TECHNICAL REFERENCES

Big Data Technology and National Security

Comparative International Perspectives on
Strategy, Policy and Law

Law and Policy Program
Data to Decisions Cooperative Research Centre

June 2018

Research Team

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

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

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

Technical References

This volume contains a series of supplementary technical reference materials which support the other Reports, particularly the *Australia Report*.

Authors
Technical Reference 1: David Vaile, Alana James
Technical Reference 2: David Vaile, Alana James
Technical Reference 3: David Vaile
Technical Reference 4: David Vaile
Technical Reference 5: Danuta Mendelson, David Vaile, Alana James
Technical Reference 6: Danuta Mendelson, Alana James, David Vaile
Technical Reference 7: David Vaile, Alana James
Technical Reference 8: Alana James, David Vaile
Technical Reference 9: Danuta Mendelson, Alana James, David Vaile
Technical Reference 10: David Vaile
Technical Reference 11: David Vaile, Alana James
Technical Reference 12: Janet Chan, Lyria Bennett Moses, Alana Maurushat, Louis de Koker

Other Reports from this Project

Australia Report
Canada Report
UK Report
Methodology Report
Comparative Report

Select Bibliography

Table of Contents – Technical References

TR 1. Relevant Australian laws, by category.

Laws are grouped by online or general application, and by application to types of entities. This is not an exhaustive list. It lists principal Acts with a small selection of the more relevant recent amending Acts. See the References List for a more comprehensive selection.

Category	Laws
Laws applicable to data related to telecommunications and networks	*Telecommunications Act 1997* (Cth) ('TA') *Telecommunications (Interception and Access) Act 1979* (Cth) ('TIA Act') *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011 (Cth)* *Telecommunications (Interception and Access) (Data Retention) Act 2015* (Cth) ('TIADRA' or 'Retention Act')
Laws applicable generally	*Acts Interpretation Act* (1901) (Cth) *Anti-Terrorism Act 2004* (Cth) (and others) *Archives Act 1983* (Cth) *Data-matching Program (Assistance and Tax) Act 1990* (Cth) *Evidence Act 1995* (Cth) *Financial Transaction Reports Act 1988* (Cth) ('FTR Act') *Freedom of Information Act 1982* (Cth) ('FOIA') *Income Tax Assessment Act 1936* (Cth) ('ITAA') *Public Governance, Performance and Accountability Act 2013* (Cth) ('PGPAA') *Public Service Act 1999* (Cth) ('PSA') *Privacy Act 1988* (Cth) ('PA') State laws include: *Invasion of Privacy Act 1971* (Qld) *Listening and Surveillance Devices Act 1972* (SA) *Listening Devices Act 1984* (NSW) *Surveillance Devices Act 2000* (NT) *Listening Devices Act 1991* (Tas) *Listening Devices Act 1992* (ACT)] *Surveillance Devices Act 1999* (Vic) *Surveillance Devices Act 1998* (WA)
National security and intelligence entity-specific laws (NS)	*Australian Security Intelligence Organisation Act 1979* (Cth) ('ASIO Act') *Charter of the United Nations Act 1945* (Cth) Part 4 *Crimes Act 1914* (Cth) (Part IAA Div 3A and ss 15AA and 19AG; Part IC relating to terrorism offences, and other provisions as far as they relate to these - *INSLM Act* s 4) *Criminal Code Act 1995* (Cth) ('CCA') (*Criminal Code* Ch 5 and provisions as far as they relate to it) *Defence Act 1903* (Cth) (Part IIIAAA etc.)

	Independent National Security Legislation Monitor Act 2010 (Cth) (INSLMA) *Intelligence Services Act 2001* (Cth) ('ISA') *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) *Office of National Assessments Act 1977* (Cth) ('ONA Act') *Inspector-General of Intelligence and Security Act 1986* (Cth) (IGISA)
Law enforcement entity-specific laws (LE) (or both LE and NS)	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) *Australian Border Force Act 2015* (Cth) *Australian Crime Commission Act 2002* (Cth) *Crimes Act 1914* (Cth) *Criminal Code Act 1995* (Cth) ('CCA') *Crimes Legislation Amendment (Powers and Offences) Act* 2012 (Cth) ('CLAPOA') *Cybercrime Legislation Amendment Act* 2012 (Cth) *Mutual Assistance in Criminal Matters Act 1987* (Cth) ('MACM Act') *Proceeds of Crime Act 2002* (Cth) *Surveillance Devices Act 2004* (Cth) ('SDA') Various state police and oversight/corruption agency laws *Police Act 1990* (NSW) *Police Powers and Responsibilities Act 2000* (Qld) *Police Act* of 2013 (Vic)
Other entity-specific laws	*Australian Border Force Act 2015* (Cth) ('ABF Act') *Data-matching Program (Assistance and Tax) Act 1990* (Cth) ('DMATA') *Taxation Administration Act 1953* (Cth) ('TAA')

TR 2. Australian agencies with national security and law enforcement roles

Agencies are categorised differently by various legislation, and have some roles overlapping. Those below are of most potential interest in this report.

Table of relevant agencies

Type of agency	Agencies
Intelligence agencies - domestic focus	• Australian Security Intelligence Organisation (ASIO) • Australian Government Security Vetting Agency (AGSVA) • Defence Security Authority (DSA)
Intelligence agencies - foreign focus	• Australian Secret Intelligence Service (ASIS) (part of DFAT) • Australian Geospatial-Intelligence Organisation (AGO) (former DIGO; part of Defence) • Australian Signals Directorate (ASD) (former DSD; part of Defence) • Office of National Assessments (ONA) (under PM) • Defence Intelligence Organisation (DIO) (part of Defence)
Criminal Law Enforcement and Police agencies	• Australian Capital Territory Policing (ACTP) • Australian Federal Police (AFP) • New South Wales Police Force (NSWPF) • Northern Territory Police (NTP) • Queensland Police Service (QPS) • South Australia Police (SAP) • Tasmania Police (TP) • Victoria Police (VP) • Western Australia Police (WAP) • Royal Australian Corps of Military Police (RACMP)
Commonwealth law enforcement	• Australian Border Force (ABF) • Australian Communications and Media Authority (ACMA) • Australian Competition and Consumer Commission (ACCC) • Australian Crime Commission (ACC) • Australian Defence Force Investigative Service (ADFIS) • Australian Hi-Tech Crime Centre (AHTCC) • Australian Information Commissioner (AIC) • Australian Prudential Regulation Authority (APRA) • Australian Quarantine and Inspection Service (AQIS) *[omit?]* • Australian Securities and Investments Commission (ASIC) • Australian Security Intelligence Organisation (ASIO) • Australian Taxation Office (ATO) • Immigration and Border Protection Department (IBPD)
Commonwealth review and integrity	• Australian Commission for Law Enforcement Integrity (ACLEI) • Independent National Security Legislation Monitor (INSLM) • Inspector-General Defence (IGD) • Inspector General of Intelligence and Security (IGIS) • Commonwealth Ombudsman (CO) • Privacy Commissioner (PC)

Type of agency	Agencies
State/territory review and integrity (including oversight bodies or inspectors of each)	• Corruption and Crime Commission (WA) (CCC-WA) • Parliamentary Inspector of the Corruption and Crime Commission (WA) • Crime and Corruption Commission (Qld) (CCC-Q) (See also Crime and Misconduct Commission of Queensland) • Independent Broad-based Anti-corruption Commission (IBAC) • Victorian Inspectorate [covers IBAC] • Independent Commission Against Corruption (NSW) (ICAC) • Inspector of the Independent Commission Against Corruption (NSW) • New South Wales Crime Commission (NSW) (CC-NSW) • Police Integrity Commission (NSW) (PIC) • Inspector of the Police Integrity Commission (NSW) • Office of Police Integrity (Vic) (OPI) • Victorian Integrity and Anti-Corruption Commission (Vic) (VIACC) • Gold Stealing Detection Unit (WA) (GSDU)
Local Government and other agencies with enforcement roles[1]	• Local councils • RSPCA • Other?

[1] PJCIS, *Advisory Report on Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015

TR 3. Abbreviations and Acronyms

See also the *Methodology Report* for this project.

AAA	Australian Airports Association
AAT	Administrative Appeals Tribunal
ABF	Australian Border Force
ACAT	Aviation Criminal Assessment Team
ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
ACC Act	Australian Crime Commission Act 2002
ACC Board	Australian Crime Commission Board
ACC	Australian Crime Commission
ACID	Australian Criminal Intelligence Database
ACIF	Australian Criminal Intelligence Forum
ACIM	Australian Criminal Intelligence Model
ACIMS	Australian Criminal Intelligence Management Strategy
ACLEI	Australian Commission for Law Enforcement Integrity
ACTC	Australian Counter Terrorism Centre
ADF	Australian Defence Force
ADR	alternative dispute resolution
AEMVF	Australian Emergency Management Volunteer Forum
AFAC	Australasian Fire and Emergency Service Authorities Council
AFP	Australian Federal Police
AFPA	Australian Federal Police Association
AGD	Attorney-General's Department
AGDRP	Australian Government Disaster Recovery Payment
AHRC	Australian Human Rights Commission
AIC	Australian Intelligence Community
AIPJ	Australia Indonesia Partnership for Justice
ALEIN	Australian Law Enforcement Intelligence Network
All-in	'All-in' airport policing model
ALRC	Australian Law Reform Commission
AMTA	Australian Mobile Telecommunications Association
ANAO	Australian National Audit Office
ANZPAA	Australian New Zealand Policing Advisory Agency
ANZTC	Australia-New Zealand Counter-Terrorism Committee
APCERT	Asia Pacific CERT (computer emergency response team)
APEC	Asia-Pacific Economic Cooperation
APP	Australian Privacy Principles
APS	Australian Public Service
APSC	Australian Public Service Commission
AQIS	Australian Quarantine Inspection Service
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASU	Australian Services Union
ATO	Australian Taxation Office
ATSA	Aviation Transport Security Act 2004
ATSILS	Aboriginal and Torres Strait Islander Legal Service
AusAID	Australian Agency for International Development
AusCheck	Australian Background Checking Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
AvSec	Aviation Security Service (New Zealand)
BCR	Building Community Resilience Grants
Beale Audit	Federal Audit of Police Capabilities
CAC	Communications Access Co-ordinator
CAC Act	Commonwealth Authorities and Companies Act 1997
CAP-AU-STD	Common Alerting Protocol - Australian Profile
CASA	Civil Aviation Safety Authority
CCC	Crisis Coordination Centre
CCS	Children's Contact Service
CCTV	Closed-circuit television
CDPP	Commonwealth Director of Public Prosecutions
CEF	Container Examination Facility
CEPO	Community Engagement Police Officer
CERT	Computer Emergency Response Team
CIPMA	Critical Infrastructure Program for Modelling and Analysis
CIR	Critical Infrastructure Resilience
CLCS	UN Commission on the Limits of the Continental Shelf
CNI	Certificates of No Impediment
COAG	Council of Australian Governments
COBRA	Classification Operations Branch Records Administration
Commonwealth Framework	Commonwealth Organised Crime Strategic Framework

