present. Two research participants (2.5.4 'Deletion of data') proposed creating a better data deletion program. The argument is strengthened by the fact that deletion programs are common in the traditional realm of archives administration, which is discussed in 3.6, and in other IT disciplines.

Their absence may also warrant a review of the factors supporting deletion from first principles, if these principles are not well appreciated among policy makers and designers in the emerging Big Data context.

---

[294] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 142A, 180, 180B, 180E.

[295] See also 2.6.1E-H.

[296] *Privacy Act 1988* (Cth) Schedule 1.

[297] The basis for data protection under the OECD model implemented in privacy laws in Australia and many other developed countries, though not the US, is this concern with permitting uses related to the original purpose, but restricting re-use for other unrelated purposes. The policy aims include restraint on the creation of open-ended data systems maintained without reference to any particular purpose.

Concluding observations

Given that Agencies are required to co-operate in collecting and disclosing data, it would be helpful for the proportionality assessment approach to be articulated and harmonised across all law enforcement and national security organisations. Developing a rigorous general framework that could be adapted for decision-makers at different levels could enable incorporation of more specific considerations relevant to particular conditions, and thus minimise the risk of formulaic application.

Additionally, the test would need to reflect clearly stated rights or interests that may be affected by the proposed action (trespass, privacy, natural justice), reasonable costs, and evidence of effective alternatives. In each test, the effectiveness of the proposed measures need also form one of the considerations.

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

The third line of inquiry focuses on some of the attributes of the existing Australian laws and regulations relevant to Big Data and national security. It responds to the third Lens item by considering whether the framework is expressed in clear, principle-based and consistent legal rules that provide officials with appropriate guidance to take reasonable decisions and perform their functions correctly and efficiently in a dynamic environment.

We consider clarity and consistency first (8.3.1), and then consider the potential tension between clarity and the flexibility required in a dynamic data environment (8.3.2), including observations about the circumstances in which technological neutrality is desirable.

3.3.1. Principle-based consistent rules

The access and control framework as described in 3.1 and 3.2 is complex. It was not possible to determine in this study whether these 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 IGIS and other independent oversight bodies provide a measure of comfort that compliance levels are high.[298] By implication it would therefore be reasonable to assume that the internal policies and operational rules are sufficiently clear 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.[299] In particular, some research participants observed that differing 'interpretations' could be an excuse to avoid sharing data, for example based on a preference for control or ownership of agency data sets (2.2.1 H-K). Differing interpretations may indicate that some aspects of the legal rules could be expressed more clearly.

In our view, the principles underlying the rules should be as consistent as possible across both data sets and agencies. While the subject matter is too complex and the nature and focus of the agencies too diverse to apply consistent rules across the board, it is desirable that the rules be based on consistent principles or policy. This view was also expressed by some research participants in 2.4.5.

The groupings of agencies for purposes of specific powers, especially relating to access to data, also differs. As discussed in 3.1*,* the regulatory framework is to some extent agency-

[298] See section 3.6 below.
[299] See 7.2.

specific and dataset-specific, with different rules, factors or definitions applying in different contexts. Agency and data-set specific rules assist in tailoring regulation to a particular context and that is important from a proportionality and effectiveness perspective. That approach, however, also complicates the development of consistent and coherent rules across the larger domain.

Agencies are often grouped in categories in different laws, possibly to facilitate a measure of consistency. Key categories include:

- Law enforcement agencies (potentially including non-criminal agencies)
- Criminal law enforcement agencies
- Security or national security agencies; intelligence or security agencies
- Interception agencies
- Integrity bodies
- Other agencies that may work closely and facilitate one of the above, or oversee it.

The assignment of an agency to such a category differ among the laws, thereby undermining consistency benefits that may flow from categorisations.

Table 3-2: Examples of agency categories in the current framework

Category and Act	Agencies
'agency' *IS Act* s 3	ASIS, AGO, ASD [omits ASIO, ONA, and DIO. Not extensible without amendment?]
'agency' *TIAA Act* s 5(1)	(a) except Ch 2 -- interception agency or enforcement agency (b) Ch 2 -- interception agency. *[excludes LEAs in latter]*
'Intelligence or security agency' *ASIO Act* s 4	ASIS, ONA, AGO, DIO, ASD [No ASIO; it is 'the Organisation.' Not extensible?]
'Law enforcement or security agency' *INSLM Act* s 4 *[List, extend by regulation]*	AFP, ACC, Customs [now DCBP], ASIO, ASIS, ADF, AGO, DIO, ASD, ONA, A police force of a State or Territory Another agency prescribed by Regulations
'law enforcement agency' *ACC Act* s 4 [no def. 'law enforcement']	AFP; Police Force of a State ; or authority or person responsible for enforcement of laws of Commonwealth or of States [extend by responsibility]
'law enforcement agency' ASIO Act s 4 [no def. 'law enforcement']	'an authority of the Commonwealth, or an authority of a State, that has *functions* relating to law enforcement ' [Not listed, defined by function. Extend by function]
'law-enforcement agency' TIAA Act s 5(1) [Prescribed list plus extensible by both function and regulation]	AFP, ACC, ACLEI, DIBP, CC, ICAC NSW, ICAC SA, IBAC, PIC, CMC, CCC Q, CrimTrac*[not CCC WA][300] A Police Force of a State [not Territory, as in INSLMA] Body responsible to Min. Council for Police & Emergency Mgt* An authority under Cth, State or Territory law prescribed by Regs A body whose *functions* include administering: (i) a law imposing a pecuniary penalty* (ii) a law relating to protection of public revenue.*
'criminal law-enforcement agency' *TIAA Act* s 5(1)	Agencies in paragraphs (a) to (k) of definition of 'enforcement agency' above.

300 Those marked with an asterisk in this cell are not a '*Criminal* LEA' in the TIAA s 5 or s 110A retention definition in the cells below.

Category and Act	Agencies
'criminal law‑enforcement agency' TIAA s 110A (data retention access) [By prescribed list + extensible by declaration.]	AFP, ACC, ACLEI, ACBPS/DIBP, CC, CMC, CCC Q, CCC WA, IBAC, ICAC NSW, ICAC SA, PIC, ASIC,*[301] ACCC* *[no CrimTrac, CMC]* A Police Force of a State *[not Territory, as in INSLMA]* Authority or body in a declaration under s 110A(3)
'authorities of Cth and States and Territories' *TA 1997* ss 313(3) and (4) *[Agencies not specified; extend by function]*	Not defined. Constrained by functions for which help to be given: (c) enforcing criminal law, and laws imposing pecuniary penalties; (ca) assisting enforcement of criminal laws in a foreign country; (d) protecting the public revenue; (e) safeguarding national security.
'interception agency' TIAA Act s 5(1) [three definitions, ASIO in one only; state agency also needs declaration in two.]	(a) except s 6R, Part 2-6 or Chapter 5: a Cth agency [AFP, ACLEI and ACC]; or eligible authority of a State [state police, CC, ICAC, PIC and inspectors, IBAC and inspectorate, CCC and inspector, ICAC SA] with a s 34 declaration in force (b) for Part 2-6: a Cth agency; or eligible authority of a State (c) for s 6R and Chapter 5: ASIO; a Cth agency; or eligible authority of a State with a s 34 declaration in force
'security authority' *TIAA Act* s 5(1) *[By function]*	Cth authority (undefined) with *functions* primarily relating to: security; collection of foreign intelligence; defence of Australia; or conduct of the Commonwealth's international affairs.

Observation

It is not clear that an obvious or consistent rule governs the categorisation of an agency as either a 'national security agency' or a 'law enforcement agency' in the relevant laws.[302] Where powers are linked to categories of agencies, a lack of consistency in this form of categorisation impacts on consistency across different laws.

Another general obstacle to greater consistency is the inconsistent use of terminology. In particular, as an article by members of the research team explains,[303] there are diverse meanings ascribed to concepts such as 'data', 'information', 'communication/electronic communication', 'document', and 'record' in various Acts.[304]

In addition to a measure of internal consistency in laws, there are also examples of attempts to ensure a consistent approach reaching beyond agencies and specific laws.

The *Australian Privacy Principles* (APPs) provide an important example of a set of principles that apply broadly. They do not apply to national intelligence agencies, but some agencies have their own sets of privacy principles that acknowledge some provisions from the APPs.

---

301 Those marked with an asterisk in this cell are not CLEAs in s 5(1), and were not in the Bill.
302 In some cases, for example there is an explicit reference to a *criminal* 'enforcement agency'. In other cases this qualifier is absent, and a much broader range of enforcement responsibilities may also be involved, for example in relation to enforcement of non-criminal regulatory laws. The difference is however not necessarily maintained consistently. ASIC and ACCC were included in the TIAA s 110A retention list as criminal law enforcement, but not in s 5.
303 Danuta Mendelson et al, 'The Absence of Clarity', forthcoming.
304 Although in 2.1.3, an operations person says that 'Increasingly there is less of a distinction between data and information. It can be one and the same at the same time. … Increasingly, all will be viewed as data, whether structured or unstructured. … We provide narrative reports and data products that contribute to intelligence operations. They can be narrative or a graph or a network chart.'

There are, however, agencies such as the ACC that neither have to comply with the APPs nor have their own equivalent principles, and other agencies have 'Privacy Rules' that with few links to the APPs.[305]

The Australian Government Information Security Management Protocol (discussed in 3.5 below) provides another example of principles that apply broadly in relation to the data relevant to Big Data, national security and law enforcement. It promotes a consistent approach to information security across all Australian Government, State and Territory agencies and bodies

3.3.2. Clarity and flexibility

Reviews in recent years have received submissions, typically from agencies, about complexity in various aspects of the rules.[306] A key issue is whether the complexity is necessary and appropriate. In some cases 'complexity' seen by agencies as an unwelcome impediment may have benefits, such as ensuring that a diversity of scenarios are regulated appropriately, or ensuring that compliance can be easily checked and audited. Assessment of the appropriate balance between these desirable characteristics of rules often requires independent perspectives, such as Parliamentary review committees or external reports by law reform or governance level bodies.

Another challenge for the design of rules in this area is the tendency of the underlying data storage and analytic technologies to continue to evolve. This forces a decision as to whether laws should be optimised for current data sets and analytic possibilities, or whether language used should abstract away from specifics in order to 'future proof' the provisions, ensuring their continued appropriateness as data types and technologies change. As was the case when clarity and precision compete, there are no clear or easy answers to the desirability of 'technological neutrality' in legislation. In some contexts, language should be more abstract to avoid the need to constantly revise legislation as practices and technologies evolve. In other contexts technological specificity can enhance clarity and ensure that a rule aligns with a technology-specific objective.

For instance, the provisions of the TIAA are generally framed as 'neutral' as they fit the relevant information into one of two categories:

---

[305] See ASIS, ASD and DIO Privacy Rules.

[306] While clarity of rules is desirable for its own sake, there are situations where it can only be done if other drafting goals, such as precision or auditability are met. See Colin Divers, 'The Optimal Precision of Administrative Rules' (1983) 93 *Yale Law Journal* 65. Complex subject matter and complex contending interests may require more complex rules if policy objectives are not to be sacrificed. For example, there may be good reasons to treat a national security agency such as ASIO differently from a law enforcement agency such as the AFP, and this may require that provisions be duplicated with modifications as they apply to each agency. Duplication, for example, may be viewed as complicating a statutory text, but can also be viewed as simplification of complex rules that apply differently to different agencies or different functions. '… there is intentional duplication for provisions that apply specifically to ASIO with separate provisions for enforcement agencies. For example, voluntary disclosure provisions for ASIO are covered under section 174 whereas section 177 relate[s] to enforcement agencies. ASIO supports the recommendation to remove legislative duplication but notes it should not be applied in instances where there is a necessary distinction between ASIO's security intelligence role and law enforcement agencies.' Australian Security Intelligence Organisation, *ASIO Submission to the Senate inquiry into a comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, 34, quoted in Senate Standing Committee on Legal and Constitutional Affairs, *Report of the Inquiry into the Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979*, 24 March 2015.

- ‘content and substance of a communication’ (which requires a warrant) and
- ‘telecommunications data’ (which requires only an authorisation).

However this general distinction becomes very complex in the data retention amendments, which have been criticised as being too vague or uncertain in their application to specific data items to interpret realistically for a technical compliance purpose.[307]

Observations

While perfect clarity, consistency or longevity of rules is not possible, there are improvements that can be made. Legislation should use consistent terminology, particularly as to basic terms such as ‘data’, ‘information’, ‘communication’, ‘electronic communication’, ‘document’, and ‘record’.

In addition, a focus on principles (as in privacy) and standards (as in information security) are also helpful in enhancing consistency while maintaining flexibility across contexts.

That said, this is a complex field and the technological developments may increase complexity, especially in the medium term. In addition, the requirements of compliance and technical translation of concepts may mean that ‘neutral’ language creates more difficulties with application than it solves, especially if it is based on once-rigid categories which now become blurred, such as the distinction between ‘content’ and ‘metadata,’ which was quite clear for analogue telephone calls but much less so for emerging technologies.

3.4. Is integrity of data and analysis supported?

The fourth line of inquiry addresses the need for data quality and integrity as well the integrity of the inferences drawn from data through analysis and employed in decision-taking. This section considers current rules that would support the integrity of data collected, retained and accessed by government for law enforcement and national security purposes, and the integrity of analytical and decision-making uses of such data and systems.

At the most basic level, integrity of data and information in this field requires retaining metadata about its provenance. This means retaining information on its source, the probability that it contains errors including as to attribution (and the confidence in that figure), its timeliness, and its completeness.[308] The analysis conducted on the data should preserve such provenance information as is relevant to assessing the confidence that can be placed in any resulting inference drawn or prediction made.

