Australian Government

Independent National Security Legislation Monitor

TRUST BUT VERIFY

A report concerning the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and related matters

Dr James Renwick CSC SC

3RD INSLM 2020 9TH REPORT

THE INDEPENDENT NATIONAL SECURITY LEGISLATION MONITOR

The *Independent National Security Legislation Monitor Act 2010* (Cth) provides for the appointment of the Independent National Security Legislation Monitor (INSLM). The INSLM independently reviews the operation, effectiveness and implications of national security and counter-terrorism laws; and considers whether the laws contain appropriate protections for individual rights, remain proportionate to terrorism or national security threats, and remain necessary.

In conducting the review, the INSLM has access to all relevant material, regardless of national security classification; can compel answers to questions; and holds public and private hearings. INSLM reports are provided to the Prime Minister, the Attorney-General or the Parliamentary Joint Committee on Intelligence and Security and are tabled promptly in Parliament.

The INSLM does not deal with complaints but welcomes submissions on the reviews. The INSLM is a part-time role and is supported by a small permanent staff located in Canberra. Further information and contact details can be found at www.inslm.gov.au. There have been 3 INSLMs since the role began in 2010: Bret Walker SC, the Hon Roger Gyles AO QC and Dr James Renwick CSC SC (pictured).

Independent National Security Legislation Monitor (INSLM) Report

Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and related matters.

978-1-921091-07-0 (Print)
978-1-921091-08-7 (Online)

Copyright notice

Enquiries regarding the licence and any use of this work are welcome at:

Office of the Independent National Security Legislation Monitor

3–5 National Circuit Barton ACT 2600

www.inslm.gov.au

Australian Government

Independent National Security Legislation Monitor

30 June 2020

The Hon Christian Porter MP
Attorney-General
Parliament House
Canberra ACT 2600

Dear Attorney-General,

REVIEW OF THE *TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018*

Under subsection 6(1D) of the *Independent National Security Legislation Monitor Act 2010* (Cth) (INSLM Act), I am required to review the operation, effectiveness and implications of amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act).

On 26 March 2019, under section 7A of the INSLM Act and paragraph 29(1)(b)(ii) of the *Intelligence Services Act 2001* (Cth), Mr Andrew Hastie MP, Chair of the Parliamentary Joint Committee on Intelligence and Security (the Committee), referred, on behalf of the Committee, the TOLA Act for my review and consideration. Mr Hastie noted that the Committee was of the view that this report would satisfy the obligation under subsection 6(1D) of the INSLM Act. I agree and I have conducted both reviews simultaneously and produced a single report.

I now enclose the report, together with a brief classified annexure. I confirm that the unclassified report omits any material referred to in s 29(3) of the INSLM Act and is therefore suitable to be tabled in the Parliament. Given the unprecedented reporting by me to both you and the Committee, I leave the specifics of tabling for the Committee to discuss with you. I only request that it is done in accordance with the requirements in the INSLM Act, and the expectations of the many interested persons who participated in the inquiry, that is, as soon as possible but in any event within 15 sitting days.

This is my final report as INSLM, as my term finishes today. In view of s 6(1)(d) of the INSLM Act, I confirm that I have seen no evidence as INSLM that Australia's counter-terrorism or national security legislation is being used for matters unrelated to terrorism and national security.

I am sure my successor will continue the strong working relationship between our Offices. It has been an honour to serve as the Third INSLM and I thank you for your support in that endeavour.

Yours sincerely

James Renwick CSC SC
Independent National Security Legislation Monitor
cc: Mr Andrew Hastie MP, Chair of the Parliamentary Joint Committee on Intelligence and Security

Australian Government

Independent National Security Legislation Monitor

30 June 2020

Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

Dear Mr Hastie,

REVIEW OF THE *TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018*

On 26 March 2019, on behalf of the Parliamentary Joint Committee on Intelligence and Security (the Committee), you referred, under section 7A of the *Independent National Security Legislation Monitor Act 2010* (Cth) (INSLM Act) and paragraph 29(1)(b)(ii) of the *Intelligence Services Act 2001* (Cth), for my consideration and reporting the question of whether the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act) contains appropriate safeguards for protecting the rights of individuals, remains proportionate to the threat of national security and remains necessary.

I note that in your letter dated 26 March 2019, the Committee was of the view that this report would also satisfy the INSLM's obligation under subsection 6(1D) of the INSLM Act to review the TOLA Act. I agree and I have conducted both reviews simultaneously and produced a single report.