CPGs	Commonwealth Procurement Guidelines
CSP	Carriage Service Provider
CrimTrac	CrimTrac
Customs Act	*Customs Act 1901*
Customs	Australian Customs and Border Protection Service (now DIBP/ABF)
CVE	countering violent extremism
CVESC	Countering Violent Extremism Sub-Committee
DBCDE	Department of Broadband, Communications and the Digital Economy
DIBP	Dept of Immigration and Border Protection
DNA	deoxyribonucleic acid
DOORS	Detection Of Overall Risk Screen
DVS	Document Verification Service
ECHR	European Court of Human Rights
ECJ	European Court of Justice
EM	Explanatory Memorandum
EU	European Union
FaHCSIA	Department of Families, Housing, Community Services and Indigenous Affairs
FASO	family and sexual offences
FMA Act	*Financial Management and Accountability Act 1997*
FOI	Freedom of Information
Fusion	Criminal Intelligence Fusion Capability
HOCOLEA	Heads of Commonwealth Operational Law Enforcement Agencies
IBAC	Independent broad-based anti-corruption commission
ICAC	South Australian Independent Commissioner Against Corruption
ICAO	International Civil Aviation Organisation
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICL	Independent Children's Lawyer
ICS	Integrated Cargo System
IGIS	Inspector General of Intelligence and Security
ILSAC	International Legal Services Advisory Council
ILUA	Indigenous Land Use Agreement
IMO	International Maritime Organisation
IP	Internet Protocol, hence IP address
IPA	Institute of Public Affairs
ISOC-AU	Internet Society of Australia (now Internet Australia, IA)
ISP	Internet Service Provider (a Carriage Service Provider or CS Intermediary)
ISPS Code	International Ship and Port Facility Security Code
ISS	International Social Service Australia
ITSA	Insolvency and Trustee Service Australia
JAIG	Joint Aviation Intelligence Group
JAIT	Joint Aviation Investigation Team
KCLS	Kimberley Community Legal Service
Law Council	Law Council of Australia
LBS	location-based solution
LSMUL	Legal Services Multi-Use List
Maritime regulations	Maritime Transport and Offshore Facilities Regulations 2003
MCPEMP	Ministerial Council for Police and Emergency Management—Police
MEAA	Media Entertainment and Arts Alliance
MoU	Memorandum of Understanding
MSIC	Maritime Security Identification Card
MTOFSA	Maritime Transport and Offshore Facilities Security Act 2003
MUA	Maritime Union of Australia
NADRAC	National Alternative Dispute Resolution Advisory Council
NCCCP	National Crisis Coordination Capability Program
NCS	National Classification Scheme
NCTC	National Counter-Terrorism Committee
NCTR	National Criminal Target Report
NDRP	Natural Disaster Resilience Program
NDRRA	Natural Disaster Relief and Recovery Arrangements
NEMC	National Emergency Management Committee
NEMVAP	National Emergency Management Volunteer Action Plan
NIINA	National Information and Intelligence Needs Analysis
NISS	National Identity Security Strategy
NNTT	National Native Title Tribunal
NOCRP	National Organised Crime Response Plan
NPRS	National Police Reference System
NSA	National Security Agency (US)
NSCDD	National Security Capability Development Division
NSDR	National Strategy for Disaster Resilience
NSW	New South Wales
NT	Northern Territory
NTS	National Target System
OAIC	Office of the Australian Information Commission
OCA	*Organised Crime in Australia* Report (various years)
OCRP	Organised Crime Response Plan

OCSF	Organised Crime Strategic Framework
OCTA	Organised Crime Threat Assessment
OLDP	Office of Legislative Drafting and Publishing
OLSC	Office of Legal Services Coordination
ONA	Office of National Assessments
OPC	Office of Parliamentary Counsel
OPCAT	Optional Protocol to the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
OPP	Office of the Public Prosecutor in Papua New Guinea
OTS	Office of Transport Security
PAES	Portfolio Additional Estimates Statements
PBS	Portfolio Budget Statements
PFA	Police Federation of Australia
PHBR	Parliament House Briefing Room
PIA	Privacy Impact Assessment
PILON	Pacific Island Officers' Network
PIM	Victorian Public Interest Monitor
PJC-ACC	Parliamentary Joint Committee on the Australian Crime Commission
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PJCLE	Parliamentary Joint Committee on Law Enforcement
PNG	Papua New Guinea
PPATK	the Indonesian Government's Financial Intelligence Unit
PPS	Personal Property Securities
PPSA	Personal Property Securities Act 2009
PPSR	Personal Property Securities Register
PSM	Public Service Medal
PSO	AFP Protective Services Officer
RAP	Reconciliation Action Plan
RFI	Request for Information
RIS	Regulation Impact Statement
SA	South Australia
SACL	Sydney Airport Corporation Limited
SACS	social and community services
SCAG	Standing Committee of Attorneys-General
SCLJ	Standing Council on Law and Justice
SCPEM	Standing Council on Police and Emergency Management
SCPEM	Standing Council on Police and Emergency Management
SES	Senior Executive Service
SGP	Strongim Gavman Program
SLCAC	Senate Legal and Constitutional Affairs Committee
SLF Program	Strengthening Legal Frameworks to Counter Terrorism Program
Smith Review	Review of Homeland and Border Security
SOCN	Serious and organised crime networks
SOG on OC	Senior Officers' Group on Organised Crime
TIA Act	*Telecommunications (Interception and Access) Act 1979*
TISN	Trusted Information Sharing Network
TRAM	Threat Risk Assessment Methodology
TWU	Transport Workers Union
UN	United Nations
UNCAC	United Nations Convention against Corruption
UNCITRAL	United Nations Commission on International Trade Law
UNODC	United Nations Office on Drugs and Crime
UPM	Universal Policing Model
URL	Uniform resource locator (translated from IP address by DNS)
VI	Victorian Inspectorate
VIC	Visitor Identification Card
VOIP	Voice over Internet Protocol
WA	Western Australia
WHS	work health and safety
WIPO	World Intellectual Property Organization
WPSS	Wireless Priority Service System
WTO	World Trade Organization

TR 4. ASIS Privacy Rules

<https://www.asis.gov.au/Privacy-rules.html>

Rules to Protect the Privacy of Australians

I, Robert John Carr, Minister for Foreign Affairs, being the Minister responsible for the Australian Secret Intelligence Service (ASIS), revoke the Rules to Protect the Privacy of the Australians made by Stephen Francis Smith, the then Minister for Foreign Affairs, on 17 September 2008 and make the attached rules, in accordance with section 15 of the *Intelligence Service Act 2001* ("the Act"), regulating the communication and retention by ASIS of intelligence information concerning Australian persons.

Before making the attached rules, I have:

a. provided a copy of the rules I am proposing to make to the Inspector-General of Intelligence and Security (IGIS) and Attorney-General; and
b. consulted the Director-General of ASIS, the IGIS and the Attorney-General.

Expressions used in the attached rules have the same meaning as in the Act.

Rule 1: Protecting the privacy of Australian persons – presumptions

1.1 These rules regulate the communication and retention of intelligence information concerning Australian persons. Where it is not clear whether a person is an Australian person

a. a person within Australia is to be presumed to be an Australian person; and
b. a person outside Australia is to be presumed not to be an Australian person;

unless there is evidence to the contrary, including from the context in which the information was collected or the content of the information.

Rule 2: Retention of intelligence information concerning Australian persons

2.1 ASIS may retain intelligence information concerning an Australian person only where it is necessary to do so for the proper performance of ASIS's functions or the retention is authorised or required by or under another Act.

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; and

b. access to that information is only to be provided to persons who require such access for the proper performance of an ASIS function.

Rule 3: Communication of intelligence information concerning Australian persons

3.1 ASIS may communicate intelligence information concerning Australian persons only where it is necessary to do so for the proper performance of ASIS's functions or where such communication is authorised or required by or under another Act. In addition, the following specific rules apply.

Information that is important for specified purpose

3.2 Intelligence information concerning an Australian person may be communicated where:

a. the information is publicly available; or

b. 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; or

c. deletion of that part of the information concerning the Australian person would significantly diminish the utility of the information for the purposes of:

(i) maintaining Australia's national security;

(ii) maintaining Australia's national economic well-being;

(iii) promoting Australia's foreign relations;

(iv) preventing or investigating the commission of a serious crime; or

(v) responding to an apparent threat to the safety of a person; or

d. the information concerns an Australian person who is, or was at the time the information was collected, the subject of an authorisation given by the Minister under section 9 of the Act.