Integrity and security are closely related but separate matters. The core government data security related documents such as the *Protective Security Policy Framework*, the *Information Security Manual* and the ASD *Cloud Computing Security* advisories (discussed in 3.5), each contain elements referring to data integrity. Data integrity and availability is

[307] Internet Society of Australia, ‘The Data Retention Bill: A threat to civil rights protections that just won’t work!’ media release, 22 January 2015) <http://www2.isoc-au.org.au/Media/InternetSociety_DataRetentionBill_20150122.pdf>.

[308] There are domain-specific refinements of more general dimensions of information integrity in data systems. For instance the Australian National Audit Office used the term ‘data integrity’ to refer to ‘the consistency, accuracy and reliability of information across [client] records’. See Australian National Audit Office, *Audit Report No.28 2008–09: Quality and Integrity of the Department of Veterans' Affairs Income Support Records* (2009) 94.

treated as a core goal of such security measures. This discussion focuses on the integrity of data while the data security aspects are considered in 3.5.[309]

3.4.1. Data integrity generally

Data integrity is a central concern of Big Data systems, as well as smaller systems delivering critical support for important functions. Data integrity and measures to ensure integrity are important factors impacting on user confidence in the system and on public trust.

Government entities are compelled by general management laws such as the *Public Governance, Performance and Accountability Act 2013* and general management principles 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, as required by the specific or general laws governing the entities. Appropriate data capture processes, secure retention of data and regular updating of information and data matching[310] are methods employed by government entities to ensure data integrity. Data integrity is also considered by the See Australian National Audit Office [ANAO] in their performance audit reports.[311] An example of the appreciations of the impact of data that lack integrity on the functioning of an agency is found in the *Intelligence Services Act 2001* (Cth). Section 3 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.'

The *Privacy Act 1988*, applying to government and private entities, also includes concrete formulations of principles governing data integrity many of which are well-entrenched globally.[312] Australian Privacy Principle 10 (Quality of Personal Information), for example, addresses data integrity as follows:[313]

---

[309] 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>.

[310] See topic in 3.2 Controls, above.

[311] 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> 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>?]

[312] 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.

[313] These should be considered as almost inevitable rather than an anomaly, given the nature of large scale data systems. As opposed to using provisions for internal reporting under such laws as *Public Interest Disclosures Act 1994* (NSW) <http://www.legislation.nsw.gov.au/maintop/view/inforce/act+92+1994+cd+0+N>, *Protected Disclosure Act 2012 (*Vic) <http://www.austlii.edu.au/au/legis/vic/consol_act/pda2012233/>.

> 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.

Law enforcement or national security agencies are exempt from many aspects of the *Privacy Act* as discussed above in 3.2, and this principle may not apply to them to the same extent. For example, in the Privacy Rules applying to ASIS the integrity principle is captured as follows in Rule 5 (Accuracy of information):

> 5.1 ASIS is to take reasonable steps to ensure that intelligence information that ASIS retains or communicates concerning Australian persons is recorded or reported in a fair and reasonable manner.[314]

Recording and reporting retained or communicated intelligence information 'in a fair and reasonable manner' is more general than 'accurate, up-to-date, complete and relevant' as required by the *Australian Privacy Principles*.

Government policy and standards are also relevant to data integrity. The Australian Government Big Data Strategy is a recent and pertinent model which includes among its six principles, 'Principle 3: Data integrity and the transparency of processes'. The notion of 'integrity' is embedded as a feature of the project, its governance and of the data *per se*:

- Agencies are encouraged to conduct Privacy Impact Assessments (PIA) for any new big data projects and publish these PIAs (or modified versions if necessary).
- Each party to a big data analytics project must be aware of, and abide by their responsibilities regarding: the provision of source data and the obligation to establish and maintain adequate controls over the use of personal or other sensitive data they are entrusted with; and/or the management of the project from start to finish and the obligation for its sound conduct, in line with the agreed requirements of the responsible agencies.
- These processes will help to strengthen the integrity of big data analytics projects and help to maintain the public's confidence in the Government's stewardship of data.[315]

3.4.2. Considering data integrity in intelligence decisions

Judging integrity of information is part of the art and science of intelligence, and will be an important aspect of any Big Data application in this context, especially as the assessment of the integrity and reliability of intelligence is a challenging function to automate.

The ACC is a key source of information and expertise in criminal intelligence, and their experience is helpful to understand existing measures to assist data and interpretive integrity. The ACC's CEO, John Lawler, was asked, in relation to the integrity of intelligence, 'if it is subsequently determined that that information is incorrect, how do you pull it back out again?' and explained the Admiralty Scale, a process for identifying and dealing with variable reliability.

---

[314] There are extensive provisions about information use in Evidence Acts, Rules of Court and other laws. See Attorney-General's Department, *Independent Reviewer of Adverse Security Assessments* <http://www.ag.gov.au/asareview>.

[315] Ben Saul, 'The Kafka-esque Case of Sheikh Mansour Leghaei,' (2010) 33(3) *UNSW Law Journal* 630. *Big Data Strategy - Improved Understanding through Enhanced Data-Analytics Capability* (2013) 21 <http://www.finance.gov.au/big-data>.

Mr Lawler**:** What we deal with is intelligence, and intelligence is assessed on the so-called admiralty scale. … this is a globally recognised process for assessing information and determining its likely veracity. Some intelligence will be A1 in that it can be corroborated, it might be sworn testimony and it might have very high levels of authenticity and reliability. Then other information that might come from a single source that is unknown will be of a much lower quality and be much less reliable, and we are likely to have everything in between that.

The purpose of the intelligence process is to use that information and build upon it so that it produces an assessment or a judgement—a professional judgement—undertaken by professional intelligence analysts that goes to inform. … it is not a matter of absolute truthfulness or absolute inaccuracy. These are assessments that are made based on a variety of … information by professional people to say in our professional judgement we think X or Y.[316]

The Admiralty code is an intelligence assessment tool widely used globally and in Australia. The code 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.)[317]

The ACC in a related inquiry described the critical third stage in an investigation, 'Analyse and Produce', in the following terms:

Intelligence analysts use a variety of techniques as part of the intelligence analysis methodology as they are dealing with incomplete, ambiguous and sometimes deceptive information. The analysts applied structured analytic techniques to bring a systematic, transparent and accountable process to their critical thinking and problem solving capabilities. Such structured analytic techniques may include a key assumptions check; structured brainstorming;[318] scenarios and indicators; analysis of competing hypotheses; What If? Analysis; assessment of cause and effect; timeline and chronology analysis; and link network analysis. A combination of techniques can also be used as appropriate ...[319]

These techniques help to deal with data integrity in traditional settings. However, for reasons outlined in the observations below, translating this 'human intelligence' into a Big Data system offers a serious challenges that will require appropriate control measures. Such measures are not currently evident in the statutory framework.

---

316 Parliamentary Joint Committee on Law Enforcement (PJCLE)*, Inquiry into the gathering and use of criminal intelligence*, 23 and 28 October 2014 <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Completed_inquiries/2010-13/criminal_intelligence/report/index>; Hansard of 21 September 2012.
317 John Joseph and Jeff Corkill Information evaluation: how one group of intelligence analysts go about the task Proceedings of the 4th Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 5th–7th December <2011 http://ro.ecu.edu.au/asi/20>.
318 See <http://www.pennassoc.com/blog/files/Common-Core-Analysis-Techniques-Part-1.php>.
319 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>.

The role of the data subject

As noted at 3.2.3, provisions enabling the data subject to request a review of an intelligence decision, including the data that was considered in such a process are included in the *ASIO Act.* It enables limited review of formal assessments, for instance by applying under s 54 to the Tribunal for the review of an adverse or qualified security assessment, or through the involvement of the Independent Reviewer of Adverse Security Assessments[320] reporting to the Director-General of Security in immigration refugee contexts.[321] Such provisions are not effective in cases where the data subject is unaware of the negative assessment.

Observations

Data integrity is not extensively regulated in Australia, at least as far as public sources reveal, and it is not clear whether there is a consistent concept of 'data integrity' between agencies.

The *Australian Privacy Principles* formulate a general integrity standard of 'having regard to the purpose of the use or disclosure, [being] accurate, up-to-date, complete and relevant,' but its mandatory use is confined to the scope of application of the Principles, thus excluding many agencies of interest to this study. A clear concept of 'data integrity' will facilitate the incorporation of different data sets into a Big Data system.

Big Data tools and culture are well known for their capacity to accept data which is less reliable, complete, accurate, up to date or relevant than usually required for data systems. But while the tools may deliver output from low integrity input or unverifiable assumptions, and preserving provenance may allow for humans to give less weight to poor quality data,[322] the integrity of the outcome remains uncertain until the Big Data system is fully implemented and regularly tested.

Law enforcement processes producing criminal evidence is guided by the rigour that accompanies testing in an adversarial, open court process with strict rules of admissibility, relevance and probative value.[323] Criminal and national intelligence processes, on the other hand, necessarily rely on less rigorously tested and verified information. As is appropriate to the nature of their task, accepted standards of 'proof' or probative value are typically below the standard of 'beyond reasonable doubt'. In addition, these processes are often necessarily secret and citizens who may suffer negative consequences as a result of incorrect data do not have the opportunity to challenge or correct the data. While this is a necessary feature of the terrain, and of necessity less reliable information has to be utilised, the use of Big Data models for decisions which have impacts on individuals without the rigorous testing of a court process raise questions about how to set the appropriate standards and expectations of integrity, probative value and relevance.

---

[320] See Attorney-General's Department, *Independent Reviewer of Adverse Security Assessments* <http://www.ag.gov.au/asareview>.
[321] Ben Saul, 'The Kafka-esque Case of Sheikh Mansour Leghaei,' (2010) 33(3) *UNSW Law Journal* 630.
[322] See eg 2.5.5AL.
[323] There are extensive provisions about information use in Evidence Acts, Rules of Court and other laws.

Intelligence analysts are skilled to deal with data that has differing levels of integrity. Action may be taken on lower quality data where a significant national security breach may be pending. Where, however, there is a less compelling or serious harm involved, making decisions affecting individuals on lower quality information may be disproportionately adverse.[324]

Legal rules do not currently regulate such intelligence decisions but clearer rules may be required for Big Data systems to ensure that uncertainty is preserved so the inferences/predictions can be given estimates of truth in line with the provenance of the underlying data. This may be consistent with the current rules (which are beyond the scope of the report).

Big Data tools, more than other intelligence methods, may be used in situations far removed from the source of the information on which they depend, the knowledge of those with actual experience of the source, and the consequences of decisions which they may suggest. One important aspect of integrity is to ensure that appropriate efforts are made to consider the logical and inferential reliability of the output as a basis for making decisions about individuals.

As noted in the literature review in chapter 2 of the Methodology Report, Big Data analytics, especially prediction of intrinsically uncertain future events, are typically based on statistical or algorithmic correlation, but legal consequences and the notion of responsibility is more often tied to causation. This potential divergence between analytical methods and a requirement of being able to attribute causal responsibility may restrain inappropriate interpretation of correlation. This is in particular so in cases where a decision could only be justified on the ground that causality is demonstrated (either because an individual is affected, or because it is assumed that a policy change will have a particular impact). No comprehensive provisions in statutory specifically address these challenges when they accompany automated intelligence analysis.

3.5. Are data and systems protected?

The fifth line of inquiry considers the rules that protect the security of relevant data and systems. Big Data systems may have a large surface of exposure, impact on more people, and have many facets which all need to be effectively protected, making security issues more challenging and more critical than for systems handling lower volumes of data. The challenges are enhanced where the system is intended to be accessed and used by a large number of individuals in different agencies and different geographic locations.

3.5.1. Security Requirements under Australian Law

A range of statutory provisions govern security of data.[325]

---

[324] This is an area where discussion of scope creep is relevant: acceptance of the need to use lower quality data in 'extreme' cases may lead to such use in less 'extreme' cases.

[325] 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

There are specific laws designed to promote data security. Law enforcement and national security agencies are required by statute to keep secure data pertaining to Australians, and unauthorised access to their information is prohibited.[326] Secrecy provisions apply to individuals dealing with information held in a data system, for instance *Crimes Act 1914* (Cth) Part VII,[327] and particularly s 79 and s 91.1 of the *Criminal Code* covering espionage and similar activities.[328]

In addition, 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 range of such offences, the most serious of which is knowingly, unauthorised access to data held in a computer with intent to use this access to facilitate a serious offence.[329] This offence applies where the restricted data is held in a Commonwealth computer or held on behalf of the Commonwealth. It also applies where the conduct is carried out by the means of a carriage service. There is also a lesser offence of intentionally and knowingly causing access to restricted data, where the restriction is 'by an access control system associated with a function of the computer'.[330] This would cover most attempts to 'hack' or bypass security for Big Data stores.[331] There are also relevant State and Territory equivalents of offences related to unauthorised access to computer data.[332]

---

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.

[326] *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.

[327] *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.

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

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

[330] CCA cl 478.1 'Unauthorised access to, or modification of, restricted data'.

[331] For State equivalents see NSW computer offences in *Crimes Act 1900* (NSW) Part 6, which includes s 308H Unauthorised access to or modification of restricted data held in computer. See also Victorian Crimes Act 1957 s 247G.

[332] 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.