I now enclose the report, together with a brief classified annexure. I confirm that the unclassified report omits any material referred to in s 29(3) of the INSLM Act and is therefore suitable to be tabled in the Parliament. Given the unprecedented reporting by me to both the Committee and the Attorney-General, I leave the specifics of tabling for the Committee to discuss with the Attorney-General. I only request that it is done in accordance with the requirements in the INSLM Act, and the expectations of the many interested persons who participated in the inquiry, that is, as soon as possible but in any event within 15 sitting days.

I thank you for the recent opportunity to brief the Committee on my recommendations – I trust it was helpful. I also thank you for the referral, which was the first by the Committee to my Office. Although my own term finishes today, I am sure the complementary relationship between the Committee and my Office will continue. I wish the Committee well in its important work.

Yours sincerely

James Renwick CSC SC
Independent National Security Legislation Monitor
cc: The Hon Christian Porter MP, Attorney-General

Contents

The Independent National Security Legislation Monitor 2
List of abbreviations 10
Technical glossary 12
The theme of this work: 'trust but verify' 23

1. EXECUTIVE SUMMARY 24
Overview 24
The review 26
TOLA's 5 schedules 27
Key principles and findings 30
The threat landscape 30
Proportionality 31
The internet, privacy and trust: key conclusions 32
Safeguards updated for new technology 35
Schedule 1 36
Schedule 2 39
Schedules 3 and 4 39
Schedule 5 40
Reporting and record-keeping and own motion review powers 41
Structure of this report 41
List of recommendations 42

2. CONDUCT OF THE REVIEW 49
Legislative history 49
Intelligence reviews 51
Submissions 52
Hearings 53
International engagement 54
A Question of Trust and IPCO 54
Those assisting me 57

3. CONTEXT: THE THREAT LANDSCAPE 58
The current threat level 59
Conclusion 66

4. CONTEXT: ANALYSIS OF TOLA 67
Pre-TOLA powers 67
Schedule 1 69
Schedule 2 79
Schedule 3 86
Schedule 4 91
Schedule 5 94

5. CONTEXT: TECHNOLOGY – DEFINITIONS AND CHALLENGES 98
A changing communications environment 99
A complex web of communications infrastructure and service providers 103
Encryption 106
Different types of data 110
Challenges for lawful access to communications 117
Exceptional access, back doors, front doors and more 120

6. CONTEXT: PRIVACY – RIGHTS AND SAFEGUARDS 123
Legitimate expectations of privacy 123
Existing privacy laws and protections in Australia 124
Reasonable expectations of privacy in the digital age: the United States 131
Reasonable expectations of privacy in the European context 136
What are reasonable expectations of privacy in Australia in the digital era? 138
Conclusion 142

7. CONTEXT: AUSTRALIA'S INTERNATIONAL OBLIGATIONS 143
International obligation to counter cybercrime 143
International obligation in the area of human rights 149
Consistency of TOLA with engaged human rights obligations 153

8. CONTEXT: THE CLOUD ACT, IPCO AND AAT 170
The IPO Bill and the AAT 176
9. FINDINGS: GENERAL PRINCIPLES 181
Schedule 1 181
Use of other TOLA powers 182
Conclusions 184
10. FINDINGS: TARS, TANs and TCNs 188
Absence of independent authorisation of TANs and TCNs 188
Findings on TANs 191
Findings on TCNs 197
Findings on TARs 203
Integrity agencies should be included in Part 15 of the Telecommunications Act 204
Key definitions 207
11. FINDINGS: AN AUSTRALIAN IPCO AND A FURTHER ROLE FOR THE AAT 215
The function of issuing TANs and TCNs 215
Courts, tribunals and persona designata 216
An Australian Investigatory Powers Commissioner 220
Technical advisers 221
An Investigatory Powers Division of the AAT 223
Figure 1: Phase 1 of the operation of the Investigatory Powers Division 225
Figure 2: New process for Technical Assistance Notices (TANs) 226
Figure 3: New process for Technical Capability Notices TCNs) 227
12. FINDINGS: SCHEDULES 2, 3, 4 & 5 228
Conclusions 228
Schedule 2: Computer access warrants 239
Schedules 3 and 4: Assistance orders 243
Schedule 5: New ASIO powers 249