Communication to ASIO, DIGO or ASD for their purposes

3.3 Intelligence information concerning an Australian person may be communicated to ASIO, DIGO or ASD (as the case requires) where it relates, or appears to relate, to the performance of the functions of the relevant agency.

Rule 4: Communication of information not deliberately collected

4.1 ASIS may communicate intelligence information concerning an Australian person that was not deliberately collected to an authority that ASIS is permitted to cooperate with, provided the authority has been approved by the Minister for the purpose of this rule.

4.2 Before approving an authority for the purpose of rule 4.1, the Minister is to be satisfied that there are satisfactory arrangements in place to ensure that the authority will abide by the ASIS privacy rules.

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.

Rule 6: Oversight by the IGIS

6.1 To facilitate the oversight role of the IGIS, ASIS is to take the following measures:

a. the IGIS is to have access to all intelligence information held by ASIS concerning Australian persons;

b. the IGIS is to be consulted about the processes and procedures applied by ASIS to the communication and retention of information concerning Australian persons; and

c. where a presumption under rule 1.1(b) has been found to be incorrect ASIS is to advise the IGIS of the incident and measures taken by ASIS to protect the privacy of the individual; and

d. in any case where a breach of these rules is identified, ASIS is to advise the IGIS of the incident and the measures taken by ASIS to protect the privacy of the Australian person or of Australian persons generally.

Rule 7: Public access to the rules

7.1 ASIS is to ensure that a copy of these rules is publicly available on the ASIS website.

TR 5. ASD Privacy Rules

<http://www.asd.gov.au/publications/broadcast/20121002-privacy-rules.htm>

Rules to Protect the Privacy of Australians

Made by the Minister for Defence, 2 October 2012

Letter of Introduction

I, Stephen Francis Smith, Minister of State for Defence, being the Minister responsible for the Australian Signals Directorate (ASD), hereby make the attached rules, in accordance with section 15 of the Intelligence Services Act 2001 ("the Act"), regulating the communication and retention by DSD of intelligence information concerning Australian persons. In making the attached rules, I have had regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by DSD of its functions.

Before making the attached rules, I have:

a. consulted the Director of DSD, the Inspector-General of Intelligence and Security (IGIS) and the Attorney-General; and
b. provided a copy of the rules I was proposing to the IGIS and Attorney-General.

Dated this 2nd day of October 2012
[Signed] Stephen Smith

Rules to Protect the Privacy of Australians

Rule 1: Protecting the privacy of Australian persons – presumptions

1.1 These rules regulate the communication and retention of intelligence information concerning Australian persons. Where it is not clear whether a person is an Australian person:

a. a person within Australia is to be presumed to be an Australian person; and

b. a person outside Australia is to be presumed not to be an Australian person;

unless there is evidence to the contrary, including from the context in which the information was collected or the content of the information.

Rules 2: Retention of intelligence information concerning Australian persons

2.1 DSD may retain intelligence information concerning an Australian person only where it is necessary to do so for the proper performance of DSD's functions or the retention is authorised or required by another Act.

2.2 Where DSD does retain intelligence information concerning an Australian person, DSD 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; and

b. access to that information is only to be provided to persons who require such access for the proper performance of a DSD function.

Rule 3: Communication of intelligence information concerning Australian persons

3.1 DSD may communicate intelligence information concerning Australian persons only where it is necessary to do so for the proper performance of DSD's functions or where such communication is authorised or required by or under another Act. In addition, the following specific rules apply.

Information that is important for specified purpose

3.2 Intelligence information concerning an Australian person may be communicated where:

a. the information is publicly available; or

b. 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; or

c. deletion of that part of the information concerning the Australian person would significantly diminish the utility of the information for the purposes of:

i. maintaining Australia's national security

ii. maintaining Australia's national economic well-being

iii. promoting Australia's foreign relations

iv. preventing or investigating the commission of a serious crime

v. responding to an apparent threat to the safety of a person, or

d. the information concerns an Australian person who is, or was at the time the information was collected, the subject of an authorisation given by the Minister under section 9 of the Act.

Communication to ASIS, ASIO or DIGO for their purposes

3.3 Intelligence information concerning an Australian person may be communicated to ASIS, ASIO or DIGO (as the case requires) where it relates, or appears to relate, to the performance of the functions of the relevant agency.

Rule 4: Communication of information not deliberately collected

4.1 DSD may communicate intelligence information concerning an Australian person that was not deliberately collected to an authority that DSD is permitted to cooperate with, provided the authority has been approved by the Minister for the purpose of this rule.

4.2 Before approving an authority for the purpose of rule 4.1, the Minister is to be satisfied that there are satisfactory arrangements in place to ensure that the authority will abide by the DSD privacy rules.

Rule 5: Accuracy of information

5.1 DSD is to take reasonable steps to ensure that intelligence information that DSD retains or communicates concerning Australian persons is recorded or reported in a fair and reasonable manner.

Rule 6: Oversight by the IGIS

6.1 To facilitate the oversight role of the IGIS, DSD is to take the following measures:

a. the IGIS is to have access to all intelligence information held by DSD concerning Australian persons;

b. the IGIS is to be consulted about the processes and procedures applied by DSD to the communication and retention of information concerning Australian persons; and

c. where a presumption under rule 1.1(b) has been found to be incorrect DSD is to advise the IGIS of the incident and measures taken by DSD to protect the privacy of the individual; and

d. in any case where a breach of these rules is identified, DSD is to advise the IGIS of the incident and the measures taken by DSD to protect the privacy of the Australian person or of Australian persons generally.

Rule 7: Public access to the rules

7.1 DSD is to ensure that a copy of these rules is publicly available on the DSD website.

[NB: these DSD/ASD Rules are reflected in identical terms in Rules for DIGO/AGO made on the same date by the Minister.]

TR 6. Examples of Ministerial Powers to directly authorise access

These examples demonstrate instances where access to relevant information or data can be directly authorised by a Minister.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 This differs from the Intelligence Services Act, which requires the responsible minister to personally authorise …. Instead the AUSTRAC CEO may authorise and in some cases the Director General of ASIS and the Director General of ONA may authorise …
126 Access by designated agencies to AUSTRAC information (1) The AUSTRAC CEO may, in writing, authorise specified officials, or a specified class of officials, of a specified designated agency to have access to AUSTRAC information for the purposes of performing the agency's functions and exercising the agency's powers. (2) An authorisation under subsection (1) is not a legislative instrument.
132 Communication of AUSTRAC information to a foreign country etc. - Foreign country (1) The AUSTRAC CEO may communicate AUSTRAC information to the government of a foreign country if the AUSTRAC CEO is satisfied that: Foreign law enforcement agency—access by Commissioner of the Australian Federal Police to AUSTRAC information (2) The AUSTRAC CEO may, in writing, authorise the Commissioner of the Australian Federal Police to have access to AUSTRAC information for the purposes of communicating the information to a foreign law enforcement agency under subsection (3).
133A When the Director-General of ASIS may communicate AUSTRAC information to a foreign intelligence agency S 133A(1) The Director-General of ASIS may communicate AUSTRAC information to a foreign intelligence agency if the Director-General is satisfied that: (2) The Director-General of ASIS may, in writing, authorise an ASIS official to access the AUSTRAC information and communicate it to the foreign intelligence agency on the Director-General's behalf.
133C When the Director-General of ONA may communicate AUSTRAC information to a foreign intelligence agency 133C(1) The Director-General of ONA may communicate AUSTRAC information to a foreign intelligence agency if the Director-General is satisfied that: (2) The Director-General of ONA may, in writing, authorise an official of ONA to access the AUSTRAC information and communicate it to the foreign intelligence agency on the Director-General's behalf.

Telecommunications (Interception and Access) Act 1979

Under the Telecommunications (Interception and Access) Act 1979 the Attorney-General may by warrant under his hand authorise telecommunications intercepts…

In an emergency the Director-General of Intelligence may issue a warrant for up to a 48 hour period and must notify the Attorney-General and Inspector General.

For foreign intelligence communications warrants the Attorney-General may authorise on advice of the Minister of Defence and the Minister for Foreign Affairs …

A judge of nominated AAT member may issue a telecommunications service warrant.

9 Issue of telecommunications service warrants by Attorney-General

(1) Where, upon receipt by the Attorney-General of a request by the Director-General of Security for the issue of a warrant under this section in respect of a telecommunications service, the Attorney-General is satisfied that:

the Attorney-General may, by warrant under his or her hand, authorize

10 Issue of warrant by Director-General of Security in emergency for Organisation to intercept telecommunications

the Director-General of Security may, by warrant under his or her hand,

11C Foreign communications warrant for collection of foreign intelligence

11C(1) Where: (a) the Director-General of Security gives a notice in writing to the Attorney-General requesting the Attorney-General to issue a warrant under this section authorising persons approved under section 12 in respect of the warrant to intercept foreign communications for the purpose of obtaining foreign intelligence relating to a matter specified in the notice; and

(b) the Attorney-General is satisfied, on the basis of advice received from the Minister for Defence or the Minister for Foreign Affairs, that:

the Attorney-General may, by warrant under his or her hand, authorise persons approved under section 12 in respect of the warrant, subject to any conditions or restrictions that are specified in the warrant, to intercept foreign communications for the purpose of obtaining that intelligence.

46 Issue of telecommunications service warrant

(1) Where an agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service, the Judge or nominated AAT member may, in his or her discretion, issue such a warrant.