These offences target access to data, not the use of the accessed data. Australian Privacy Principle 11 (Security of Personal Information) also addresses data security as follows:[333]

> '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.' [334]

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. Under the ASIS Privacy Rules, for example, there is an obligation to keep secure the data of Australians with a focus on reasonable precautions against loss, or unauthorised use or misuse.[335] These requirements are not prescriptive, and offer no benchmarks, standards or methods of confirmation of adequacy. Compared to the personal information security obligations under the *Privacy Act*, whose place they take, they offer little effective protection in the event of inappropriate use or failure of security.[336]

3.5.2. Security Standards and Best Practice

Clear, achievable security standards and models for best practice at the agency level appear to be crucial elements of a data security framework.

In one sense, Big Data is just a variant on other IT and data systems, and its security issues are not unique. However, many of the security challenges applicable to data systems and software platforms generally are exacerbated by the features of Big Data systems: there is more data at risk, the pathways from the outside world may be larger, the potential value of a successful intrusion may be higher, and especially relevant to this study, the involvement of large amounts of criminal and national security intelligence may add to the general level of security threat.

Protective Security Policy Framework

The AGD holds the responsibility for cyber security policy coordination on behalf of the Australian Government. Its Cyber Security Strategy envisages building a secure, resilient and trusted electronic operating environment that supports national security and maximises the

---

[333] *Privacy Act 1988* (Cth) Schedule 1.

[334] The Office of the Victorian Privacy Commissioner (OVPC) told the Cybercrime inquiry that the protection of information privacy and reduction of e-security risks are closely related concepts. House Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime,* [9.2], 21 June 2010 <http://www.aph.gov.au/parliamentary_Business/Committees/House_of_Representatives_Committees?url=coms/cybercrime/report/chapter9.htm>.

[335] '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.

[336] See in relation to the proposed laws mandating warnings about data breaches, Chris Duckett, 'Australian data breach notification laws will not be passed in 2015: Brandis, *ZDNet* (online), 13 October 2015 <http://www.zdnet.com/article/australian-data-breach-notification-laws-will-not-be-passed-in-2015-brandis/>.

benefits of the digital economy.[337] AGD also administers the Australian Government's *Protective Security Policy Framework*.

A 2014 *Directive on the Security of Government Business*[338] directs agency heads to apply the *Protective Security Policy Framework* (PSPF) and to promote protective security as part of their agency's culture. The PSPF addresses appropriate governance, personnel security, physical security and also information security. Although the PSPF is not legally prescribed, it supports statutory protective security requirements and reflects the aims and objectives of the Australian Government.

Agencies are required 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
- information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements
- information is classified and labelled as required [339]

The Protective Security Policy Framework embeds the following mandatory information security requirements:

---

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

[338] Issued by the Attorney-General on 21 October 2014 <https://www.protectivesecurity.gov.au/ExecutiveGuidance/Pages/Directive-on-the-security-of-Government-business.aspx>.

[339] *Australian Government Securing Government Business - Protective security guidance for executives* (2014 as amended in April 2015) [2.3].

Table 3-3: Protective Security Policy Framework requirements

Item	Requirement
INFOSEC 1	Agency heads must provide clear direction on information security through the development and implementation of an agency information security policy, and address agency information security requirements as part of the agency security plan.
INFOSEC 2	Each agency must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risks to the agency's information environment.
INFOSEC 3	Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats), which match their value, importance and sensitivity.
INFOSEC 4	Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' as detailed in the Australian Government Information Security Manual.
INFOSEC 5	Agencies must have in place control measures based on business owner requirements and assessed/accepted risks for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. Agency access control rules must be consistent with agency business requirements and information classification as well as legal obligations.
INFOSEC 6	Agencies must have in place security measures during all stages of ICT system development, as well as when new ICT systems are implemented into the operational environment. Such measures must match the assessed security risk of the information holdings contained within, or passing across, ICT networks, infrastructures and applications.
INFOSEC 7	Agencies must ensure that agency information security measures for all information processes, ICT systems and infrastructure adhere to any legislative or regulatory obligations under which the agency operates.

INFOSEC 2 (information security) requires agencies, among others, to document information security requirements in contracts, enter into MOUs when regularly 'sharing' (disclosing) information and make them public if possible, check and get necessary permissions before providing information to third parties and ensure that security and classification measures are in place.[340]

INFOSEC 5 (controlled access)[341] for example requires agencies to put in place a series of controls based on assessment under National e-Authentication Framework, requiring specific authorisation to access agency ICT systems including a unique identifier for each person. It also addresses the need for IT management policies, wireless access security, logging and monitoring of IT systems for security events, and risk assessments extending personal devices and storage. These requirements establish a framework within which national security and law enforcement agencies develop specific measures.

The PSPF is complemented by the Australian Government *Information Security Manual*.

Information Security Manual

The *Information Security Manual* (ISM), which in turn supports the guiding principles and strategic priorities government's *Cyber Security Strategy*, sets security standards for government ICT systems. Published by the ASD, it aims to assist Australian government

[340] 30, Australian Government, *Protective Security Policy Framework* (PSPF), v1.10, July 2015.
[341] Australian Government, *Protective Security Policy Framework* (PSPF), v1.10, July 2015, 32 <https://www.protectivesecurity.gov.au/ExecutiveGuidance/Pages/default.aspx>.

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 -.[342]

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.)[343]

ASD Cloud Computing Security guidance

The Australian Signals Directorate provides advice and assistance on information and communications security risks for Australian federal and state government agencies, in addition to its foreign signals intelligence role for the ADF. As government Big Data increasingly comes to rely on the cloud, ASD guidance on cloud security will be relevant for the potential overlap with law enforcement and national security uses, and may discourage its use for critical purposes.

A series of ASD Cyber Security Operations Centre (CSOC) *Protect Notices* set out security considerations[344] for agencies seeking to use cloud based resources, the most recent from the perspective of 'tenants' and cloud service providers.[345] They identify a range of risks (some general, some related to particular cloud delivery models as defined by the US National Institute of Standards and Technology), and list mitigation measures for each risk.

The tenant and provider documents focus on the use of cloud services for storing or processing sensitive data and highly sensitive data, requiring higher protection for highly sensitive data.[346] It defines 'sensitive data' for Australian government agencies and for the purposes of this document as data that is unclassified with a dissemination limiting marker (DLM) such as 'For Official Use Only' or 'Sensitive: Personal', aligning the latter with the definition of 'sensitive data' in the *Privacy Act 1988*[347] The Certified Cloud Services List (CCSL)

---

[342] *Information Security Manual* <http://www.asd.gov.au/infosec/ism/>.

[343] ASD, *Australian Government Information Security Manual – Controls* (2015) 318 <http://www.asd.gov.au/infosec/ism/index.htm>.

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

[345] 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>.

[346] Department of Defence, Australian Signals Directorate, ASD *Cloud Computing Security for Cloud Service Providers, April 2015 < https://asd.gov.au/publications/protect/cloud-security-providers.htm>. See for example Mitigation Reference Numbers 12 and 16.*

[347] 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 par 7: For Australian government agencies and for the purposes of this document: sensitive data is defined as data that is unclassified with a dissemination limiting marker (DLM) such as For Official Use Only (FOUO) or Sensitive: Personal (which aligns with the definition of sensitive information in the Privacy Act 1988); highly sensitive data is defined as data classified as PROTECTED." It therefore explicitly applies the *Privacy Act 1988* definition of 'sensitive information', which is defined in s 6 of that Act as: '(a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi)

of providers certified under this model are the only ones permitted to be used by Australian government agencies applying the *Information Security Manual*.

Observations

Sensitive information as defined in the *Privacy Act 1988* (unauthorised disclosure of which would typically impact individuals more than agencies) is given a lower classification rating, and thus is more likely to be hosted in cloud-based services. The classification scheme may suited to risks to agencies and official data, but the assumptions underlying this low level of protection for sensitive personal information warrant reconsideration.

The degree to which Big Data access, analysis or virtualisation methods could enable law enforcement and national security uses of data in a lightly protected cloud also warrants consideration. At what point does data being used for these purposes cease being assigned the classification it was originally given, before such more serious uses were enabled? The outcome of the analysis, and perhaps in some cases the data itself if it has been re-contextualised in place, may need reclassification.

The security risks do not appear to include appropriate consideration of a foreign entity being able to assert control over the data store, such as has arisen in the recent Microsoft Ireland case.[348] While data sovereignty is referred to in a link to the Department of Finance 'cloud' page, it may be more appropriate to address this directly in the guidance document.

ISO 27001 and related standards

Standards have an important role in formulating widely accepted models for assessing and responding to risks.

One relevant international standard for the security of information held in a data system is ISO/IEC 27001:2013, a specification for an information security management system. It addresses a framework of policies and procedures for the legal, physical and technical controls involved in an organisation's information risk management processes.[349] The 27001 standard does not mandate specific information security controls, but it provides a checklist of controls that should be considered in the accompanying code of practice, ISO/IEC 27002:2013, which describes comprehensive information security control objectives and generally accepted good practice security controls.

ISO 27001 should be taken into account in developing tailored security controls in this area, to the extent the issues it covers are not addressed in the more specific standards.

---

membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.'

[348] The US Department of Justice is asserting extraterritorial obligations regarding data about non-citizens held in another jurisdiction by a subsidiary of a US based firm. The dispute is not yet decided.

[349] ISO 27001 uses a top-down, risk-based approach and aims to be technology-neutral. The specification covers documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. See ISO, *ISO/IEC 27001 - Information security management*, 2013 <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.

State and Territory-level laws and standards

Binding data security and integrity standards were 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. Along with the *Information Privacy Act 2000*, the *CLEDS Act* was incorporated into the *Privacy and Data Protection Act 2014 (Vic*), which also provided the Victorian Commissioner for Privacy and Data Protection with the authority to develop a Victorian protective data security framework for monitoring and assuring the security of public sector data.[350]

This protective data security framework must be as consistent as possible with standards relating to information security (including international standards and the PSPF) prescribed for the purposes of the Act.[351] The Commissioner is empowered to issue standards that accord with the Victorian protective data security framework, for the security, confidentiality and integrity of public sector data and access to public sector data.[352] The Commissioner may also issue standards for the security and integrity of law enforcement data systems and crime statistics data systems as well as in relation to access to, and release of, law enforcement data and crime statistics data.[353]

Each of the other states and territories has its own non-legislative arrangements in this area, with varying levels of detail and compliance requirements.

Observations

Australia 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.

The framework is however not complete. The mandatory data breach notification law, which might enable regulators or those affected to take remedial and timely action, was expected to accompany the data retention regime. Such a notification regime is important as the personal information security risks posed by diverse 'honeypots' of privately-held telecommunications metadata may fall without remedy[354] on data subjects.

Despite some gaps, the *Protective Security Policy Framework* reflects dynamic mechanisms that seek to address risks as they arise in a coherent manner. The *Framework* provide an example of a system that could serve the dynamic and challenging legal and policy needs of Big Data solutions for national security purposes.

3.6. Is accountability maintained?

This section probes aspects of the Australian legal and policy framework to determine whether (1) access to data and data analysis and use decisions are tracked and audited for justification, security and intrusiveness, and (2) decisions are subject to appropriate internal governance as well as independent oversight and accountability.

---

[350] *Privacy and Data Protection Act 2014* (Vic) s 85(1).
[351] *Privacy and Data Protection Act 2014* (Vic) s 85(2).
[352] *Privacy and Data Protection Act 2014* (Vic) s 86(1).
[353] *Privacy and Data Protection Act 2014* (Vic) s 92(1).
[354] For instance, see s 315(5) and (6) *Telecommunications Act 1997* (Cth), which offers immunity from civil suit for providers who act in good faith. Individuals or businesses suffering from a security breach or other failure arising from this actions covered by the immunity are unable to recover.

These two aspects are intertwined. They are a useful starting point is to consider the role of the independent accountability structures that are relevant to a Big Data and national security framework. Appropriate governance and accountability measures are vital to ensure the public trust and acceptance of invasive national security measures.

3.6.1. Oversight Mechanisms

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

The description of each agency of its executive and independent accountability and oversight mechanisms provide an insight into the frameworks that apply in practice to each. ASIS for example describes its accountability and oversight framework as follows:[355]

> We are accountable to the Government through the Minister for Foreign Affairs under the Intelligence Services Act 2001. ASIS's Director-General is directly responsible to the Minister, and holds regular meetings with him to discuss ASIS's activities. ASIS is subject to Parliamentary oversight through the Minister for Foreign Affairs and the Parliamentary Joint Committee on Intelligence and Security (PJCIS) which reviews our expenditure and administration (as well as ASIO's and ASD's), and other matters referred to it by the Minister or either House of Parliament. Any legal issues and the propriety of ASIS's activities are overseen by the Inspector-General of Intelligence and Security (IGIS), who reports to the Prime Minister annually. ASIS's financial and administrative affairs are regularly audited by the Australian National Audit Office (ANAO). ASIS also prepares a classified Annual Report.

AUSTRAC, on the other hand, in an external scrutiny discussion in its Annual Report 2013-2014[356] lists its reporting line to the Attorney-General and the Minister for Justice, its transparency and accountability to the Parliament and:

- The Commonwealth Ombudsman; and
- The Australian National Audit Office.

According to CrimTrac, its external scrutiny includes:

- the Commonwealth Ombudsman,
- the Australian Public Service Commission,
- the Office of the Australian Information Commissioner,
- the Australian Commission for Law Enforcement Integrity, and
- the Australian National Audit Office.

The accountability frameworks therefore displays similar characteristics with some features, such a as the role of the Australian National Audit Office being common to all, while the Inspector-General of Intelligence and Security's role does not extend to AUSTRAC or CrimTrac.