13. APPENDICES **258**

Appendix A: Referral letters 258

Appendix B: List of submissions 261

Appendix C: Public hearing program 263

Appendix D: Section 317E listed acts or things 265

Appendix E: Analysis of submissions 267

List of abbreviations

Term	Notes
AAT	Administrative Appeals Tribunal
ABF	Australian Border Force
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
ACLEI	Australian Commission for Law Enforcement Integrity
ACMA	Australian Communications and Media Authority
ACSC	Australian Cyber Security Centre
ADA	Australian Designated Authority
ADJR Act	*Administrative Decisions (Judicial Review) Act 1977* (Cth)
AFP	Australian Federal Police
AGD	Attorney-General's Department
AHRC	Australian Human Rights Commission
ALRC	Australian Law Reform Commission
APPs	Australian Privacy Principles
ASD	Australian Signals Directorate
ASIS	Australian Secret Intelligence Service
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
Budapest Convention	*Convention on Cybercrime* of the Council of Europe
CAW	Computer Access Warrant
CDPP	Commonwealth Director of Public Prosecutions
CFREU	Charter of Fundamental Rights of the European Union
CLOUD Act	*Clarifying Lawful Overseas Use of Data Act* (US)
Constitution	*Commonwealth of Australia Constitution Act* (Cth) (Australian Constitution)

Crimes Act	*Crimes Act 1914* (Cth)
Criminal Code	*Criminal Code Act 1995* (Cth)
CSLI	Cell-site Location Information
Customs Act	*Customs Act 1901* (Cth)
GDPR	General Data Protection Regulation
IBAC	Independent Broad-Based Anti-Corruption Commission
ICCCA	International Crime Cooperation Central Authority
ICCPR	*International Covenant on Civil and Political Rights*
IGIS	Inspector-General of Intelligence and Security
INSLM	Independent National Security Legislation Monitor
INSLM Act	*Independent National Security Legislation Monitor Act 2010* (Cth)
Investigatory Powers Act or IP Act	*Investigatory Powers Act 2016* (UK)
IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioner's Office
IPO	International Production Order
IPO Bill	Telecommunications Legislation Amendment (International Production Orders) Bill 2020
MACM Act	*Mutual Assistance in Criminal Matters Act 1987* (Cth)
OAIC	Office of the Australian Information Commissioner
Ombudsman	Commonwealth Ombudsman
PJCHR	Parliamentary Joint Committee on Human Rights
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Privacy Act	*Privacy Act 1988* (Cth)
QDW	Questioning Detention Warrants
QW	Questioning Warrants
SD	Security Division (of the Administrative Appeals Tribunal)

SD Act	*Surveillance Devices Act 2004* (Cth)
Siracusa Principles	*Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*
TAN	Technical Assistance Notice
TAR	Technical Assistance Request
TCN	Technical Capability Notice
Telecommunications Act	*Telecommunications Act 1997* (Cth)
TIA Act	*Telecommunications (Interception and Access) Act 1979* (Cth)
TOLA	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)
TOLA Bill	Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018
UNGA	United Nations General Assembly

Technical glossary

Term	Definition	Notes
Access control	Security technique that regulates access to data based on factors such as who someone/something is, where they are and what they want to do	
Access network	Type of telecommunications network that connects users to their immediate service provider	
Application Service Providers (ASP)	Organisation providing computer-based services to users over a network. In this context the services are things that help the user do something useful	Examples include Twitter providing social media feed and Xero providing accounting services

Apps	Stand-alone software programs that perform a specific function or allow a user to interact with a specific online service	Examples on a mobile phone include Calculator, Maps, Facebook Messenger and Google Mail
Asymmetric encryption	A form of **encryption** where different keys are used to encrypt and decrypt data	This can improve security, as the key used by the receiver of the message is kept private
Authentication	Security measure to confirm that a user is who they say they are and that they are authorised to access the system or data	Authentication methods often require the user to provide **credentials** to prove their identity
Back door	Undocumented feature in a system that allows normal security measures to be bypassed	
Backup	Copy of computer data taken and stored elsewhere so that it can be used to restore the system if data is lost	
Circuit-switched	Mode of communication where a dedicated network connection is established between the parties for the duration	Normal mode used for 'traditional' or **PSTN** voice calls
Client	Clients interact with services provided by **servers**	Examples include laptops, smartphones and desktop computers
Cloud computing	On-demand availability and use of computing facilities owned and operated by another party	