Australian Security Intelligence Organisation Act 1979 The Minister may issue a [search s25] warrant and a [computer access s25A] warrant and a [surveillance devise s26] warrant and a [inspection of postal articles s27] warrant…
Section 27A: the Minister under his own hand may issue a foreign intelligence warrant 25 Search warrants - Issue of search warrant 25 (1) If the Director-General requests the Minister to do so, and the Minister is satisfied as mentioned in subsection (2), the Minister may issue a warrant in accordance with this section.
25A Computer access warrant - Issue of computer access warrant (1) If the Director-General requests the Minister to do so, and the Minister is satisfied as mentioned in subsection (2), the Minister may issue a warrant in accordance with this section.
26 Issue of surveillance device warrants (1) If the Director-General requests the Minister to do so, and the Minister is satisfied as mentioned in subsection (3), the Minister may issue a warrant in accordance with this section.

Crimes Act 1914

Allows an issuing officer to sign a warrant.

3E When search warrants can be issued:

3E(1) An issuing officer may issue a warrant to search premises if the officer is satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises.

Defence Act 1903

8 Powers of Minister in relation to Defence Force

The Minister shall have the general control and administration of the Defence Force, and the powers vested in the Chief of the Defence Force, the Chief of Navy, the Chief of Army and the Chief of Air Force by virtue of section 9, and the powers vested jointly in the Secretary and the Chief of the Defence Force by virtue of section 9A, shall be exercised subject to and in accordance with any directions of the Minister.

Australian Crime Commission Act 2002

ACCA allows an issuing officer to authorise warrants.

S 22 Search warrants

(1) An eligible person may apply to an issuing officer for the issue of a warrant under subsection (2) if:

(2) Where an application under subsection (1) is made to an issuing officer, the issuing officer may issue a warrant authorizing a member of the Australian Federal Police or of the Police Force of a State, or any other person, named in the warrant, with such assistance as he or she thinks necessary and if necessary by force:

(a) to enter upon the land or upon or into the premises, vessel, aircraft or vehicle;

(b) to search the land, premises, vessel, aircraft or vehicle for things of the relevant kind; and

(c) to seize any things of the relevant kind found upon the land or upon or in the premises, vessel, aircraft or vehicle and deliver things so seized to any person participating in the special ACC operation/investigation.

TR 7. Exceptions to state listening device prohibitions on interception and surveillance

CCH provides a useful table showing the various means to lawfully use devices for surveillance in its *Privacy Service* at [12-160].

Table 8.7A - Listening Devices Legislation

COMPARISON OF STATE AND TERRITORY LISTENING DEVICES LEGISLATION						
Jurisdiction	**Exception**					
	Authorisation by warrant	Authorisation under Commonwealth law	Urgent circumstances such as an imminent threat of serious violence to a person or substantial damage to property, or when there is a reasonable belief that it is necessary to use a listening device because a serious drug offence is about to be committed	Information unintentionally obtained in an otherwise lawful recording	Record of police interview	Consent of either one or all parties to the conversation
ACT (*Listening Devices Act 1992*)		×		×		× (consent of both parties required)
NT (*Surveillance Devices Act 2007*)	×	×	×	×		× (use of device by one party not prohibited)
NSW (*Surveillance Devices Act 2007*)	×	×	×	×		× (consent of both parties required, with limited exception for protection of lawful interests)

COMPARISON OF STATE AND TERRITORY LISTENING DEVICES LEGISLATION						
Qld (*Invasion of Privacy Act 1971)*	× (and *Drugs Misuse Act 1986* in respect of drug offences)	×	× (and *Drugs Misuse Act 1986* in respect of drug offences)	×	×	× (use of device by one party not prohibited)
SA (*Listening Devices Act 1972*)	×					× (use of device by one party not prohibited)
Tas (*Listening Devices Act 1991*)	×	×	×	×	×	× (consent of both parties required)
Vic (*Surveillance Devices Act 1999*)	×	×		×		× (use of device by one party not prohibited)
WA (*Surveillance Devices Act 1998*)	×	×		×		× (use of device by one party not prohibited)
× Jurisdictions in which the exception to the prohibition on use of listening devices applies.						

TR 8. MOUs and access to data by agencies

A Memorandum of Understanding (MoU) is an agreement between agencies setting out the terms of their provision of data, or access to data, to each other, subject to their statutory rules. Some of the MoUs which are public are set out below. They may not be readily available in the public domain for national security intelligence information.

The table below covers a sample of MOUs and indicates the parties, whether they are public and, if known, whether they address further distribution. They cover a number of other provisions. Here, the focus is on control of access.

Agency	MOUs with?	Public?	Content [2]
ISA agencies (ASIS DIO, ONA, DGO) DGO	Australia Radiation Protection & Nuclear Safety Agency (date unknown)	**No** Existence identified in senate file list.[3]	N/A. Not public.
ASIO	AUSTRAC (date unknown)	**No[4]**	• **Scope:** ASIO has online access to AusTrac financial transaction report databases • **Transfer to offshore agencies:** ASIO may communicate this information to foreign intelligence agencies provided an appropriate undertaking as to confidentiality are given by the foreign agency.
ASIO	All state and territory police (date unknown)	**No.** Existence identified in Vic Pol report,[5]	N/A. Not public.
AFP	APRA (7 July 2014)	**Yes[6]**	• **Transfer to other agencies:** with consent or as required by law ([11] – [13]). If consent, condition that agency will keep information confidential
AUSTRAC	APRA (18 February 2007)	**Yes [7]**	• **Transfer to other agencies:** with consent or as required by law [6.5] • **Notification of data breach:** must notify the agency whose information was disclosed [10.4]

[2] Re: disclosure to third party in AU or offshore; auditing onward distribution; data breach obligations.
[3] Australia Radiation Protection and Nuclear Safety Agency, *Indexed List Of Files Created During The Period 1 July – 31 December 2012*, <http://www.arpansa.gov.au/pubs/FileLists/JulytoDecember2012.pdf>, p. 2
[4] Existence identified in ASIO Report to Commonwealth Parliament 2002 -2003, ASIO, Report to Parliament 2003-2003, <https://www.asio.gov.au/img/files/ASIOsReportToParliament02-03.pdf>, p. 18 and Parliamentary Joint Committee on the Australian Security Intelligence Organisation, Committee activities (inquiries and reports), *A watching brief: the nature, scope and appropriateness of ASIO'S public reporting activities*, <http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcaad/asio/chapter03.pdf>, [3.41].
[5] *Response to Terms of Reference* of the Senate Legal and Constitutional Inquiry into ASIO Legislation Amendment (Terrorism) Bill 2002 <http://www.aph.gov.au/~/media/wopapub/senate/committee/legcon_ctte/completed_inquiries/2002_04/asio_2/submissions/sub241_doc.ashx> 2.
[6] Australian Federal Police and Australian Prudential Regulation Authority, *Memorandum of Understanding concerning co-operation and* information *sharing*, 2014, <http://www.afp.gov.au/~/media/afp/pdf/ips-foi-documents/ips/publication-list/afp%20mou%20concerning%20cooperation%20and%20information%20sharing%20with%20apra.pdf>
[7] AUSTRAC and Australian Prudential Regulation Authority, *Memorandum of Understanding on Co-operate and Exchange of Information,* 2007, <http://www.apra.gov.au/AboutAPRA/Documents/MoU-AusTRAC-Australian-Transactions-Report-and-Analysis-Centre.pdf>

Agency	MOUs with?	Public?	Content [2]
CrimTrac	AFP and all State and Territory Police Forces including separate inclusion of ACT Policing (not as a part of AFP (29 June 2006)	**Yes**[8]	• **Scope:** "detailed, current and accurate police information" (p. 1). The MoU *does not* specify the types of information but other CrimTrac documents lists the national databases it operates including the National Police Reference Services (criminal history of individuals)[9] • **Audit:** general audit of access and security (at 12.5-12.7), p. 7. • **Third party sharing:** the MOU *does not* specify when this can occur however. However the CrimTrac Australian Privacy Principle Policy[10] states that information is not routinely shared with other Commonwealth agencies except for CrimTrac board approved organisations, of which there are 5 ACC, Customs, ASIC, ICAC and the QLD Crime and Misconduct Commissions • **Transfer to offshore agencies:** can be disclosed to international agencies for a relevant reason[11]
ATO	With AFP (6 July 2010)	**Yes**[12]	• **Notification of data breach:** where confidentiality or security has been breached [Sch cl. 14] • **Transfer outside Australia:** with consent of party providing it only [Sch cl. 14]. • **Audit**: general audit provision – party can call for review of confidentiality and integrity of data with reasonable notice [Sch cl. 15]
VIC Police	None	N/A	N/A.
NSW Police	Joint Counter Terrorism Team MOU with ASIO, NSW Crime Commission and AFP (date unknown)	**No**. Existence identified in Martin Place report[13]	N/A, not public.

[8] CrimTrac, Partnership Memorandum of Understanding, 2006, <https://www.crimtrac.gov.au/sites/g/files/net526/f/Partnership%20Memorandum%20of%20Understanding.pdf>

[9] CrimTrac, *CrimTrac in Brief,* 1 July 2015, p. 7 <https://www.crimtrac.gov.au/sites/g/files/net526/f/CrimTrac%20in%20Brief.pdf>

[10] CrimTrac, *Australia Privacy Principle Policy*, p. 4 <https://www.crimtrac.gov.au/sites/g/files/net526/f/CrimTrac%20APP%20Privacy%20Statement%20-%20Full.pdf>

[11] see CrimTrac, *Australia Privacy Principle Policy*, p. 6 <https://www.crimtrac.gov.au/sites/g/files/net526/f/CrimTrac%20APP%20Privacy%20Statement%20-%20Full.pdf>

[12] <http://foi.iorder.com.au/downloadfile.aspx?filename=MYM55961-p2.pdf>

[13] Department of Prime Minister and Cabinet and Department of Premier and Cabinet NSW, *Martin Place Siege: Joint Commonwealth – New South Wales Review*, <https://www.dpmc.gov.au/sites/default/files/publications/170215_Martin_Place_Siege_Review_1.pdf> p 15.