The most important independent oversight bodies as far as the subject matter of this report is concerned, are the following:

---

[355] Australian Secret Intelligence Service, 'General FAQ: Who oversees ASIS's activities and expenditure?', ASIS (online), 2014 <http://www.asis.gov.au/about-us/faq/general-faq.html>.
[356] <http://www.austrac.gov.au/annual-report-13-14-management-accountability - scrutiny>.

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)*. It is located in the Prime Minister's portfolio. IGIS has oversight of ASIO, ASIS, ONA, DIO, DIGO and ASD. In addition, the Prime Minister may request the Inspector-General to inquire into an intelligence or security matter relating to any other Commonwealth agency.[357]

Key objects of *Inspector-General of Intelligence and Security Act 1986 (Cth)* include assisting Ministers in the oversight and review of:

- the compliance with the law by, and the propriety of particular activities of, Australian intelligence agencies, including ensuring that the activities of those agencies are consistent with human rights;
- the effectiveness and appropriateness of the procedures of those agencies relating to the legality or propriety of their activities; and
- certain other aspects of the activities and procedures of certain of those agencies.[358]

It also includes assisting the Government in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies, including the activities and procedures of intelligence agencies, are open to scrutiny.[359]

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
- are 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*.

However, IGIS can only inspect such acts or practices if the Australian Human Rights Commission refers them to IGIS.[360]

Agencies are required to provide IGIS with access to information and have to report certain mattes to IGIS. For example the DIO *Guidelines to Protect the Privacy of Australian Persons* oblige the Agency not only to provide 'access to all intelligence information held by DIO concerning Australian persons', but also in cases where: [361]

> a presumption under paragraph 3b [that 'the information concerns activities in respect of which the Australian person is a representative of the Commonwealth or a State or Territory in the normal course of official duties'] has been found to be incorrect, DIO is to advise the IGIS of the incident and measures taken by DIO to protect the privacy of the individual.

With respect to privacy, the *Guidelines* require under that:[362]

---

[357] 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>.

[358] S 4(a) *Inspector-General of Intelligence and Security Act 1986*.

[359] S 4(d) *Inspector-General of Intelligence and Security Act 1986*.

[360] S 8 *Inspector-General of Intelligence and Security Act 1986*.

[361] DIO *Guidelines to Protect the Privacy of Australian Persons* [5] and [5.1(c)].

[362] DIO *Guidelines to Protect the Privacy of Australian Persons* [5.1(d)].

in any case where a breach of these guidelines is identified, DIO is to advise the IGIS of the incident and the measures taken by DIO to protect the privacy of the Australian person or of Australian persons generally.

IGIS may at the request of the Minister, inquire into the action (if any) that should be taken to protect the rights of a person who is an Australian citizen or a permanent resident in a case where ASIO has furnished a security assessment report on a person to a Commonwealth agency in terms of Part IV of the *Australian Security Intelligence Organisation Act 1979* where that may result in the taking of action that is adverse to the interests of the person; and where the report could not be reviewed by the Security Appeals Division of the Administrative Appeals Tribunal.[363]

It may then in particular inquire into whether the person should be informed of the report and given an opportunity to make submissions in relation to the report.[364] IGIS may also launch such an inquiry where the responsible Minister has given a direction to ASIO on the question whether:[365]

(i) the collection of intelligence concerning a particular individual is, or is not, justified by reason of its relevance to security; or
(ii) the communication of intelligence concerning a particular individual would be for a purpose relevant to security;

to consider whether that collection is justified on that ground or whether that communication would be for that purpose, as the case may be.[366]

The IGIS's powers are not extra-territorial – its and ability to respond to a complaint is limited to extent that Australian citizens or permanent residents are affected, or an Australian law may be violated.[367]

The IGIS also has a role under the *Archives Act 1983* and the *Freedom of Information Act 1982.* Essentially it provides expert evidence to the Administrative Appeals Tribunal and the Information Commissioner in relation to national security, defence, international relations and confidential foreign government communications exemptions. It also investigates public interest disclosures relating to national intelligence agencies.[368]

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 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. The inquiries that it does undertake have been of value.

In 2013, for example, 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.[369]

---

[363] S 8(1)(c) *Inspector-General of Intelligence and Security Act 1986*.
[364] S 8(1)(c) *Inspector-General of Intelligence and Security Act 1986*.
[365] S 8(1)(d) *Inspector-General of Intelligence and Security Act 1986*.
[366] S 8(1)(d) *Inspector-General of Intelligence and Security Act 1986*.
[367] S 8 *Inspector-General of Intelligence and Security Act 1986*.
[368] S 8A *Inspector-General of Intelligence and Security Act 1986* creates assumptions and restrictions that apply to the exercise of IGIS functions in relation to disclosures under the *Public Interest Disclosure Act 2013*.
[369] Inspector-General of Intelligence and Security, *Annual Report 2012–13* (2013) 9.

ASIO and the DIO. In the following year it reviewed the progress of ASIO in implementing the recommendations of that report. In 2014, IGIS initiated an inspection project to review ASIO's progress in implementing the recommendations of that report. In its *Annual Report 2014–2015*, IGIS reported as follows:[370]

> In early 2014, ASIO invited the former Director-General of ONA, Mr Allan Gyngell AO, to conduct a comprehensive review into the state of analytic tradecraft and practices supporting the assessment function in ASIO. The inspection project was undertaken shortly after this review, and ASIO was in the process of developing and trialling new organisation-wide policies. The review project noted that there remained inconsistency in relation to ASIO analytic tradecraft, but the adoption of the organisation-wide policies was expected to lead to improvements. In June 2015 ASIO advised that the policies had been endorsed and were now being implemented across the Organisation.

IGIS's 2011 inquiry into allegations of inappropriate vetting practices in the Defence Security Authority provides another example of its ability to investigate the management aspects related to data integrity and analysis.[371] Former contractors who were data-entry operators in Defence Security Authority's security vetting operation made public allegations regarding inappropriate vetting practices. The IGIS inquiry confirmed the substance of the allegations. In essence, difficulties in uploading data into a new system led to the use by vetting staff of 'workarounds' to address both database incompatibilities and situations where an applicant had not provided all of the data required. For example, incomplete security records on officials that needed to be vetted, would be rejected by the system. Data-entry operators would complete with the fields with such incorrect data as wrong addresses, employment dates and travel destinations, to ensure that the forms are accepted by the system. This corrupted data had then entered the Australian Security Intelligence Organisation (ASIO) and was used for security assessments. The IGIS report highlighted a number of serious matters that required attention, including inadequate formal documentation and manuals, inadequate training for contractors and staff, poor systems and process change management, inadequate quality assurance, inadequate management oversight and contractual arrangements, and sustained pressure for output following increases in demand.

The systemic nature of these inadequacies gleaned from just one section of the national security framework suggests that there is a need for and value in systematic, self-instigated and detailed investigations by IGIS into data-related procedures and activities of organisations under its remit.

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.[372] 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.[373] ASIO and the IGIS are excluded from the scope of the

---

[370] Inspector-General of Intelligence and Security, *Annual Report 2014–15* (2015) 29.
[371] IGIS *Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority* (2011) <https://www.igis.gov.au/publications-reports/public-reports>.
[372] Overview of the Commonwealth System of Administrative Review <http://www.arc.ag.gov.au/Aboutus/Pages/OverviewoftheCommonwealthSystemofAdminReview.aspx#28>.
[373] S 3 read with s 5(1) of the *Ombudsman Act 1976.*

Ombudsman Act 1976.[374] 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 AFP, AUSTRAC and CrimTrac are also covered by the Commonwealth Ombudsman.[375]

The Ombudsman investigates administrative actions by government agencies. These investigations can be launched at its own initiative or as a consequence of complaints filed by individuals, groups or organisations. In either case, the Ombudsman can recommend, where required, that remedial action be taken by an agency. Such action may be directed at an individual case or may be broader and require a change to legislation.

As discussed below, the Ombudsman also 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*. It is responsible for promoting awareness and understanding of the Scheme and for monitoring its operation. It is also responsible for providing guidance, information and resources about making, managing and responding to public interest disclosures. IGIS shares these responsibilities in relation to the national intelligence agencies. In addition, it also acts as the Ombudsman in relation to a number of specific schemes, for example the in relation to the Defence Force, Law Enforcement and the Postal Industry. The Commonwealth Ombudsman is also the ACT Ombudsman under the *Ombudsman Act 1989 (ACT)*.

The Ombudsman was given an additional and extensive oversight function in terms of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)*.[376]

Certain restrictions apply to the jurisdiction of the Ombudsman. For example, in addition to having ASIO outside its scope, the Ombudsman is not authorized to investigate action taken by a Minister.[377] Under s 9(3) of the Ombudsman Act 1976*, the* Attorney-General can prevent the Ombudsman from accessing information if he or she certifies that 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.

For purposes of this report, 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.

---

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

[375] *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/>.

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

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

Australian National Audit Office

The Auditor-General,[378] an independent officer of the Parliament[379] established under the *Auditor General Act 1997*[380] 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. Some of the relevant performance reports are discussed below at 8.6.3.

The Federal Privacy Commissioner and Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (OAIC) 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.[381]

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 *Privacy Act* entitles persons to lay complaint with the Information 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 matters. It may for example conduct an assessment of whether an entity is maintaining and handling personal information in accordance with the *Privacy Act 1988*. 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

---

378 Functioning under the *Auditor-General Act 1997*.
379 *Auditor General Act 1997* (Cth) s 8.
380 *Auditor General Act 1997* (Cth) s 7.
381 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.

complaints where conciliation has not resolved the matter or in relation to Commissioner initiated investigations.[382]

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

There are also key roles for OAIC in exceptions to the APPs. Under APP 6.3(d) for instance, the exemption for non-enforcement agencies for disclosure of biometric information is conditional on compliance with Commissioner's guidelines for this purpose. Such guidelines have not yet been issued. Further, under s 16A(2), the Commissioner may make rules about disclosure for missing persons purposes under Item 3 in the Permitted General situation exception in APP 6.2(c).[383]

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 OAIC now retains ongoing responsibility for its three areas of responsibility (FOI, privacy and information policy).[384]

State Privacy Commissioners

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

For instance, a research participant in 2.1.3 described their role in this context as follows: 'The Attorney General's Department review our *Telecommunications Act* compliance. The [State] Privacy Commissioner looks over the Memorandums of Understanding we have with external agencies and between units. Some agencies generate audit reports of all requests to confirm they comply with privacy requirements; it depends on the terms of the MoU.'

In NSW, the *Privacy and Personal Information Protection Act 1998* (NSW) applies the Personal Information Privacy Principles to NSW Police, although there are a series of law enforcement, investigation and oversight agency exemptions in ss 23, 24 and 27.

---

[382] 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.

[383] See OAIC Privacy (Persons reported as Missing) Rule 2014 <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-the-privacy-persons-reported-as-missing-rule-2014>. Note that the *Telecommunications (Interception and Access) Act 1979* s 178A enables an 'authorised officer' (typically an authorised AFP or state police officer) to authorise disclosure of telecommunications data if necessary to help find a notified missing person.

[384] See Attorney General's Department 'Portfolio Budget Statement', May3 2016, 261 <https://www.ag.gov.au/Publications/Budgets/Budget2016-17/Pages/Portfolio-Budget-Statements-2016-17.aspx>

Other independent oversight mechanisms

Australian Human Rights Commission

The Australian Human Rights Commission operates under the *Australian Human Rights Commission Act 1986* (Cth) as well as federal laws[385] 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 receives and works to resolve complaints, examines laws, investigates practices and encourages positive law reform and builds an awareness and recognition of human rights throughout Australia. 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.[386]

Australian Commission for Law Enforcement Integrity (ACLEI)

The Australian Commission for Law Enforcement Integrity and the Integrity Commissioner[387] 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.[388]

The office of the Integrity Commissioner and the Australian Commission for Law Enforcement Integrity are established by the *Law Enforcement Integrity Commissioner Act 2006*.[389] ACLEI supports the Integrity Commissioner to provide independent assurance to government about the integrity of prescribed law enforcement agencies and their staff members. ACLEI's primary role is to investigate law enforcement-related corruption issues, giving priority to serious and systemic corruption. The agencies subject to the Integrity Commissioner's jurisdiction are:

- the Australian Border Force
- the Australian Crime Commission
- the Australian Federal Police (including ACT Policing)
- the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- the CrimTrac Agency

---

385 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*.

386 S 11(3) Australian Human Rights Commission Act 1986 (Cth).

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

388 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*.

389 See <https://www.comlaw.gov.au/Series/C2006A00085>.

- prescribed aspects of the Department of Agriculture
- the Department of Immigration and Border Protection, and
- the former National Crime Authority.

A challenge facing ACLEI is that those law enforcement officers subject to investigation by the Integrity Commissioner are likely to be well versed in law enforcement methods, and may be skilled at countering them in order to avoid scrutiny.[390] Hence ACLEI has access to a range of special law enforcement powers and methods, including telecommunications and electronic surveillance. The degree to which these powers extend to direct oversight of proper data storage and analytics practice is not known. Rather than responding to every report of corruption, the Integrity Commissioner's role is to ensure that indications and risks of corruption in law enforcement agencies are identified and addressed effectively. This may imply an interest in systemic indicators.

Parliamentary oversight

Parliament is the ultimate oversight body, holding relevant Ministers accountable for the agencies under their control.[391] 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 (PJCIS).