Communications /Carriage Service Providers (C/CSP)	Organisation providing communications services over a network	Detailed definition in *Telecommunications Act 1997* (Cth)
Computer Network Exploitation (CNE)	Technique through which computer networks are used to infiltrate target computers' networks to extract and gather data in contrast to Computer Network Defence (CND) and Computer Network Attack (CNA)	
Content of data	Any element of the communication, or any data attached to or logically associated with the communication, that reveals anything that might reasonably be considered the meaning (if any) of the communication but excludes any meaning arising from the fact of the communication	Definition taken from *Investigatory Powers Act 2016* (UK)
Credentials	Information used to confirm (**authenticate**) the identity of a user	Examples include name, password, token and biometrics
Cryptanalysis	The use of mathematical techniques to seek to decipher coded messages without having access to the decryption key	This often tries to find and exploit weaknesses in the encryption methods being used
Data	Information stored, processed or communicated in digital form	
Data at rest	Data stored on digital media and not actively moving from device to device	Examples are data physically stored on a mobile phone or

		on a laptop hard drive
Data centre	Purpose-built facility for computer **servers** that provides power, network connectivity and stable conditions to control heat and humidity	Data centres may be physically in Australia or overseas, without the user being aware
Data in transit	Data actively moving from one location to another such as across the internet or through a private network	
Data retention	Obligations for a service provider to retain specified metadata for all users for a specified period	Obligations specified in Part 5-1A of *Telecommunications (Interception and Access) Act 1979* (Cth)
Designated Communications Provider (DCP)	Covers the breadth of communications providers across the communications network, including: carriage service providers, 'telcos', those who supply or install such services and those who develop software used in connection with such services	Defined in s 317C of the *Telecommunications Act 1997* (Cth)
Decryption	The process of decoding information that has been **encrypted** so that it may be understood	
Digital footprint	Trail of data that a user creates when using digital services	This footprint may be stored by different organisations in different places, and often users are unaware of the full

		extent of their digital footprint
Domain Name Server (DNS)	Servers that are contacted by a client to look up names of websites in order to work out actually where to route the traffic	These can be thought of as the internet's equivalent of a phonebook
Encryption	The process of encoding information so that it may only be understood by the authorised recipient	
End User Device	The physical device used by the person who ultimately enjoys the benefits of the digital services	Examples are a mobile phone, smart watch and laptop
End to end (E2E) encryption	Data that remains encrypted from when it leaves the sender until it is received by the receiver – that is, it is not decrypted and re-encrypted at any intermediate point in the chain of communications	Often this also is taken to mean that only the receiver of the data has the key to decrypt it
Exceptional access	Functionality that allows a third party to access specific contents of communication, even if normally encrypted or otherwise protected from unauthorised access	
Fixed access network	An **access network** that makes use of physical cables and electric signals	For example, the NBN network connections to premises in Australia
Front door	An explicit, documented feature to allow an authorised user to bypass security controls	Examples may be: - System administrator account that has access to all users'

		files stored on a system - Lawful interception interface built into many pieces of network equipment as standard
Global System for Mobile communications (GSM)	The standards developed for the first digital mobile telephone networks	
Hacking	Interacting or using a computing system in a manner for which it was not designed, often in order to exploit deficiencies to reveal sensitive information or obtain unauthorised access	
Internet	Global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols	
Internet of Things (IOT)	Interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data	
Internet Protocol (IP)	A set of rules that control how data is sent over the internet or other network	IP is now ubiquitous – almost every network that transmits data today uses this protocol

Lawful Interception (LI)	Synonymous with **telecommunications interception**	This term is commonly used in overseas jurisdictions
Machine to machine (M2M)	Communication between computing devices without any human control or intervention	An example would be automated updates sent from electricity smart meters to the power company
Malware	Abbreviation of 'malicious software' – a program or application that is operational on a computing system and that performs malicious activity	
Metadata	Data about the fact and nature of a communication, but excluding the **content**	
Mobile Network Operator (MNO)	Organisation that builds and operates a mobile phone network and uses this to provide mobile telecommunications services to its customers	Typically owns and operates the mobile phone towers and a network that connects them together. In Australia, Telstra, Optus and Vodafone are the main MNOs
Network	The connections between a group of computers or other electronic devices that allow them to communicate and share data	
Over The Top (OTT)	Refers to the provision of application services by a provider independent of the telecommunications and network infrastructure being used	Examples are Skype audio and video calls and WhatsApp messaging

Packet switched	Mode of communication where data is split up into 'packets' and each packet is sent separately. In contrast to a **circuit-switched** communication, there is no single continuous network connection and path	This means that potentially each packet in a single communication could be sent by a different route, even traversing different countries
Plain Old Telephone Service (POTS)	Term used to describe voice-grade telephone services provided over copper cables	These are the traditional home phone line used only for voice calls from a standard telephone
Public Key Encryption	A form of asymmetric encryption where the key used by senders to encrypt the messages to a person is generally made available to anyone – but only that person knows the key to decrypt them	
Public Switched Telephone Networks (PSTN)	Term used to describe voice grade telephone services provided over copper networks and mobile phone networks	Broader than **POTS**, as it also covers mobile phone calls, but only refers to traditional 'circuit-switched' calls, where you dial a number and have a dedicated connection for the duration of the call
Rack space	Physical space within a data centre where computer systems can be installed and connected	