TR 9. Controls – Proportionality factors in different Acts and Schemes

This appendix contains details of the proportionality factors in various Acts and schemes, as summarised in 'Requirements of Proportionality' in the Australia Report. It includes coverage in statutes and guidelines.

Intelligence Services Act and proportionality factors like 'necessity'

The test of 'reasonable necessity' is applicable to enabling legislation, for example, *Intelligence Services Act 2001* (ISA), which governs the Australian Secret Intelligence Service (ASIS), Australian Geospatial-Intelligence Organisation (AGO), and Australian Signals Directorate (ASD).

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[14] 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."[15]

The test of proportionality involves the following questions in descending order of particularity:

1. What is purpose of the statute?
2. What is the express purpose of the provisions in question?
3. Are the authorised actions/measures authorised "reasonably necessary and reasonably appropriate and adapted" for the expressed statutory purpose? In particular, are there significant potential costs and risks to privacy (and other relevant rights, freedoms and interests) from the proposed actions or measures]?[16]
4. If the risks are significant, do the authorising provisions provide for alternative yet similarly efficient and effective actions or measures that could fulfil the statutory purpose while minimising the costs and risks?

If the answer to the fourth question is negative, the authorising provision would fail the test of reasonable necessity and be open to constitutional challenge as disproportionate.

While ISA and some other agency-specific Acts contain provisions that incorporate, to a greater or lesser extent, the test of reasonable necessity in relation to access;[17] others include the test in their

[14] *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].

[15] *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.

[16] Is there adequate quantifiable evidence about effectiveness, costs and risks?

[17] This may explain why proportionality test is not explicitly a part of the *Rules to Protect Privacy of Australians* <https://www.asis.gov.au/Privacy-rules.html> made under s 15 *Intelligence Services Act 2001* that apply to the

Privacy Guidelines, though it has to be noted that the latter do not have the status of legislative instruments.[18]

Attorney-General's Guidelines for ASIO

The test of proportionality regarding the balance between the need for obtaining national security-related information and privacy considerations finds its fullest expression in in the *Attorney-General's Guidelines for ASIO*.[19] In accordance with the statutory functions set out in *Australian Security Intelligence Organisation Act 1979*, s 17,[20] paragraph 10.4 of the Guidelines provides that information[21] is to be obtained by ASIO in "a lawful, timely and efficient way", and "*any means used for obtaining information must be proportionate* to the gravity of the threat posed and the probability of its occurrence". [emphasis added]

The term "proportionate" is not defined per se; however, the following instructions on determining if, how, when and what means should be employed to obtain information, suggest that the drafters of Attorney-General's Guidelines for ASIO paid close attention to the criteria discussed in the High Court's decision in *Maloney v The Queen*:[22]

(b) 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;
(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.'

These ASIO Guidelines adopt and apply a test of proportionality by requiring undertaking of an analysis involving consideration of alternative measures before undertaking any action involving intrusion into individual privacy.

Australian Secret Intelligence Service, the Australian Geospatial-Intelligence Organisation, and the Australian Signals Directorate, and the guidelines developed by the Office of National Assessments. Each of these organisations has *Guidelines to Protect Privacy of Australians* adapted for the particular organisation, but closely adhering to the *Rules to Protect Privacy of Australians*

[18] For obligations in relation to instruments, see Office of Parliamentary Counsel, *Legislative Instruments Handbook*, December 2015 <http://www.opc.gov.au/about/docs/LI_Handbook.pdf>. Provisions on the status of these guidelines can be found in the relevant agency legislation.

[19] <http://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf>

[20] *Australian Security Intelligence Organisation Act 1979*, s 17(1) provides, inter alia that the 'functions of the Organisation are: (a) to obtain, correlate and evaluate intelligence relevant to security; (b) for purposes relevant to security, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes; (c) to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are relevant to their functions and responsibilities.'

[21] The term 'information' is defined in *Attorney-General's Guidelines for ASIO* §10.3 as including: '(a) the identity and relevant activities of individuals and groups of interest, including persons associated with the group of interest and of other persons likely to be knowingly concerned in furtherance of its plans or activities; and the finances, the geographic dimensions, and the past, present and prospective activities of the individuals or groups.'

[22] *Maloney v The Queen* [2013] HCA 28; 252 CLR 168 at [161], [182] and [183].

Telecommunications (Interception and Access) Act – Authorisations and Proportionality

The term 'proportionate' did not appear in *Telecommunications (Interception and Access) Act 1979* until the 2015 Data Retention Act, which amended s 180F.[23] Chapter 4 implied two forms of proportionality assessment for certain authorisations, with obligations to consider privacy or necessity. The amended s 180F explicitly introduced a 'proportionate' test, and added several factors in relation to the gravity of the conduct of interest.

TIAA Section 180F now requires authorised officers to consider privacy in making an authorisation for access to information, not being 'content or substance of a communication' (in other words, this applies to telecommunications data or 'metadata'). It is in the following terms:

> "Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate, having regard to the following matters:
>
> (aa) the gravity of any conduct in relation to which the authorisation is sought, including:
> (i) the seriousness of any offence in relation to which the authorisation is sought; and
> (ii) the seriousness of any pecuniary penalty in relation to which the authorisation is sought; and
> (iii) the seriousness of any protection of the public revenue in relation to which the authorisation is sought; and
> (a) the likely relevance and usefulness of the information or documents;
> (b) the reason why the disclosure or use concerned is proposed to be authorised."

By omitting reference to Division 3, s 180F excludes ASIO. It appears ASIO is not subject to this requirement for consideration of privacy. This therefore applies to law enforcement, including AFP.

By including Division 4A, it includes authorisation for disclosures to foreign law enforcement agencies through the AFP. In the case of disclosure to foreign LEAs, there is a second stage of assessment in s 180A(5) of Div 4A:

> "(5) The authorised officer [of the AFP] must not make the authorisation unless he or she is satisfied that:
>
> (a) the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and
> (b) the disclosure is appropriate in all the circumstances."

There is no mention there of any factor to take into account, like privacy, but there is an invitation to consider 'appropriateness' and 'all the circumstances', which are unspecified.

In neither case was the decision-maker's attention drawn to the range of potential proportionality factors, other than interference with privacy in s 180F; or the methods of weighing up any competing factors. The new s 180F now explicitly imports proportionality and sets out a number of factors in

[23] Version C2015C00537 of the *Telecommunications (Interception and Access) Act* includes the new wording with a proportionality test from 13 October 2015. Inserted by *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015 (No. 39, 2015) ('Data Retention Act') Schedule 1 Part 2, clauses 6J, 6K.

relation to the gravity of the conduct of interest. There still appears no articulation of any competing factors against which the proportionality of the authorisation might be weighed and assessed.

Need to consider factors like effectiveness: In s 180F, there is limited guidance as to whether there needs to be any evidence the disclosure would be effective for a specified purpose, although 'relevance and usefulness' may imply something of this.

In s 180F, The use of '*reasonably necessary'* in the specific authorisation would require that the authorisation be reasonably necessary (e.g. reveal information that would be of some demonstrable benefit or assistance in the aim of that particular authorisation, e.g. enforcing the criminal law and without which there would be a likelihood that such enforcement could not occur. 'Relevance and usefulness' sits as a factor to be considered as part of the 180F proportionality test. It suggests a two part process: Is the authorisation reasonably necessary for enforcing the criminal law? If so, would the disclosure of the telecommunications data be justifiable and proportionate when weighing it against the privacy considerations in 180F?

The term 'reasonably necessary' may thus imply a consideration of whether there is such evidence of effectiveness. Given the breadth of 'all the circumstances' it would be open to explore this question, but there is no requirement to do so, so the proportionality assessment model is somewhat limited and ambiguous. The meaning of 'reasonably necessary' as a statutory expression was considered in *Thomas v Mowbray* (2007);[24] concerns there with this term being too vague were dismissed by the majority, with Hayne and Kirby JJ dissenting. However, it was in the statutory context of the Criminal Code. (This term is also used in authorisations in ss 178 to 180.)

Scope for further considerations to be identified: Under s 183 TIAA, there is scope for the Communications Access Coordinator to create additional requirements for these metadata authorisations, in consultation with the Information Commissioner (formerly the Privacy Commissioner.) This offers a mechanism for more robust articulation of factors to be taken into account, and methods for assessing their 'weight' for proportionality assessment, to be added by legislative instrument.[25]

Telecommunications (Interception and Access) Act – Stored Communications Warrants and Proportionality Factors

Section 116 TIAA includes two provisions requiring consideration of proportionality factors.

It covers warrants for stored communications including the content or substance, so it may be substantially less relevant for a 'Big Data' approach, since analysis of content is more difficult than analysis of 'metadata', and obtaining warrants requires greater effort to articulate what the purpose is.

In s116(2), the authority issuing a warrant for stored communications, other than for Mutual Assistance, must have regard to the following factors:

> "(a) how much the *privacy* of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and
> (b) the *gravity of the conduct* constituting the serious contravention; and
> (c) how much the information referred to in subparagraph (1)(d)(i) would be *likely to assist* in connection with the investigation; and

[24] (2007) 233 CLR 307*;* 237 ALR 194; [2007] HCA 33. See Ben Saul, 'Between the Crime and the War Falls the Terror: Comment on Thomas *v Mowbray'*, Working Paper 2, Sydney Centre for International Law, Faculty of Law, University of Sydney, 2009 <http://sydney.edu.au/law/scil/documents/2009/SCILWP2_Final.pdf>
[25] For example, Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2015.

(d) to what extent *methods* of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or *are available* to, the agency; and
(e) how much the use of *such methods would be likely to assist* in connection with the investigation by the agency of the serious contravention; and
(f) how much the use of *such methods would be likely to prejudice* the investigation by the agency of the serious contravention, whether because of delay or for any other reason." [emphasis added]

There is a mention of the extent of interference with privacy in 116(2)(a), while (b) and (c) consider the target and benefits.