Parliamentary Joint Committee on Intelligence and Security (PJCIS)

S 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 must consist of 11 members. Five members must be Senators and six must be members of the House of Representatives.[392]

The PJCIS functions include the review of the administration and expenditure of ASIO, ASIS, AGO, DIO, ASD and ONA, including the 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 AFP of its functions under Part 5.3 (Terrorism) of the *Criminal Code.*[393]

However, a range of matters fall outside the PJCIS' 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

---

[390] See ACLEI, 'About ACLEI', <http://www.aclei.gov.au/Pages/AboutACLEI.aspx>; *ACLEI Corporate Plan 2015–16*, 2015 <http://www.aclei.gov.au/Documents/ACLEI-corporate-plan-2015-16.pdf>.
[391] *Church of Scientology v Woodward* (1982) 43 ALR 587.
[392] Amendments to the composition and scope of the PJCIS were envisaged in the Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1011>. The Bill lapsed on 17 April 2016.
[393] S 29(1) *Intelligence Services Act 2001* (Cth).

evaluation activities undertaken by ONA.[394] The PJCIS furthermore does not have the power to decide to review any matter without it being referred to the Committee.[395]

The PJCIS report *Inquiry into Potential Reforms of National Security Legislation*[396] is an example of the work undertaken by the Committee. It investigates telecommunications interception, data retention and related matters that informed the subsequent law reform.

Observations about oversight mechanisms

As was seen in 2.5, independent oversight officers and agencies are a crucial component of the regulatory regime. They play a policy role ('[IGIS] also critiques the benchmark') and can play a powerful role in encouraging compliance (see 2.5.2A-C, 2.5.3A-D). On the negative side, there may be some duplication (see 2.5.4 'Duplication of oversight').

All oversight bodies are able to perform and do perform important functions but 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. Mindful of the need to cooperate, especially where powers and scope may overlap, the bodies 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.

3.6.2. 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.[397] 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

---

[394] S 29(2) *Intelligence Services Act 2001* (Cth).
[395] The power was envisaged in Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015. The Bill lapsed on 17 April 2016.

[396] See <http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_committees?url=pjcis/nsl2012/report.htm>.
[397] 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>.

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.[398]

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.

Archives Act 1983

The *Archives Act 1983* empowers the National Archives of Australia to oversee recordkeeping practices for Commonwealth records.[399] This Act regulates, for example, the transfer of Commonwealth records to the National Archives and access to such records if kept elsewhere as well as the destruction, or alteration of Commonwealth records. Generally such records can be accessed by the public after a period, transitioning from 30 years to 20 years over the period 2011 to 2021 under amendments to the Act passed in 2010.[400]

The *Archives Act 1983* (Cth) regulates the destruction or disposal of Commonwealth records and, indirectly therefore, also the retention of such records.

This discussion will provide a brief overview of the retention and deletion regime of the Act, before discussing aspects of its transfer and access rules.

Retention and deletion of records

Commonwealth records may not be destroyed, damaged, altered or their 'custody or ownership' transferred unless this is 'required by law' (not merely authorised), with the permission of the Archives or in the process of placing records not already in custody into the custody of a Commonwealth entity entitled to have custody, or in accordance with normal administrative practice unless Archives has notified the entity of its disapproval.[401]

The National Archives issues 'records authorities' setting out detailed requirements for the retention of specified records. General records authorities set out requirements for keeping, destroying or transferring records of business common to many Commonwealth agencies. The Administrative Functions Disposal Authority (AFDA)[402] and AFDA Express provide for a range of common administrative functions. The extensive Technology and Telecommunications chapter of the AFDA, Chapter 19, stipulates for example the following retention periods for the following types or records:

---

[398] 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. See also the discussion below.

[399] S 2A *Archives Act 1983*.

[400] S 2(7) *Archives Act 1983*.

[401] S 24(2) *Archives Act 1983* (Cth)

[402] See <http://www.naa.gov.au/records-management/publications/afda.aspx>.

Table 3-4: Examples from AFDA Chapter 19: Technology and Telecommunications[403]

Class no	Description of records	Disposal action
2086	Records documenting the development, modification and maintenance of specific applications to meet business needs which go into production. Includes: • feasibility studies; • pilot studies; • final version of all system documentation, user and • technical manuals; • application specific data dictionaries; • final version of business rules; • final version of user requirements; • final version of system specifications; • rectification of problems (includes Year 2000 remediation); • requests for system changes; and • final sign-off by all parties.	Destroy 5 years after(sub)system is defunct and any data supported is either migrated destroyed[404]
2090	Final internal and external audit reports relating to the technology and telecommunications function	Destroy 5 years after action completed[405]
2096	Records documenting agency compliance with mandatory proportional standards or with statutory requirements relating to the technology and telecommunications function	Destroy 5 years after action completed[406]
2099	System logs which are used to show a history of access or change to data (e.g. system access logs, internet access logs, system change logs and audit trails etc)	Destroy 7 years after action completed[407]
2159	Records documenting testing activities where unexpected results are found. Includes: • testing strategy; • testing plan; • result forms; and • test report.	Destroy when problem has been rectified[408]
2160	Records documenting testing activities where expected results are found. Includes: • testing strategy; • testing plan; • result forms; and • test report.	Destroy 7 years after action completed[409]

---

403 The records authority issued for AUSTRAC, stipulates for example that in relation to intelligence records relating to the maintenance of systems used to store and analyse data, the AFDA provisions relating to Technology and Telecommunications in relation to Maintenance apply.
404 National Archives of Australia AFDA, 300.
405 National Archives of Australia AFDA, 302.
406 National Archives of Australia AFDA, 304.
407 National Archives of Australia AFDA, 305.
408 National Archives of Australia AFDA, 322.
409 National Archives of Australia AFDA, 322.

In addition to the general records authorities, the National Archives collaborates with agencies to develop agency-specific record authorities.[410] These are meant to be read in conjunction with the general records authorities.[411] The records authority issued in respect of ASIO,[412] for example, relates to all its core business records relating to Foreign Intelligence Collection, Protection of Agency Personnel and Personnel Records, Security Intelligence Assessment and Advice, and Security Intelligence Collection.

In respect of the Security Intelligence Collection set of documents, for example, the authority identifies a range of documents that must be retained for the National Archives.[413] It then proceeds to identify documents that may be destroyed, in some cases only after 150 years:

Table 3-5: Examples from AFDA: Disposal

Class no	Description of Records	Disposal Action
61099	Warrants, excluding warrants covered in class 61098, and records documenting the administration and authorisation of warrants including: • warrant requests; • internal approvals; • legal reviews; • internal liaison for compliance and accuracy; • liaison and review with Attorney-General's Department; • authorisation details; • liaison with external agencies; • facilitation of inspections by the Inspector-General of Intelligence and Security;[414] • maintenance of the warrants register; and • warrant policy and procedures and related advice.	Destroy 150 years after last action

[410] See <http://www.naa.gov.au/records-management/agency/keep-destroy-transfer/agency-ra/index.aspx>.

[411] National Archives of Australia, Australian Security Intelligence Organisation - Records Authority 2012/00324244, 3.

[412] Records authority 2012/00324244 <http://www.naa.gov.au/records-management/agency/keep-destroy-transfer/agency-ra/index.aspx>.

[413] These include 'Class 61098' records documenting security intelligence collection activities such as Ministerial arrangements, guidelines, determinations and directions issued to the agency; negotiation, development and monitoring of agreements, cooperative arrangements, conventions, and alliances developed or agreed to by the agency; development and application of security intelligence equipment, facilities, systems and technology; and authorisations including Ministerial Authorisations and Director-General Authorisations.

[414] A records authority has also been issued for the Office of the Inspector-General of Intelligence and Security. National Archives of Australia - *Records Authority - Office of the Inspector-General of Intelligence 2010/00216680* May 2010 requires documents with enduring value (e.g. registers and summaries of inquiries and complaints) to be kept for the National Archives. The following however are examples of documents that may be destroyed 15 years after the last action was taken: Reports of inspections and inquiries; Complaint handling; Advice and submissions with implications for the internal procedures of an agency, department or organisation and Briefings by an agency, department or organisation.

Class no	Description of Records	Disposal Action
61101	Records documenting routine security intelligence collection activities including: • requests, collection and monitoring; • evidence and data collected including under warrant; • management of sources and contacts; • development and management of specialised agency facilities, techniques, technology and equipment; • liaison and information sharing with government agencies, industry, foreign governments and the community necessary to conduct security-related inquiries and facilitate operational requests; • internal committee and task force meetings relating to security intelligence collection; • informal and internal conferences, conventions or consultations; • internal reviews of security intelligence collection programs, services and operations; • contact reporting; and • evidence of the action taken.	Destroy 20 years after last action
61102	Records documenting administrative activities relating to intelligence collection including: • resourcing, interception requests, reports, certifications and authorisations; • policies and procedures for securing of evidence required to support litigation action; • operational/business plans, policies and procedures, routine and reports documenting internal developments, decisions and actions; • informal and internal collection advice, guidelines, distribution and instructions; • training programs and related materials developed and delivered to agency staff; • Inspector-General of Intelligence and Security compliance reports and related action; and • negotiation, development and monitoring of agreements.	Destroy 5 years after last action

Observations

While the *Archives Act* requires a significant number of records to be retained it allows many records relevant to data access and mining to be destroyed. 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.

Transfer and access rules relating to intelligence records

The *Archives Act 1983* (Cth) compels and regulates the transferral of records of Commonwealth institutions to the National Archives[415] or, alternatively, full and free access by the Archives, at all reasonable times, to all Commonwealth records in the custody of a Commonwealth institution other than the Archives.[416] Section 29 provides for certain exemptions to be created:

> A Commonwealth institution or its representative may, with the concurrence of the Director-General responsible for the National Archives, determine that a Commonwealth record or class of records in its possession or relating to its functions is not a record that is required to be transferred to the care of the Archives or one to which the Archives is entitled to have access under the Act or only enjoy such access on specified conditions.

Section 29(8) strengthens the exemption in relation to intelligence agencies and the IGIS. It states that the following agencies can issue such a determination unilaterally without the concurrence of the Director-General:

- the Australian Security Intelligence Organisation;
- the Australian Secret Intelligence Service;
- the Defence Imagery and Geospatial Organisation;
- the Australian Signals Directorate;
- the Defence Intelligence Organisation;
- the Office of National Assessments; and
- the Inspector-General of Intelligence and Security.

This arrangement is extended to the AFP but only in relation to a record that contains information the release of which would endanger the safety of a person who is, or has been, assessed for inclusion in the National Witness Protection Program; or who is, or has been, a witness within the meaning of the *Witness Protection Act 1994* under that Program.

A Commonwealth record held in terms of this Act is publicly accessible after the specified period (30 years being managed down to 20 in terms of the current scheme of the Act) provided it is not an exempt record in terms of section 33. Section 33 allows for a range of grounds for such an exemption. For example, a record is exempt if it contains information or matter of any of the following kinds:[417]

- information or matter the disclosure of which under the *Archives Act* could reasonably be expected to cause damage to the security, defence or international relations of the Commonwealth;
- information or matter that was communicated in confidence by, or on behalf of, a foreign government, an authority of a foreign government or an international organisation to a Commonwealth entity, which the disclosing entity advises is still confidential, and where would be reasonable to maintain the confidentiality; or
- information or matter the disclosure of which would, or could reasonably be expected to:
  - prejudice the conduct of an investigation of a breach, or possible breach, of the law, or a failure, or possible failure, to comply with a law relating to taxation or

[415] S 27 *Archives Act*.
[416] S 28 *Archives Act*.
[417] Before deciding that a document is not exempt under the *Archives Act 1983* on intelligence and security-related, grounds the Administrative Appeals Tribunal must seek evidence from the IGIS. See *IGIS Annual Report 2013–2014* (2014) 14 for the practical implications.

prejudice the enforcement or proper administration of the law in a particular instance;

- disclose, or enable a person to ascertain, the existence or identity of a confidential source of information in relation to the enforcement or administration of the law; or
- endanger the life or physical safety of any person.

Observations

The *Archives Act* tries to balance operational secrecy required by law enforcement and intelligence agencies with the need of the public and future generations to access government information when it is not sensitive. In many cases sensitivity generally declines over time and a result key documents can be made available after a period of time.

Where the time period is too long, the documents are only of historic interest. The *Archives Act* does therefore not empower the public to access information regarding the development and implementation of Big Data systems within time periods that would enable the public to hold authorities accountable. As mentioned earlier, the relatively short periods for the retention of key documents regarding the development and implementation of technological and telecommunications systems are also unhelpful. While the retention of the documents do support independent oversight functions, most of the relevant operational documents will be destroyed long before the disclosure period under the *Archives Act* commences.

As far as the public is concerned, the destructions, exemptions and the relatively long period of non-disclosure of records that are not exempt from disclosure render the current scheme of little control value in relation to the rapid evolution of analytics technology. This increases the responsibility of independent oversight bodies to inspect the relevant records and to audit practices.

3.6.3. Compliance audits and reviews

Compliance management is part of the management responsibility of the senior officials of the relevant agencies. Aspects of compliance may however be reviewed by oversight bodies such as IGIS and also by the Auditor-General, especially in performance audits.

IGIS

According to IGIS it regularly examines agency records to ensure that the activities of the intelligence agencies comply with the relevant legislative and policy framework, including guidance provided by the responsible minister and the agency's own internal policies and procedures.[418] IGIS however has a closer focus on the ASIO, ASIS, DIGO and ASD given their intrusive powers and investigative techniques, than on DIO and ONA. In 2013-2014, for example, its risk-based inspection program focused on ASIO, ASIS and ASD but allocated fewer resources to DIGO, DIO and ONA.[419] Inspection activities relating to DIO and ONA are generally limited to ensuring that their assessments comply with administrative privacy guidelines (which have a similar effect to the privacy rules applying to ASIS, ASD and DIGO – see Technical References 4 and 5).

---

[418] IGIS, *Annual Report 2013–2014* (2014) 18.
[419] IGIS, *Annual Report 2013–2014* (2014) 18.

The annual reports of IGIS lists various instances of non-compliance by agencies. In many cases, especially of privacy breaches, these were reported to IGIS by the agency concerned and related to accessing of information of Australian citizens while they were assumed to be foreign citizens.[420] Attention is also given to whether telecommunication data and financial data held by other agencies were correctly accessed. IGIS for example found that ASIO was not as non-compliant with AUSTRAC's guidelines on the storage of certain AUSTRAC information [421] and that ASIS was deficient in some of its obligations under the AML/CTF Act. It also identified a case where ASIO communicated AUSTRAC information to a foreign intelligence agency without first receiving appropriate undertakings for the protection and use of the information.[422]

As noted above, IGIS appears to be mainly focused on access, management and sharing of data but analysis receives attention in specific inquiries and review projects.

Commonwealth Ombudsman

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 arises from, and is detailed in laws such as the *Telecommunications (Interception and Access) Act 1979*. The Ombudsman does not have a public reporting mechanism under this Act. It reports its findings to the AGD and the practice is to include a summary of the findings of the Ombudsman in its published annual report on the *Telecommunications (Interception and Access) Act 1979.*[423] In its 2013-2104 report, it reported as follows on the Ombudsman's inspection findings that year: [424]

Overall, the Ombudsman considered that agencies demonstrated a good understanding of the Act's requirements, with all agencies found to be compliant with the majority of the Ombudsman's inspection criteria. The Ombudsman's inspection criteria are:

- Were restricted records properly destroyed (s 79)?
- Were the requisite documents kept in connection with the issue of warrants (s 80)?
- Were warrants properly applied for and in the correct form (s 49)?
- Were the requisite records kept in connection with interceptions (s 81)?
- Were interceptions conducted in accordance with the warrants (s7) and was any unlawfully intercepted information properly dealt with (s 63)?

While these inspections are important, the inspection criteria are largely focused on technical compliance. Inquiries do not seem to extend to justification for access to the data or analysis and use of the data.

Australian National Audit Office

The Auditor-General,[425] assisted by the Australian National Audit Office (ANAO), provides 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

---

[420] IGIS, *Annual Report 2013–2014* (2014) 25.
[421] IGIS, *Annual Report 2012–2013* (2013) 16–17.
[422] IGIS, *Annual Report* 2013–2014 (2014) 31.
[423] Commonwealth Ombudsman, *Annual Report 2013–2014* (2014) 64.
[424] AGD, *Telecommunications (Interception and Access) Act 1979 Annual Report 2013–14* 30.
[425] Functioning under the *Auditor-General Act 1997*.

management practices, the ANAO's performance audits are the most important means to investigate the data management practices of agencies. Examples of relevant reports include:

- Data Management in the APS[426]

  The audit assessed the efficiency, effectiveness and accountability of data management by government agencies. It focused mainly on data collected by departments and agencies from non-departmental organisations and institutions.

- Managing Data Privacy in Centrelink[427]

  This audit assessed the systems put in place by Centrelink to protect data privacy. The audit reviewed the adequacy of the policies, procedures and the administrative framework associated with data privacy, and the computer systems that are used to store and disseminate data. The ANAO also examined compliance with legislative requirements.

- The Australian Taxation Office's Use of Data Matching and Analytics in Tax Administration[428]

  The audit assessed the ATO's corporate management of data matching, including analytics. The ANAO examined the ATO's strategic goals and governance arrangements for data matching and analytics, compliance with privacy requirements and whether the ATO is achieving intended results, including revenue collection, optimised compliance and provision of improved services to taxpayers.

- Cyber Attacks: Securing Agencies' ICT Systems[429]

  The audit assessed compliance by selected agencies with the mandatory ICT security strategies and related controls in the Australian Government Information Security Manual.

- AUSTRAC's Administration of its Financial Intelligence Function[430]

  The audit assessed the effectiveness of AUSTRAC's arrangements for processing financial intelligence, to assist domestic partner agencies and international counterparts in their operations and investigations.

These independent audits provide important perspectives on key aspects of data management. They are however not undertaken consistently and are, by their nature, not able to cover all relevant aspects. Legal questions such as proportionality and technical questions regarding the actual functioning of IT-based analytical systems are generally not probed. The performance audit of AUSTRAC's administration of its financial intelligence function provides a useful illustration.

The audit found for example that breaches have occurred in the past where partner agencies have detected inappropriate use of AUSTRAC data by their employees. Partner agency usage of access to AUSTRAC data is extensive, as discussed in3.1.

---

[426] ANAO, *Data Management in the APS,* Audit Report No.48 1997–1998.
[427] ANAO, *Managing Data Privacy in Centrelink* Audit Report No.8 1999–2000.
[428] ANAO, *The Australian Taxation Office's Use of Data Matching and Analytics in Tax Administration*, Audit Report No.30 2007–08.
[429] ANAO, *Cyber Attacks: Securing Agencies' ICT Systems*, Audit Report No. 50 2013–14.
[430] ANAO, *AUSTRAC's Administration of its Financial Intelligence Function*, Audit Report No.47 2012–13.

In its 2012-2103 Annual Report AUSTRAC advised that it implemented a Reason for Access (RFA) function, enabling partner agency users to record the grounds for conducting searches. This function enables AUSTRAC to improve its monitoring and audit of AUSTRAC database usage.[431]

The international exchange agreements with international counterparts that the ANAO examined did not require them to report breaches to the agreement to AUSTRAC.[432] AUSTRAC has since advised that the international exchange agreement template has been amended to include specific provisions requiring the reporting of known unauthorised disclosures and consequences.[433]

Most financial transaction reports filed by private sector entities such as banks are transmitted electronically into AUSTRAC's (TRAQ) database, discussed above in 3.1. Financial intelligence assessments provided to partner agencies by AUSTRAC may be initiated from a number of sources, including an irregular financial transaction detected in the TRAQ database by AUSTRAC's automated monitoring system (TargIT).[434] A TargIT clause can be triggered by names, bank account details or other identifying fields, and each 'hit' is assessed as either being of high, medium or low priority.[435] The report states:

> AUSTRAC advised that there is no requirement or expectation that all hits will be assessed. A large volume of hits, have historically and continue to be, false/positives, generated by data quality issues. Better matching, as TargIT clauses have been refined, has improved the reliability of the top performing clauses, but reliability issues still occur. Consequently, it is not practical to expect that every hit will be assessed.

In view of this information the report then considered the management of the TargIT workload and especially the management and communication of backlogs on unassessed hits. The report did not reflect however that the audit team assessed the clauses or monitoring rules to determine whether they are appropriate and no indication is given that the audit team considered any steps that must be taken to improve the quality of data analysis.

(Note that AUSTRAC is currently in the process of replacing the TargIT system with its own *AUSTRAC Intelligence* (AI) system, as discussed in 3.1).

OAIC

Under section 33C of the *Privacy Act*, the OAIC has the power to conduct assessments (previously known as audits) of a range of matters including whether:

- personal information is being handled by an APP entity in accordance with the APPs or a registered APP code;
- information held by an entity is being maintained and handled in accordance with Part IIIA of the *Privacy Act* or the registered CR code;

---

[431] AUSTRAC *Annual Report* 2012–2013 (2013) 63.
[432] ANAO, *AUSTRAC's Administration of its Financial Intelligence Function*, Audit Report No.47 2012–13 [2.54].
[433] ANAO, *AUSTRAC's Administration of its Financial Intelligence Function,* Audit Report No.47 2012–13 [2.54].
[434] ANAO, *AUSTRAC's Administration of its Financial Intelligence Function,* Audit Report No.47 2012–13 [1.10].
[435] ANAO, *AUSTRAC's Administration of its Financial Intelligence Function,* Audit Report No.47 2012–13 [1.10].

- TFN information held by a file recipient is being maintained and handled in accordance with the TFN Rules;

- a data matching program complies with Part 2 of the *Data Matching Act*;

- information to which section 135AA of the *National Health Act 1953* applies is being maintained and handled in accordance with the rules issued under that section.

Under section 309 of the *Telecommunications Act 1997*, the Australian Information Commissioner has the function of monitoring compliance by telecommunications' companies with the record keeping requirements of sections 306 and 306A of that Act.

The OAIC undertakes a range of assessments each year, including a strategic assessment program under section 33C and under various MOUs with the Department of Immigration and Border.

Observations

It is important that aspects of compliance can and must be reviewed by oversight bodies such as IGIS and the ANAO. Systemic overviews, such as the telecommunications compliance audits done by the Commonwealth Ombudsman, focus on technical compliance aspects and do not consider the grounds for access or the methods employed to analyse the data. In relation to data sharing, there is little indication of a consistent investigation of MOUs or of monitoring of compliance with MOUs. In fact the isolated performance reports of the ANAO and the special IGIS reports show the value of such investigations but also highlights the absence of consistent, systemic consideration of these matters.

3.6.4. Complaint mechanisms as sources of information and review

External complaints

A range of complaints handling entities 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.[436] Where it does not but can potentially be received by another entity, a complainant will normally be advised to contact that other body. Such complaints may lead to investigations and reviews of data access and usage practices. Particularly relevant bodies for purposes of this study are the IGIS, the Commonwealth Ombudsman and the Privacy Commissioner:

Members of the public can make complaints to the IGIS in relation to any of the agencies over which IGIS has jurisdiction. Some restrictions apply:[437]

- Only Australian citizens or permanent residents may lodge a complaint against ASIS, ASD or DIGO.
- Any Australian or foreign citizens may lodge a complaint about ASIO.
- IGIS is not statutorily empowered to receive complaints about ONA or DIO but indicated that it would consider any submission that provided substantial evidence that ONA or DIO acted improperly. The IGIS may in such a case commence own inquiries.

---

[436] See for example <http://www.ombudsman.gov.au/pages/related-sites/other-complaint-handling-review-agencies.php>.
[437] IGIS, 'Making a Complaint', IGIS web page <https://www.igis.gov.au/making-complaint>.

The Commonwealth Ombudsman can in general investigate complaints about wrong, unjust, unlawful, discriminatory or unfair actions and decisions of Australian Government agencies. The Commonwealth Ombudsman also acts, among others as the Defence Force Ombudsman, the Immigration Ombudsman and the Law Enforcement Ombudsman. The Commonwealth Ombudsman and the AFP's Professional Standards have joint responsibility for handling complaints about the AFP.[438] From 1 May 2015, the Inspector-General of Taxation handles the bulk of complaints about the ATO while the Commonwealth Ombudsman will continue to deal with complaints concerning Freedom of Information or Public Interest Disclosures issues relating to the ATO.

The Privacy Commissioner can investigate complaints from individuals about interferences with privacy under the *Privacy Act 1988* (Cth) against Australian and ACT government agencies and private sector organisations. As discussed above, the application of the *Privacy Act* is limited in relation to intelligence agencies. Breaches of the privacy rules relating to specific intelligence agencies subject to IGIS oversight are investigated by IGIS, when reported by the agency concerned.[439]

While there is a range of bodies that may receive data-related complaints, the chances of a breach coming to the attention of an affected person are 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 the IGIS. In its 2013-2104 *Annual Report* the IGIS noted that it received 504 complaints. 487 of those complaints related to visa-related security assessment.[440] Security assessments are undertaken as part of the visa application processing and a negative finding would result in the refusal of a visa.[441] A person who is negatively affected by a decision to decline a visa is therefore alerted to the assessment and, if the person feels aggrieved, can approach IGIS. Such disclosure is uncommon in relation to the use and analysis of data outside formal law enforcement processes.

Staff complaints

While internal staff complaints processes are internal, administrative and management processes that do not require statutory backing, the *Public Interest Disclosure Act 2013 (Cth)* was adopted to channel formal, serious disclosures. This Act facilitates disclosure and investigation of wrongdoing and maladministration in the Commonwealth public sector. It recognises the value of a mechanism that enables concerns to be raised without fear of retribution, and with some prospect that serious issues will be acknowledged and fed into a process that is impartial and capable of taking whatever action is warranted.

The Act commenced on 15 January 2014. This Act also 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 did receive a number of enquiries regarding the scheme.[442]

---

438 <http://www.ombudsman.gov.au/pages/our-legislation/australian-federal-police/>.
439 *IGIS Annual Report 2013–2014* (2014) 23.
440 *IGIS Annual Report 2013–2014* (2014) 15.
441 *Plaintiff M47-2012 v Director General of Security* [2012] HCA 46.
442 *IGIS Annual Report 2013–2014* (2014) 14.

The AFP has an extensive complaints scheme that also allows for members of the public to lodge minor complaints that are dealt with at a management level.[443]

The value of such disclosures is illustrated by the 2011 inquiry into allegations of inappropriate vetting practices in the Defence Security Authority. [444] That inquiry was triggered by former staff contractors, and the inquiry in effect vindicated their concerns.

Observations

Complaints processes are important mechanisms to draw attention to possible administrative problems. Existing mechanisms, especially enhanced by the *Public Interest Disclosure Act 2013 (Cth)*, can inform and support the functioning of the of the independent oversight bodies. External complaints can, however, only be lodged by persons who have sufficient knowledge about the access or handling of their data to feel aggrieved. The lack of disclosure of relevant practices lessens the chances of such complaints being lodged.

3.7. Are principles and rules regularly reviewed?

This section considers whether the Australian 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.

The Australian legal framework provides a range of mechanism that allow for the review of certain laws, rules and practices. Internal reviews of the effectiveness and efficiency of systems and processes should occur in agencies and also within government as part of the management of the business of government. This inquiry is however concerned with public and independent review mechanisms as these mechanisms impact on the general public trust in the system. In the Australian context public and independent review mechanism includes Parliament, Commissions of Inquiry and independent oversight bodies as well as processes such as regulatory impact assessments and privacy impact assessments.