S 116(2)(d)-(f) are interesting in that they address the proportionality issue of whether there are alternative less intrusive methods available, and their potential to assist or prejudice the investigation. This is a useful specification of a requirement to consider potentially effective alternatives which is absent in other such assessment or consideration requirements. Subsection (e) could imply an inquiry into whether there is evidence that the method chosen is likely to be effective in practice, although this is not stated.

For Mutual Assistance applications, s 116(2A) has a truncated set of factors for the issuing authority to have regard to:

"(a) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and
(b) the gravity of the conduct constituting the serious foreign contravention; and
(c) how much the information referred to in subparagraph (1)(d)(ii) would be likely to assist in connection with the investigation, to the extent that this is possible to determine from information obtained from the foreign country to which the application relates."

This does not include consideration of alternative methods.

Telecommunications (Interception and Access) Act – Telecommunications Service Warrants and Proportionality Factors

Section 46 TIAA includes a provision requiring a Judge or nominate AAT member to give consideration of proportionality factors in deciding the grant of a Telecommunications Service Warrant application. S 46A mirrors its provisions for Named Person Warrants. The matters to which they have to give regard are:

"S 46(2)(a) how much the *privacy of any person or persons* would be likely to be interfered with by intercepting under a warrant communications made to or from the service referred to in subsection (1);[26] and
(b) the *gravity of the conduct* constituting the offence or offences being investigated; and
(c) how much the information referred to in paragraph (1)(d) would be *likely to assist* in connection with the investigation by the agency of the offence or offences; and
(d) to what extent *methods* of investigating the offence or offences that do not involve so intercepting communications have been used by, or are available to, the agency; and
(e) how much the use of such *methods would be likely to assist* in connection with the investigation by the agency of the offence or offences; and
(f) how much the use of such *methods would be likely to prejudice* the investigation by the agency of the offence or offences, whether because of delay or for any other reason; and

[26] S 46A has a minor variation, still directed at how much 'the privacy of persons' would be interfered with.

(fa) in relation to an application by an interception agency of Victoria--any *submissions made by the Victorian PIM* under section 44A to the Judge or nominated AAT member; and
(g) in relation to an application by an interception agency of Queensland--any *submissions made by the Queensland PIM* under section 45 to the Judge or nominated AAT member." [emphasis added]

As with s116 above, there is consideration of both interference with privacy and the viability of alternative less intrusive methods.

Telecommunications (Interception and Access) Act – Ministerial Determinations and Proportionality Factors

Section 189(4) of the TIAA includes a provision requiring a Minister proposing to make a determination in relation to an international standard about the requirements of interception agencies in relation to the interception of telecommunications passing over a network to give consideration of proportionality factors. The matters to which they have to give regard are:

(a) the interests of law enforcement and national security; and
(b) the objects of the *Telecommunications Act 1997* ; and
(c) the privacy of the users of telecommunications systems.

The Minister can of course take into account other relevant matters.

This Section 189(4) is a different model of identifying factors, perhaps in part due to the broader scope of such a determination compared to the more operationally specific subjects of warrants and authorisations, and to the part that determinations play in the wider national security and law enforcement framework.

It refers not to "interference with privacy" as in the sections above, but to "privacy" and to "the users of telecommunications systems" – a broader class than affected by specific warrants and authorisations above, yet in some ways potentially narrower. In addition, the objects of the *Telecommunications Act* are covered, which may imply concern with commercial and technical matters not referred to in the earlier requirements. This is not surprising, as the determinations may have significant impacts on industry regarding compliance with a particular international standard.

There is no requirement to consider for instance whether there are alternative viable methods than those which may be covered by the standard, submissions by a PIM, the gravity of the matters to which the determination may apply, or the degree to which the determination may or may not assist investigations or other operations.

Public Interest Monitor role and proportionality submissions

A further interesting addition, included to provide scope for Public Interest Monitors (PIMs)[27] from relevant states to make submissions, is found in ss 46(2)(fa) and (g). These PIMs are intended to partially address the suspension of natural justice that arises from parties being excluded from decisions or legal proceedings concerning them and, albeit without instructions from the subject, may seek to raise other factors relevant to the decision. They appear to only exist in Victoria and Queensland.[28]

Observation: The role of PIM is potentially a valuable and independent addition to the measures which may improve the fairness and effectiveness of assessments of the proportionality of a particular data or information practice which of operational necessity has limited or no provision for the subject to offer submissions.

For consistency and to support better decision-making in necessarily unfair circumstances, such a role could be created in relation to other data and information decisions, not only those under s 46, and not only for citizens subject to interception requests from Queensland and Victoria, as at present.

The existing PIM role is restricted to one form of warrant. It is not immediately apparent why this role should not apply to all such decisions, including Authorisations for telecommunications data, although the circumstances of the authorisation process would not involve a warrant hearing as in s 46(2) TIAA.

Public Interest Advocate under a Journalist Information Warrant

Also of potential interest are the new PIAs (Public Interest Advocates) under the journalist information warrant regime for telecommunications data authorisations.[29] This is a further instance of entities with a role to make submissions in circumstances where the affected parties are not in a position to do so on their own behalf. This similar to the role of PIMs, although on a narrower basis.

The Minister must declare one or more PIAs who may make submissions to the Minister or issuing authority for warrants under ss 180L or 180T respectively, including whether to issue such a warrant and any conditions on it.

While the regulations may prescribe matters relating to the performance of the PIA role, there is no other guidance in the Act as to the scope of the issue to be covered, nor of the basis on which the advocate can or must proceed, in terms of evidence about the circumstances of the proposed warrant or the interests of the persons affected.

---

[27] See *Public Interest Monitor Act 2011* (Vic) <http://www.ibac.vic.gov.au/docs/default-source/legislation/public-interest-monitor-act-2011.pdf> The role of the PIM in Victoria is to appear at a hearing to 'test the content and sufficiency of the information relied upon and the circumstances of the application' by asking questions and making submissions: s 14. See also *Police Powers and Responsibilities Act* 2000 (Qld), Chapter 21 Part 5, ss 740-745 <http://www.austlii.edu.au/au/legis/qld/consol_act/ppara2000365/>

[28] The role of the PIM at the state level has been around since 2011 (Vic) and 2012 (Qld). The Vic PIM was introduced into the TIA Act in 2012.

[29] See *Telecommunications (Interception and Access) Act 1979* s 180X Public Interest Advocates <https://www.legislation.gov.au/Details/C2016C00102/Html/Text#_Toc442179624> or <http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/s180x.html>

TR 10. Models for cost allocation for data storage for access purposes

This appendix compares features of some of the models for cost allocation and reimbursement in relation to telecommunications interception and data retention activities.

Telecommunications Act – 'do your best' – prevention of offences – s 313(1)

1. In s 313(1) and (2) of the *Telecommunications Act*, measures taken, in effect at their discretion, by a carrier or carriage service provider in pursuit of the obligation to "do your best" to prevent the infrastructure from being used in the commission of offences are compensated at the rate of 0%.

The reimbursement scheme in s 314 does not apply to these s 313(1) and (2) "preventive" provisions, only to the "reasonably necessary help" provisions in ss 313(3) and (4) for law enforcement, pecuniary penalty, revenue protection and national security purposes.

This may be because, again unlike ss 313(3) and (4), these "preventive" provisions do not authorise any entity to make requests a provider to take particular action, nor themselves impose an obligation of compliance with such requests, nor offer any guidance as to the scope or necessity of any action taken for this preventive purpose. In the absence of any entity authorised under s 313(1) or (2) to make a request, and any duty under these preventive provisions to comply with any request from any entity, it would be difficult to identify the entity responsible, and the appropriate amount, for any reimbursement.

Telecommunications Act – 'reasonably necessary help' - preservation - law enforcement and national security – s 313(3)

2. In s 313(3) and (4) of *Telecommunications Act*, measures required to be taken to give "reasonably necessary help" to officers and authorities for the criminal law enforcement, pecuniary penalty, revenue protection and national security purposes are compensated at 100%. Section 314(2) mandates a mechanism for arrangements where the entity must comply with the requirement to give help "on the basis that the person neither profits from, nor bears the costs of, giving that help," and the provider can take advantage of binding arbitration in the event of a dispute over the quantum or other calculations.

The question of whether reasonable infrastructure or development costs are to be factored in, where the systems and infrastructure required to comply with the request for assistance are in addition to what is required for normal operations, is not addressed explicitly.[30] One interpretation would be that if giving 'reasonable assistance' requires further capability or functionality not otherwise necessary and in place for ordinary operations, to avoid financial loss in providing the assistance a contribution to necessary extra infrastructure costs might be appropriate. Alternatively, it may be that this provision was meant only to apply on a case by case basis to marginal extra costs where enforcement requires assistance on systems which are already functioning and capable, and giving the assistance requires no significant extra infrastructure or capability development effort.

If this second interpretation is the case, it is unclear whether, if extra capability were needed in order to give the assistance (for instance if it were similar to the new data retention scheme technical

[30] *Telecommunications Act* S 314 provisions are apparently considered to be designed for a case by case basis in which law enforcement requires assistance on systems already functioning, although this is not set out in the provision; and there appears to be no direct equivalent of TIA Act in relation to split allocation between s 207 'interception capability' and s 208 'delivery capability', discussed below.

demands), s 314 would cover it; and if not covered, whether this would affect a 'reasonableness' assessment.

This question may also arise over time for already functioning systems as affected data volumes, bandwidth, storage and other parameters increase with the continual rapid increase in online traffic.

The Note in s 206 TIAA[31] states that s 314 TA covers the allocation of costs in relation to carriers complying with authorisations under Division 3 or 4 of Part 4-1 *Telecommunications (Interception and Access) Act 1979,* which refer to 'voluntary disclosure' to ASIO or enforcement agencies or disclosure under authorisations made on their behalf. This implies s 314 TA may apply to costs in respect of telecommunications data ('metadata') as dealt with in those authorisations, rather than the interception matters covered in s 206 TIAA, although the language of s 313(7) TA appears to imply preservation and retention of whole messages, not just metadata.

Telecommunications (Interception and Access) Act – Interception – delivery *cf.* capability

3. Under the model for carriers, the 'interception capability'[32] is paid for by the carrier[33] and the 'delivery capability'[34] imposed on the carrier is paid by the interception agency.[35] S 209 TIAA sets out the method for calculating and managing this contribution, and the basis for the terms of provision settled by agreement or determination by ACMA. It is based on principles set out in 209(2) for cost effectiveness, and the allocation of costs for 'delivery' and 'interception' capabilities between carrier and agencies respectively. In the event of a dispute, under s 209(4) the terms must provide for ACMA to arbitrate, and if it does ACMA can independently seek information about cheaper options (s 210), and require an audit (s 211), before determining the appropriate level of costs.

It may be worth investigating the degree to which the interception/delivery distinction, apparently initially derived from older telephone infrastructure and interception methods, remains relevant for 'Big Data' models.

4. There has been reference to another different earlier model under the TIAA, where the assumption was that providers would pay for the investment in fixed infrastructure to make a measure possible, and the requestors would pay on a case by case basis the extra operational costs of complying with particular requests. This may be a variation of the s 209 model (though note s 208 above explicitly included 'capital' costs of a delivery capability as part of those to be paid by the agency). Where the fixed costs were small, infrequent and each interception request created a substantial manual configuration and later remediation cost, as in the past with traditional telephone interception, this may have put most of the overall costs in this agency basket.

Telecommunications (Interception and Access) Act data retention – retention

5. Query whether the reverse situation to the traditional telephone model applies for the new telecommunications data retention scheme. To what extent would most of the costs of a scheme of comprehensive telecommunications data retention be 'capability' costs, the fixed costs of continually expanding volumes of storage and extraction bandwidth, and the routine operational costs of in effect a 'retain everything' model (which does not involve regular repeated requests to retain); rather than 'delivery' costs, the limited one-off operational costs of occasional, possibly automated,

[31] See <http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/s206.html> or <https://www.comlaw.gov.au/Details/C2015C00537/Html/Text#_Toc433199317>.
[32] Parts 5-3 to 5-4 *TIAA Act*, ss 189–202, referring to obligations imposed by ss 190 and 191.
[33] Part 5-6 Div 2 of *TIAA Act*, s 207.
[34] Part 5-5 of *TIAA Act*, ss 203–205.
[35] Part 5-6 Div 3 of of *TIAA Act,* ss 208–211.

access requests? Given the unabated growth of online traffic,[36] these may be relatively limited in comparison to the cost of establishing, operating, protecting and regularly upgrading the necessary systems over time.[37]

6. In negotiations for the data retention scheme, the up-front capital costs to the industry were estimated by PricewaterhouseCoopers (PwC) to be between $188.8 million and $319.1 million. The Government committed $128.4 million to a funding pool to directly contribute to industry's upfront costs associated with meeting the new data retention obligations. This funding was 50 percent of the mid-point of the PwC estimates.

The Government is thus contributing a fixed amount for the 'startup' period of about 18 months,[38] half of the estimates of cost for this component. Variation of startup actual costs from the estimates presumably falls to the providers. The actual costs may be affected by how questions are resolved about the technical implications of the language of the Data Retention Act for the data items to be collected, and thus the volume and other technical parameters of compliance.[39]

As is the case with other obligations in the TIA Act, providers bear the cost of complying with regulatory requirements. However, providers are able to recover the costs of complying with particular requests on a no-profit no-loss basis.

Estimates of such 'one-off' compliance costs do not appear to be readily available, nor do those for incremental further capital costs arising from the normal data volume increase over time.[40]

There appears to be no statutory scheme for independent arbitration of disputes similar to that in s 314 TA, which enables ACMA to appoint an arbitrator if the parties cannot agree on one, or s 209 TIA Act, which says ACMA arbitrates disputes if requested by the agency.

---

[36] Estimates of traffic growth vary but suggest a regular doubling in relatively short periods. 'Mobile data use is expected to grow at an annual rate of 38 % [78% for 4G], from an estimated monthly average of 22.2 PB in 2013 to 81.1 PB in 2017.' ACMA, 'Australia benefits from going mobile,' April 2014 <http://www.acma.gov.au/Industry/Spectrum/Spectrum-projects/Mobile-broadband/australia-benefits-from-going-mobile>; ABS recently reported a 50% annual increase to December 2015 in fixed line data traffic (98% of all internet downloads): Australian Bureau of Statistics, 'Volume of data downloaded,' *8153.0 - Internet Activity, Australia, December 2015*, <http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/8153.0Main%20Features4December%202015?opendocument&tabname=Summary&prodno=8153.0&issue=December%202015&num=&view=>.

[37] Rob Nicholls, 'For What it's Worth: Cost Benefit Analysis of the use of Interception and Access in Australia' (2009) *The Fourth Workshop on the Social Implications of National Security* 63 <http://www.researchgate.net/publication/237011552_Chapter_8_For_What_its_Worth_Cost_Benefit_Analysis_of_the_use_of_Interception_and_Access_in_Australia>, and the debates noted in Cat Barker and Jaan Murphy, 'Telecommunications data retention,' *Budget Review 2015-16*, Parliamentary Library, May 2015 <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201516/Telco>.

[38] Internet Society Australian Chapter, 'Internet Society calls on Government to guarantee to fund data retention short fall', media release, 12 May 2015; Communications Alliance, 'Data retention—focus needed on efficient compliance arrangements', media release, 12 May 2015, cited in Cat Barker and Jaan Murphy, 'Telecommunications data retention,' *Budget Review 2015-16*, Parliamentary Library, May 2015 <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201516/Telco>.

[39] David Ramli, 'Federal budget 2015: Telecommunications firms seek clarity over data retention funding', *Australian Financial Review* (online), 12 May 2015.

[40] [Source for typical rate of growth of data volume]

A Data Retention Industry Grants Program for the funding pool was established in early 2016.[41] According to the Program Guidelines, its objectives are to be met by 'making a contribution to the typical up-front costs of compliance' with data retention obligations, at [16], so 'that the telecommunication industry has the necessary technical capability to comply with data retention obligations', at [17]. This appears to focus on initial start up costs rather than on-going operation or future upgrade costs. The Customer Information Guide offers more detail on matters that can be claimed, and while not explicit about the question of ongoing costs, it includes capital and commissioning costs of new equipment but not depreciation (which might be expected to cover funding replacement of capital over time).[42]

[41] See <http://www.business.gov.au/grants-and-assistance/communications/DRIGP/Pages/default.aspx>. Program Guidelines address the funding model <http://www.business.gov.au/grants-and-assistance/communications/DRIGP/Documents/DRIGP-ProgrammeGuidelines.PDF>

[42] Data Retention Industry Grants Program, *Customer Information Guide*, DIIS/AGD, January 2016, [8.1], [8.2] <http://www.business.gov.au/grants-and-assistance/communications/DRIGP/Documents/DRIGP-CustomerInformationGuide.pdf>

TR 11. Examples of purpose or types of offence covered

Different statutory provisions refer to different types of offences or threats as a basis for their coverage. This table sets out some examples.

Examples of statutory purpose

Purpose or category	Coverage
'security' *ASIO Act* s 4 [covers terrorism in 'politically motivated violence'?]	(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from: (i) espionage; (ii) sabotage; (iii) politically motivated violence; (iv) promotion of communal violence; (v) attacks on Australia's defence system; or (vi) acts of foreign interference; whether directed from, or committed within, Australia or not; and (aa) the protection of Australia's territorial and border integrity from serious threats; and (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).
'Serious and organised crime' is an offence: *ACCA* s4	(a) that involves 2 or more offenders and substantial planning and organisation; and (b) that involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques; and (c) that is committed, or is of a kind that is ordinarily committed, in conjunction with other offences of a like kind; and (d) that is a serious offence, an offence against Subdivision B or C of Division 471, or D or F of Division 474, of the Criminal Code, an offence of a kind prescribed by the regulations or an offence that involves any of the following: (i) theft; (ii) fraud; (iii) tax evasion; (iv) money laundering; (v) currency violations; (vi) illegal drug dealings; (vii) illegal gambling; (viii) obtaining financial benefit by vice engaged in by others; (ix) extortion; (x) violence; (xi) bribery or corruption of, or by, an officer of the Commonwealth, an officer of a State or an officer of a Territory; (xii) perverting the course of justice; (xiii) bankruptcy and company violations; (xiv) harbouring of criminals; (xv) forging of passports;

	(xvi) firearms; (xvii) armament dealings; (xviii) illegal importation or exportation of fauna into or out of Australia; (xix) cybercrime; (xx) matters of the same general nature as one or more of the matters listed above; and (da) that is: (i) punishable by imprisonment for a period of 3 years or more; or (ii) a serious offence [excludes two categories]

TR 12. Survey instrument – Australia

[See *Methodology Report* for discussion of these instruments.

Big Data Technology and National Security

A. Interviews with law enforcement and intelligence officials – AUSTRALIA

Introductory Information

Thank you for agreeing to an interview. Before we start I would like to tell you a bit more about the study and what we hope to achieve from the interviews. As you would be aware from the Participant Information Statement, the main aim of this project is to examine the policies, regulatory approaches, processes and strategies used by Australia to balance the management and exploitation of Big Data for law enforcement and national security purposes, while safeguarding confidentiality and security of sensitive personal information, as well as the accuracy of data sets. This research project is not concerned with information that may be private, classified, or in relation to specific criminal offences. You are requested not to disclose such information during the interview. We would like to also remind you that anything we talk about will remain confidential to the project and if we use anything you say in this interview in our publications, we will make sure that you will not be identifiable.