3.7.1. Review Mechanisms

Parliament and Government

Parliament provides the forum where new laws concerning data collection, access, disclosure, and use can be debated. Where laws are controversial, review mechanisms or sunset clauses may be inserted. These provide Parliament with an opportunity to review the impact of the law and to consider whether it should be amended or withdrawn.

Sunset clauses typically provide for all or a part of legislation to expire at a pre-determined time. That leaves Parliament with a choice to pass new legislation, renewing or amending those provisions, or to allow their termination.[445] The section giving rise to a new offence of 'entering, or remaining in, declared areas',[446] created in the *Criminal Code*, which provides a

---

[443] http://www.afp.gov.au/about-the-afp/standards.
[444] IGIS *Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority* (2011) < https://www.igis.gov.au/publications-reports/public-reports>.
[445] Nicola McGarrity, Rishi Gulati and George Williams 'Sunset clauses in Australian Anti-Terror Laws' 2012 33 *Adelaide Law Review* 307.
[446] S 119.2 Criminal Code, *Criminal Code Act 1995 (Cth)* Schedule 1.

recent example of the use of sunset clause. The section will cease to have effect at the end of 7 September 2018. When this Act was debated, various different views were expressed regarding sunset clauses. The majority favoured sunset clauses but differed about the ideal length of the sunset period. The fact that government wanted to use the Act to extend the sunset period for a number of other provisions also elicited criticism. The Independent National Security Legislation Monitor raised the point that sunset clauses are not necessarily accompanied by provisions requiring their review of the relevant measures close to the end of the sunset periods, to inform a decision on whether or not they should be further extended or potentially made permanent.[447] Where that is not required the decision whether to allow the provision to be terminated or renewed may not be appropriately informed.

Statutory review mechanisms can also be inserted into legislation. Section 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, and for a report of the review to be prepared and tabled in Parliament.[448]

Where a review is not statutorily required, the Government often takes the lead in launching the review. In 2012, for example, the Council of Australian Governments' (COAG) undertook a review of counter-terrorism legislation. This resulted from a 2005 decision by COAG to review these laws formally after five years.[449] More often, however, reviews of laws and their implementation would be requested by Ministers and by agencies. A particularly important role in this regard is performed by the Attorney-General and the Australian Law Reform Commission. The Commission is an independent federal agency operating under the *Australian Law Reform Commission Act 1996 (Cth)*. It conducts inquiries into areas of law at the request of the Attorney-General of Australia. Such inquiries often review aspects of existing laws and processes.

Independent National Security Legislation Monitor

The Independent National Security Legislation Monitor (INSLM) acts in terms of the *Independent National Security Legislation Monitor Act 2010* (Cth). The INSLM reviews the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation on an ongoing basis. This includes considering 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.

---

[447] See <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1415a/15bd034>. This matter was addressed in the Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015, which would, if adopted, have provided the Committee with the function of conducting a pre-sunset review <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1011>. The Bill lapsed on 17 April 2016.

[448] Attorney-General's Department Report on the Statutory Review of the Anti-Money Laundering and Counter Terrorism Financing Act 2006 and Associated Rules and Regulations *(2016) <https://www.ag.gov.au/consultations/pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx>.*

[449] <http://www.ag.gov.au/Consultations/Pages/COAGReviewofCounter-TerrorismLegislation.aspx>. The review processes commenced only 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.

The INSLM is ideally suited for balanced review of the type identified in the lens. Its focus is however limited to counter-terrorism and national security legislation. The INSLM's recommendations have furthermore gone unheeded by government.[450]

The government signalled its intent to repeal the *Independent National Security Legislation Monitor Act 2010* (Cth) by introducing a Bill to this effect.[451] 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.[452] After acting in the position for some months the current INSML was appointed for a period of two years in August 2015.

Commissions of Inquiry

A range of important inquiries regarding national security have been conducted.[453] Important inquiries include the Royal Commission on Intelligence and Security (1974–77, Justice Robert Hope);[454] the Royal Commission on Australia's Security and Intelligence Agencies (1983–84, Justice Robert Hope); the Inquiry into Australian Intelligence Agencies (2004, Philip Flood)[455] and the Independent Review of the Intelligence Community (2011, Robert Cornall and Rufus Black).[456] The scope and depth of such reviews depend on the terms of reference and the resources allocated to the inquiry.

Independent Oversight Bodies

The independent oversight bodies discussed in 3.6.3 also perform important review functions. Compliance and thematic reviews are however limited by the scope and powers of each body. While the Australian Human Rights Commission may consider the impact of a law on human rights its review may not extend to the commercial impacts on business entities that may be compelled to unfairly shoulder the cost impact of the law.

3.7.2. Assessment tools

Regulatory impact statements and assessments and privacy impact assessments are important tools that can inform review processes.

Regulation Impact Statements

The Australian government adopted a regulatory assessment regime that includes Regulation Impact Statement that must accompany regulatory submissions to Cabinet and for all decisions made by the government and its agencies that are likely to have a regulatory impact on businesses, community organisations or individuals, unless the proposed change is a minor change. Proposals that proceed without a compliant Regulation Impact Statement, must be the subject of a Post-Implementation Review that should generally be completed within two years of the implementation of the regulation. In addition, for

---

450 Independent National Security Legislation Monitor *Annual Report 2013–2104* (2014) 3.
451 Independent National Security Legislation Monitor Repeal Bill 2014 (Cth) <https://www.comlaw.gov.au/Details/C2014B00041>.
452 <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5189>.
453 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.
454 <http://www.naa.gov.au/collection/explore/security/royal-commisson>.
455 <https://fas.org/irp/world/australia/flood.pdf>.
456 <http://www.dpmc.gov.au/pmc/publication/2011-independent-review-intelligence-community>.

regulations assessed by Office of Best Practice Regulation[457] as having a substantial or widespread impact on the Australian economy, a Post-Implementation Review must be completed within five years following the implementation of the regulation. Such a review examines the problem that the regulation was intended to address, the objectives of government action, the impacts of the regulation and whether the Government's objectives could be achieved in a more efficient and effective way. Review processes include public consultation and the extent of the engagement of the impact of measures on society depends in part on the level and nature of participation in the process.

Privacy Impact Assessments

The Office of the Australian Information Commissioner (OAIC) encourages agencies and organisations to consider the need for a privacy impact assessment when embarking on any project that will involve the handling of personal information.

Privacy Impact Assessments are considered above, under Rules in 6.3.

Observations

> Big Data tools and applications in this area are in a state of rapid evolution and development. Risks and opportunities may not be clear or be fully appreciated and relevant rules may prove not to be appropriate or sufficient. Review is an important and predictable need. An appropriate Big Data framework will require 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. To the extent that problems are broad or systemic, thorough overall reviews will be required to inform appropriate reforms.
>
> 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 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.

3.8. 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.

[457] 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.

These challenges informed the position taken by many research participants on transparency (2.6.4).

This inquiry considers whether, to the extent consistent with the need for operational secrecy, the framework ensures that the nature of data accessed, the analytic 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.

3.8.1. General access to data

In general, Australians enjoy access to government data, subject of course to national security and operational confidentiality principles.

The *Freedom of Information Act 1982 (Cth)* (FOI Act), administered by the OAIC, 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 FOI 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. Access in general extends to documents that contain information about the applicants or about government programs, policies and decisions. In some circumstances individuals can also ask Ministers and agencies to correct or add a note to any information they hold about them. The FOI Act also requires agencies to publish specified categories of information, and allows them to proactively release other information.

Section 7 of the *FOI Act*, especially read with Schedule 2 to the Act, creates a range of exemptions that limit the value of the *FOI Act* for purposes of transparency regarding Big Data and national security. Under section 2A an agency is, for example, exempt 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.

The *Privacy Act 1988* has similar FOI like rights embedded in its *Australian Privacy Principles* 1, 5, 10, 12 and 13.[458] For example, taken as a whole, APP 1 comprises a set of collective requirements that seek to increase agencies' transparency and accountability in relation to the manner in which they collect and handle personal information. 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 APPs and the *Privacy Act*, as discussed in section 8.2 above.

The Australian government formally expressed its intention to join the Open Government Partnership in May 2013.[459] The Partnership is a multilateral government and civil society initiative launched in 2011 that aims to secure concrete commitments from governments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance. To qualify for membership a country must endorse a high-level Open Government Declaration, deliver a country action plan developed with public consultation, and commit to independent reporting on their progress going forward. More than sixty governments have made such commitments.[460] Australia has however not yet followed up on its membership application by making the required commitment. If Australia

---

[458] See the Schedule with APPs at <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html>.
[459] <http://www.opengovpartnership.org/country/australia>.
[460] <http://www.opengovpartnership.org/about#sthash.TITriZwc.dpuf>.

joined, the principle of transparency of government will receive greater commitment, which may strengthen access to information.

3.8.2. Sources of general information

There are a significant number of sources of information available on data access and general management of data by government agencies for the purposes covered in this report. These include:

- Parliamentary debates, evidence and reports, for example those stemming from the work of the Parliamentary Joint Committee on Intelligence and Security;[461]
- Annual reports by agencies. In the case of intelligence agencies their availability is more limited: ASIO and IGIS produce annual reports that are tabled in Parliament. The ONA and ASIS do not produce public annual reports. The annual report of the Department of Defence makes includes general references to the activities of ASD, DIO and AGO.[462]
- Public government policy documents and operational documents, such as the *Australian Government Information Security Manual*[463] and Regulation Impact Assessments; and
- Annual and special reports by independent oversight bodies.

3.8.3. Information in relation to individual cases

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[464] 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.

In their *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* the Parliamentary Joint Committee on Intelligence and Security recommended the introduction of a mandatory data breach notification scheme by the end

---

461 For example, Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 27 February 2015 <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report>.

462 See for example Department of Defence, *Defence Annual Report 2013–14* (2014) vol 1 42–43.

463 Australian Government, ASD, *Australian Government Information Security Manual* (ISM), 2015 <http://www.asd.gov.au/infosec/ism/>

464 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>.

of 2015.[465] The Australian Government announced that it accepted this recommendation.[466] Having made a commitment to develop mandatory data breach notification laws, it was able to amend and pass the data retention amendment Bill. A draft of data breach notification law was published for comment in December 2015.[467] The exposure draft proposes that:

- Entities already exempt from the *Privacy Act* will also be exempt from this requirement and that includes intelligence agencies.
- A law enforcement body will 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.[468]
- The Commissioner's right to direct an entity to file such a notification where the Commissioner believes on reasonable grounds that there has been a serious data breach is limited in relation to enforcement bodies: An exemption is available where the chief executive officer of the enforcement body has given the Commissioner a certificate stating that the body believes on reasonable grounds that compliance with the direction would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, it.[469]

If enacted in its present form, the proposed law will enable data breaches affecting national security and law enforcement agencies to be brought to the attention of the data subject only in very limited circumstances.

---

[465] The Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) 299. A similar recommendation was made in PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, 192. Currently the Privacy Commissioner accepts data breach notifications on a voluntary basis. The Commissioner has also published guidelines to assist organisations to respond to a data breach involving personal information. Such notification is however not compelled by the *Privacy Act 1988*. See PJCIS *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) 295–296.

[466] Recommendation 38, Attorney-General's and Minister for Communications' joint media release in response to the Parliamentary Joint Committee on Intelligence and Security's *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (3 March 2015) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FirstQuarter/Government-Response-To-Committee-Report-On-The-Telecommunications-Interception-And-Access-Amendment-Data-Retention-Bill.aspx>.

[467] 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>.

[468] 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>.

[469] Cl 26WD of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015. See also Explanatory Memorandum for Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, AGD (2015), [77], [102].

Observations

Information on this topic in Australia, 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. Thought should be given to improved transparency as well as mechanisms that appropriately balance security and law enforcement needs for secrecy and confidentiality with the right of data subjects to be informed of serious privacy and data breaches, especially where that could enable them to protect themselves against loss or criminal exposure.

4. CONCLUSION

This study of Australia was undertaken as a part of a broader comparative study of Big Data and national security (*Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law in Australia, the United Kingdom, the United States, New Zealand and Canada*). An overview of the research project, including the research questions, methods and sources of empirical data, and indicators of a legal and policy framework that supports 'desirable and effective' Big Data practices can be found in the Methodology Report. Three separate Country Reports- on Australia (the current Report), Canada and the UK- provide details of the empirical findings and legal analysis in each jurisdiction. Comparative perspectives and recommendations for law reform in Australia are set out in the Executive Summary and Recommendations.

This chapter summarises the key findings and insights from the Australia study.

Interviews were conducted from 25 March 2015 to 13 November 2015 and the legal analysis present the law as it stood on 31 March 2016, except where important developments necessitated minor updates.

4.1. Using Big Data for national security: Stakeholders' perspectives

This report collected and analysed stakeholders' responses to questions regarding their use of data, their perception of risk and challenges in relation to the use of Big Data for law enforcement and national security, and their views on the regulation of data access, sharing and retention. The research is based on face-to-face interviews with 38 stakeholders (research participants) who were working in operational agencies (19 participants), policy, research and advocacy agencies or organisations (8 participants), technology companies (7 participants) or independent offices and agencies (4 participants). 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 a relatively modest sample size. The interviews explored the following broader themes:

- Current use of data
- Current concerns regarding access to data
- How problems can be overcome
- Big Data: potentials, limits and risks
- Risk of using Big Data
- Values and Big Data

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 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.**

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

General attitudes towards computer technology

Most participants in operational organisations saw digital/computer technology as both helpful and a hindrance, with three expressly recognising its inevitability.

Types of data used

Research participants 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. In some cases, data used was identified broadly as in 'a signal that can be sucked up' or 'any data that we can get our hands on lawfully'.

Types of data generated

Data generated within agencies may be in the form of reports, including text and visual elements, or may be raw data or visualisations that can be manipulated by others. Data is also generated for diverse purposes; their formats include: records of intelligence on individuals and networks, records of criminal trends, reports for internal purposes (such as performance measurement and compliance), and data to be incorporated in briefs of evidence. Such distinctions may be important when developing efficient tools to store and link agency-generated data.

Sharing of data

The sharing of data between agencies domestically and internationally is a highly curated process. 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). 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 relates to identifiable individuals. Data may also be shared with the public, either directly, through the media or through social media, for example in response to emergency situations.

Main purpose of using data

Research participants from operational organisations 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.

4.1.2. Current concerns regarding access to and sharing of data

Three main concerns were raised: 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 related to real or perceived legal requirements, including in relation to privacy issues. 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.

4.1.3. How problems can be overcome

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 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.

4.1.4. Big Data: potentials, limits and risks

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, 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.

Capability of Big Data

In terms of capability, Big Data was seen by 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: 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.

Use of Big Data and data analytics

More than half of the participants working in law enforcement and national security agencies 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.

Barriers/challenges to using Big Data

Many of the barriers and challenges to the use of Big Data listed by 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 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.

Risks of using Big Data

Overall, privacy, 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.

Overall, research participants collectively identified most of the risks discussed in the literature (see *Methodology Report* 2.3). The risk of inappropriate local application was not identified, but was largely irrelevant given the types of analysis research participants described. A more significant issue is the variability of identified risks between individuals and organisations, suggesting that broader awareness of the diversity of risks across sectors would be beneficial.

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. In particular, the most common answer to the question, who was exposed to risks, was 'everyone'. 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.

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 diverse types of risk.

4.1.5. Regulation

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 to observe the differences between groups in terms of the kinds of laws identified.

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. Some participants stated that they relied directly on legislation whereas others stated that they 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.

Accountability, transparency and oversight mechanisms

Research participants 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 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.

Appropriateness and effectiveness

Those 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 difference may follow 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 IGIS did so positively. Views on the appropriateness and effectiveness of privacy laws were more mixed.

Perceived shortcomings in law and regulation and proposals for reform

Research participants 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.

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 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.

Not all issues we raised were taken into account in design. Fewer research participants 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 gave various responses to questions about designing for agency inter-operability, including the fact that the challenges were not primarily technical.

The 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.

4.1.6. Values and Big Data

Protections where individual consents to use or sharing of their data[470]

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.

Attitudes to privacy

There was a wide spectrum of views among 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.

Privacy versus security: A scenario (see Methodology Report 5.2.2)

Participants 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, 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.

What transparency is required (see Methodology Report 5.2.8; 3.8)

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 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.

---

[470] See *Methodology Report* 5.2.5.

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.

How views align with others

Research participants 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.

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 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.

Sources of views

Research participants 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. The 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.

4.2. Big Data, law enforcement and national security: The legal environment in Australia

Early in the study, it became clear that Australia has not adopted Big Data-specific strategies, policies, laws, regulatory frameworks, practices and technologies relating to law enforcement and national security. However, it does have a host of measures that are directly or indirectly relevant to Big Data applications. To assist in differentiating between what was of greater or lesser relevance to Big Data in this context the team developed a mechanism that reflects not only what would be indicative of effective practices but also what would be desirable to balance the different policy objectives that are relevant in this context.

The initial set of indicators, though not necessarily complete, represents a useful starting point for an appropriate overarching legal and policy framework. Collectively, the presence of these indicators would indicate a framework that can support the effective use of advanced analytics and large data sets for law enforcement and national security 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, discussed in greater detail in Chapter 5 of the Methodology Report, are summarised in the following questions:

1. Is access for data mining enabled?
2. Are legal controls comprehensive and proportional?
3. Are legal rules clear, principle-based, consistent and instructive?
4. Is integrity of data and analysis supported?
5. Are data and systems protected?
6. Is accountability maintained?
7. Are principles and rules regularly reviewed?
8. Is there a sufficient measure of transparency?

4.2.1. Is access for data mining enabled?

In Australia information has traditionally been available for law enforcement purposes on the strength of warrants, such as specific-purpose search and seizure warrants, or orders setting out particulars of the information, location, time, circumstances and things (including electronic devices) that were allowed to be seized and accessed. The principles are reflected in legislation, rules of court and procedure for such orders. Big Data tools, on the other hand, are accompanied by new approaches to access to data that may require different access rules and processes.

The analysis focused on four types of data:

- government-held data,
- 'open source' data,
- privately held data,
- data held by foreign governments.

'Government-held data' refers to information stored by all levels of government (federal, state and local) in data systems. As a consequence of the *Australian Privacy Principles* (APPs) that restrict the use of personal information for a purpose unrelated to that for which it was collected and of secrecy or confidentiality provisions in laws governing government agencies and civil servants, the general principle is that data collected by an agency cannot be shared with (or more precisely, 'disclosed to') or accessed by another agency unless this is authorised under a statutory mechanism that allows such disclosure or access. Such statutory mechanisms are quite wide in scope.

Consequently, access to government-held data is governed by general exceptions and specific statutory or delegated authorisations, including those detailed in public and confidential Memorandums of Understanding (MOUs), as well as by other general mechanisms such as rules or guidelines issued by the Privacy Commissioner for particular scenarios. This means that access rules are located in a complex combination of statutes, guidelines and inter-agency agreements, some of which may not be public documents. In addition to these exception-based access rules, exceptional processes were also created to support limited sharing of data within government. The National Criminal Intelligence Fusion Capability of the Australian Crimes Commission (now being strengthened through a merger with CrimTrac and the formation of the Australian Criminal Intelligence Commission) provides an example of an exceptional process to enable sharing of government-held data to combat serious and organised crime.

This study did not locate any statutory rules specifically regulating access to '**open source**' information (such as publicly available Twitter feeds) by federal or state law enforcement or national security intelligence agencies. In the absence of such provisions it appears such ‘open’ data can be accessed, collected and shared within government, where government can gain access to the data. Technical and legal barriers may prevent such access, for example where data is held outside Australia.

A significant source of data for government agencies is data held by private corporations and persons, such a financial data and telecommunications data (‘**privately held’**) data. Substantial controls, discussed below, regulate access to such data.

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 instruments, but a holistic framework regulating these instruments and agreements is absent.

4.2.2. Are legal controls comprehensive and proportional?

A range of constitutional controls and rules about data arise from Australia’s federal structure. They involve a complex set of controls on communication of intelligence information about persons, and collecting, accessing or disclosing information for intelligence purposes. 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 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. There are however inconsistencies in both the presence and content of such 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. Australian persons are treated differently from non-Australian persons.

While 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, 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 quality and reliability of Information and data used for intelligence purposes is often, of necessity, very variable. Publicly-available information does not reflect mandatory assessment or grading of the quality and significance of the particular data (collected or analysed) that requires balancing national security purpose against adverse risks to the interests of of data subjects or third parties. The decisions of analysts regarding accessing data and the analysis of the accessed data may have profound legal, reputational and commercial implications for subjects of the assessment and it is submitted that such a test as well as a public requirement to apply the test, are important to ensure public trust in the fairness of the analytical process.

There are however general data-matching laws, guidance and protocols. These are relevant to the data analysis function but any protocols that may apply to or intra-agency or inter-agency data-matching involving law enforcement and national security agencies are not publically available.

The current rules provide insufficient opportunity for data subjects to correct their data and be notified of errors that may adversely affect their legal rights and reputation. Given the national security context, this is a sensitive matter but it would be possible to create appropriate mechanisms to provide notification in cases where it is apparent that the information may be incorrect, where personal information has been disclosed without legal authorisation, or where such information was accessed by unauthorised means.

A streamlined control framework should also improve the current patchwork of rules regarding data retention and destruction.

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

The access and control framework as described above is complex and, as indicated by research participants, these factors impact on data exchanges and flows. A lack of terminological clarity and consistency complicates the interpretation of and inter-relationship between different laws. Differing interpretations in particular are forming data access barriers in some cases.

In our view, the principles underlying the rules should be as consistent as possible across both data sets and agencies. While the subject matter is too complex and the nature and focus of the agencies too diverse to apply consistent rules across the board, or to support full consistency as desirable, it is preferable that the rules be based on consistent principles or policy. This view was also expressed by some research participants.

4.2.4. Is integrity of data and analysis supported?

Data integrity and measures to ensure integrity are important factors impacting on user confidence in the system and on public trust. While a range of policies, laws and principles are relevant to data integrity, it is not comprehensively regulated in Australia. It appears however that there is a consistent understanding of the concept of 'data integrity' between agencies in practice.

Big Data tools and culture are well known for their capacity to accept data which is less reliable, complete, accurate, up to date or relevant than usually required for data systems. But while the tools may deliver output from low integrity input or unverifiable assumptions, and preserving provenance may allow for humans to give less weight to poor quality data, the integrity of the outcome remains uncertain until the Big Data system is fully implemented and the outcomes regularly assessed. Intelligence analysts have a range of techniques that help to deal with data integrity in traditional settings. However, automating intelligence analysis give rise to serious challenges that will require appropriate control measures. Such measures are not currently evident in the statutory framework.

The *Australian Privacy Principles* formulate a general integrity standard of 'having regard to the purpose of the use or disclosure, [being] accurate, up-to-date, complete and relevant,' but its mandatory use is confined to the scope of application of the Principles, thus excluding many agencies of interest to this study. The *Australian Government Big Data Strategy* is a recent and pertinent model which includes among its six principles, 'Principle 3: Data integrity and the transparency of processes'. The notion of 'integrity' is embedded as a feature of the project, its governance and of the data *per se.* A clear concept of 'data integrity' will facilitate the incorporation of different data sets into a Big Data system.

4.2.5. Are data and systems protected?

Australia 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.

A number of the current data security policies are general and do not address Big Data issues explicitly, or else they may not cover criminal intelligence and national security concerns in depth. However, they offer a well-established and widely understood framework within which Big Data security issues can be addressed. In addition, to the extent that these tools make use of access to data in other repositories rather than entirely replicated special purpose copies or abstracts of such data sets, the general requirements apply.

The current data security standards framework reflects dynamic mechanisms that seek to address risks as they arise in a coherent manner. It provide an example of a standards-based approach that could serve the dynamic and challenging legal and policy needs of Big Data solutions for national security purposes, especially if the gaps are addressed, and there is a watching brief alert to unexpected impacts on affected parties.

The general legal framework will however be improved with the enactment of mandatory data breach notification. The proposed legislation in that regard is however too limited in relation to national security and law enforcement agencies. A statutory tort that specifically applies to a serious intrusion of privacy or to consequences resulting from inadequate security is also required. Individuals currently may not generally have a clear and enforceable remedy in circumstances where there is unlawful or inappropriate access or use of that individual's data as a result of inadequate security.

4.2.6. Is accountability maintained?

Independent oversight is a crucial component of the current regulatory regime.

The Australian oversight bodies are able to perform and do perform important functions. No single body, however, 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. Mindful of the need to cooperate, especially where powers and scope may overlap, the bodies 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. There is also little indication of a consistent investigation of MOUs or of monitoring of compliance with MOUs that regulate access to and exchange of data.

The quality and effectiveness of oversight is dependent on the availability of information and records evidencing decisions and decision-making processes. The *Archives Act* tries to balance operational secrecy required by law enforcement and intelligence agencies with the need of the public and future generations to access government information when it is not sensitive. In many cases, sensitivity generally declines over time and as a result key documents can be made available after a period of time. Where the time period is too long, the documents are only of historic interest. The *Archives Act* does therefore not empower the public to access information regarding the development and implementation of Big Data systems within time periods that would enable the public to hold authorities accountable.

The relatively short periods for the retention of key documents regarding the development and implementation of technological and telecommunications systems are also unhelpful. While the retention of the documents do support short-term independent oversight functions, most of the relevant operational documents will be destroyed long before the disclosure period under the *Archives Act* commences. Document destruction may also undermine the longer term assessment of design decisions that informed analytical systems employed by agencies.

Complaints processes are important mechanisms to draw attention to possible administrative problems. Existing mechanisms, especially enhanced by the *Public Interest Disclosure Act 2013 (Cth)*, can inform and support the functioning of the of the independent oversight bodies. External complaints can, however, only be lodged by persons who have sufficient knowledge about the access or handling of their data to feel aggrieved. The lack of disclosure of relevant practices lessens the chances of such complaints being lodged.

4.2.7. Are principles and rules regularly reviewed?

Big Data tools and applications in this area are in a state of rapid evolution and development. Risks and opportunities may not be clear or be fully appreciated and relevant rules may prove not to be appropriate or sufficient. An appropriate Big Data framework will require 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 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.

4.2.8. Is there a sufficient measure of transparency?

There is large body of general information available regarding law enforcement and security agencies. The information must however be parsed from a large range of documents. Even then, it remains partial and general. It does not enable Australians to know whether their data collected by one government agency was shared with another domestic or even foreign agency and how their data is being analysed and used. For Big Data systems to enjoy the measure of public confidence required, thought must be given to sensitive ways to appropriately provide sufficient transparency, recognising the need for secrecy and the vulnerabilities that may accompany over-disclosure. Balanced data breach notification measures will also enhance transparency. The impact of the proposed mandatory data breach notification legislation will however be too limited in relation to national security and law enforcement agencies to enhance public confidence that the appropriate balance was attained.