1. Please describe the responsibilities of your current position and the organisation and team or unit in which you are employed.
   [NB: if you have any concerns about being identified, we will not include specifics about your position/responsibilities that could be used to identify you.]

2. Could you tell us (a) what your education and training background is, and (b) about your work experience prior to the current position?

General

3. When does digital/computer technology hinder you in your work and when is it particularly helpful?

Data Sources, Access and Sharing

I am going to ask some questions around data sources, access and sharing. In these questions, I use the term "data" broadly to capture records, information and intelligence.

4. What types of data do you (or your unit) use in your work?

5. What types of data do you (or your unit) generate in your work? How is this captured?

6. Does your unit share data with other agencies, and if so, which ones?

7. What are you major concerns in relation to data access from other agencies or sharing data with other agencies?

8. Do these problems affect your (or your staff's) morale or sense of professionalism?

9. How can these problems be overcome?

Data Analytics

10. What do you (or your unit) mainly use these data for?

11. How do you (or your unit) normally use data for [law enforcement investigation/crime prevention/security intelligence etc] as described above?

12. 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?

13. What are the most serious issues/problems that may prevent you (or your unit) making greater use of data analytics?

14. Do you think your agencies' access to data and analytical tools is better or worse that other agencies, your foreign counterparts and the private sector?

Big Data

15. This research project is concerned with the use of Big Data. The term 'Big Data' has been used by people in a number of ways. How would you define Big Data?

16. As far as you know, what is Big Data capable of doing that "ordinary data" can't?

17. To what extent are you (or your unit) making use of Big Data tools in your work?

18. What are the most serious issues/problems that may prevent you (or your unit) from making more use of Big Data?

19. What do you see are the risks of using Big Data for law enforcement or security intelligence?

Regulation

20. As you know, there are laws, regulations or procedures governing the use of data by law enforcement or security agencies. In your view are these laws, regulations, procedures, guidelines etc appropriate? Are they effective?

21. How do you think the law should strike a balance between privacy/individual rights and public concerns such as national security, terrorism and serious crimes?

Thank you very much for taking the time to be interviewed. Your input is much appreciated.

Big Data Technology and National Security

B. Interviews with technologists/designers – AUSTRALIA

Introductory Information

Thank you for agreeing to an interview. Before we start I would like to tell you a bit more about the study and what we hope to achieve from the interviews. As you would be aware from the Participant Information Statement, the main aim of this project is to examine the policies, regulatory approaches, processes and strategies used by Australia to balance the management and exploitation of Big Data for law enforcement and national security purposes, while safeguarding confidentiality and security of sensitive personal information, as well as the accuracy of data sets. This research project is not concerned with information that may be private, classified, or in relation to specific criminal offences. You are requested not to disclose such information during the interview. We would like to also remind you that anything we talk about will remain confidential to the project and if we use anything you say in this interview in our publications, we will make sure that you will not be identifiable.

Current Position

1. Please describe the responsibilities of your current position and the organisation in which you are employed.
   [NB: if you have any concerns about being identified, we will not include specifics about your position/responsibilities that could be used to identify you.]

2. Could you tell us (a) what your education and training background is and (b) your work experience prior to the current position?

Big Data – Capabilities

3. This project is concerned with the use of Big Data. The term 'Big Data' has been used by people in a number of ways. How would you define Big Data? What does it mean in the context of your work? How does it relate to other terms you might use?

4. Do you use Big Data in your work/systems? What role do Big Data techniques have in your work/systems? What is your role in relation to these?

5. What types of data analysis do you or does your organisation do? What are the outputs? How reliable/accurate are these outputs?

6. Who are the users of your product/system? Who can access data within the system? What mechanisms are used to ensure the security and privacy of data within the system?

7. In your organisation/system, what are the main challenges you face with respect to Big Data or data analysis?

8. What do you see are the opportunities or possibilities that [data analysis/data science if they used these terms] or Big Data can open up for law enforcement and security intelligence?

9. What data analytic and data visualization tools or software do you use when dealing with large data sets? What do these tools provide you with? Are they useful?

10. What do you know about Big Data that everyone in the field will know in five years? How would you improve the way your organisation designs systems or builds tools for working with national security and law enforcement data?

11. What issues do you think are likely to come up in the future for Big Data or data analytics? What advice would you give policy-makers on the use of Big Data or data analytics/data science for law enforcement or national security purposes?

Risks

12. What are the risks of using data analytics to support law enforcement and enhance national security relating to your work or product? Who is exposed to these risks? How should these risks be managed?

13. How important is it that outputs of your system are reliable and accurate? How tolerant of invalid, unreliable, corrupted or non-relevant data can your system afford to be?

Design Issues

14. Who sets the design parameters for your product/system?

15. To what extent can some of the risks of data analytics be mitigated through the design of analytical tools? For each of the following issues, please indicate whether you take it into account in your design (Yes/No), and if so, how:

Issues	Yes/No	How is it taken into account?
Protection of privacy		
Communications confidentiality		
Personal information security		
Data integrity, [ie that information held is accurate, current, relevant and not misleading]		
Regulatory compliance		
Testing and evaluation		
Comprehensibility to decision-makers		
Avoiding unintended consequences		
Avoiding discrimination		
Potential for de-identified data to be re-identified		
Agency inter-operability		
Cost		

Thank you very much for taking the time to be interviewed. Your input is much appreciated.

Big Data Technology and National Security

C. Interviews with policymakers, citizen groups – AUSTRALIA

Introductory Information

Thank you for agreeing to an interview. Before we start I would like to tell you a bit more about the study and what we hope to achieve from the interviews. As you would be aware from the Participant Information Statement, the main aim of this project is to examine the policies, regulatory approaches, processes and strategies used by Australia to balance the management and exploitation of Big Data for law enforcement and national security purposes, while safeguarding confidentiality and security of sensitive personal information, as well as the accuracy of data sets. This research project is not concerned with information that may be private, classified, or in relation to specific criminal offences. You are requested not to disclose such information during the interview. We would like to also remind you that anything we talk about will remain confidential to the project and if we use anything you say in this interview in our publications, we will make sure that you will not be identifiable.

Current Position

1. Please describe the responsibilities of your current position and the organisation in which you are employed.
   [NB: if you have any concerns about being identified, we will not include specifics about your position/responsibilities that could be used to identify you.]

2. Could you tell us (a) what your education and training background is and (b) your work experience prior to the current position?

Big Data – Capabilities

3. This project is concerned with the use of Big Data. The term 'Big Data' has been used by people in a number of ways. How would you define Big Data?

4. As far as you know, what is Big Data capable of doing that ordinary data can't?

5. To what extent is Big Data currently being used for law enforcement and security intelligence in Australia?

6. Do you think Australian agencies access to data and analytical tools is better or worse that their foreign counterparts and the private sector?

7. In your view should this use by Australian agencies be expanded? If so, in what way should this be expanded and what could be achieved? If not, why not, and what would be the implications?

8. What do you see are the opportunities or possibilities that Big Data can open up for law enforcement and security intelligence? How can these possibilities be delivered? What are the barriers and how could they be overcome?

Big Data – Regulation

9. What are the challenges and risks of Big Data technology to support law enforcement and enhance national security? Who is exposed to these risks? How should these challenges and risks be managed?

10. How is the use of Big Data currently being regulated? What laws, policy, codes of practice, standards, etc. are in place in this jurisdiction? How effective are they? What are their shortcomings?

11. [If appropriate] Do you have a sense of the history of these regulations? If yes, why are they the way they are?

12. What accountability, transparency or oversight mechanisms are in place? Are they appropriate and effective?

13. What protections, if any, should remain in place in circumstances where an individual consents to the use or sharing of their data?

14. What future strategies are required for Big Data?

Scenario:

15. Now I would like to ask you a series of questions in relation to a hypothetical scenario:

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?

What difference would it make if this was not just a kidnapping but there's suspicion of paedophilia? What difference would it make if there was suspicion that the kidnapping was linked to terrorism, with an intent to blow Lucy up in a public place?

16. To what extent should considerations such as privacy give way in the face of serious, imminent threats such as child kidnapping, child sexual abuse or terrorism?

17. Assuming that Big Data had been proven effective in other instances, are there ways that Big Data techniques could be used appropriately? What kind of laws, regulations, accountability mechanisms would need to be in place?

18. To what extent should there be transparency about the nature of data collected or the algorithms employed in analysis, both within an agency or more broadly?

19. How do you think your / your organisation's views about the design and regulation of Big Data technology align with the views of other stakeholders? Do you have any thoughts on how any conflict might be resolved?

20. To what extent are your views shaped by internal or personal experience as opposed to external sources such as blogs, watch groups and media?

Thank you very much for taking the time to be interviewed. Your input is much appreciated.

TR 13. Australian Criminal Intelligence Forum (ACIF) members

The Australian Criminal Intelligence Forum[43] is comprised of:

- Australian and New Zealand Policing Advisory Agency (ANZPAA)
- Australian Capital Territory Police
- Australian Crime Commission (ACC)
- Australian Federal Police (AFP)
- Attorney General's Department (AGD)
- Australian Security and Investments Commission (ASIC)
- Australian Taxation Office (ATO)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- CrimTrac
- Department of Border Protection (DIBP)
- New South Wales Police Northern Territory Police
- Queensland Police
- South Australia Police
- Tasmania Police
- Victoria Police
- Western Australia Police

[43] See <http://www.anzpaa.org.au/our-work/collaborations/australian-criminal-intelligence-forum-acif>