Radio Access Network (RAN)	An **access network** that makes use of radio/wireless connections	For example, a mobile phone network, or a Wi-Fi hotspot
Ransomware	Type of **malware** that prevents legitimate access to information or computing resources until a ransom is paid to the attacker	
Secure Sockets Layer (SSL)	Secure protocol used for sending information securely over the internet to or from a website	
Server	A computer system operated by a service provider that serves a dedicated function or purpose – for example, a website or an image-sharing service	Servers normally interact with **clients** that present services to end users
Short Message Service (SMS)	Text messaging service to allow short messages to be sent from one mobile phone to another, typically limited to 10 characters or fewer	SMS is provided by the **MNO** and has been today largely overtaken by **OTT** messaging services
Source code	A human-readable text listing of commands or instruction to be executed by a computer. Software developers write source code to create software. The source code is compiled or translated into a machine-readable form to allow it to be executed	Commercial companies that sell software typically distribute compiled programs and keep their source code secret, as this is often considered to be valuable intellectual property and hence commercially sensitive. However, some software is 'open-source' – the

		source code is available to anyone
Spyware	A form of **malware** that covertly monitors activity and content on a user's computer or device – for example, 'key loggers', which capture and forward on keystrokes; 'adware', which identifies users' interests; and software that covertly captures data from the inbuilt microphones or cameras on a device	Spyware is used by criminals but can also be used by agencies as part of **computer network exploitation** operations
Symmetric encryption	A form of **encryption** where the same keys are used by the sender to encrypt data and by the receiver to decrypt data	This is often considered less secure than **asymmetric encryption**, since the sender and receiver need to find a way to agree on the key being used; however it is generally easier and cheaper to implement
Telecommunications Interception (TI)	Providing access to, or a copy of, the contents of a communication to a party other than the sender and recipient of the communication	Normally refers to the action of doing so under the specific authorities set out in Chapter 2 of the *Telecommunications (Interception and Access) Act 1979* (Cth)
Transport Layer Security (TLS)	Protocol that provides **authentication**, privacy and data integrity between 2	Today TLS has largely superseded **SSL**, although the 2

	communicating computer applications	terms are often used interchangeably
Ubiquitous encryption	A term used to refer to the widespread adoption of encryption within computer and communications systems by default	Users often no longer need to proactively enable encryption or even understand it – it is built-in and used without them being aware
Virtual Mobile Network Operator (VMNO)	Service provider that provides mobile phone service running on infrastructure owned by third parties	
Voice Over Internet Protocol (VoIP)	Technology that allows real-time voice communications to be carried across data (**IP**) networks	This is key to allowing **OTT** providers such as Skype to provide audio calls that replace traditional **C/CSP** call services
World Wide Web	The overall ecosystem of interactions between users and websites across the **internet**	

The theme of this work: 'trust but verify'

Public consent to intrusive laws depends on people trusting the authorities, both to keep them safe and not to spy needlessly on them … Trust in powerful institutions depends not only on those institutions behaving themselves (though that is an essential prerequisite), but on there being mechanisms to verify that they have done so. Such mechanisms are particularly challenging to achieve in the national security field, where potential conflicts between state power and civil liberties are acute, suspicion rife and yet information tightly rationed … Respected independent regulators continue to play a vital and distinguished role. But in an age where trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency.

David Anderson QC, Independent Reviewer of Terrorism Legislation,
A Question of Trust: Report of the Investigatory Powers Review 2015[1]

[1] UK Government, London, 2015, [13.3]–[13.4]. David Anderson QC is now the Rt Hon Lord Anderson of Ipswich KBE QC.

1. EXECUTIVE SUMMARY

Overview

1.1. This, my ninth report as Independent National Security Legislation Monitor (INSLM), is a review of the Telecommunications *and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA) and related matters.

1.2. The essential effects of TOLA are as follows:

a. Schedule 1 gives police and intelligence agencies new powers to agree or require significant industry assistance from communications providers.

b. Schedules 2, 3 and 4 update existing powers and, in some cases, extended them to new agencies.

c. Schedule 5 gives the Australian Security Intelligence Organisation (ASIO) significant new powers to seek and receive both voluntary and compulsory assistance.

1.3. Schedules 1 and 5 have proven controversial; Schedules 2, 3 and 4 less so.

1.4. My task is to consider the operation, effectiveness and implications of TOLA and whether it is necessary, is proportionate to the threats it seeks to meet and treats human rights properly. Where powers have not yet been used, my task involves prediction.

1.5. *As to necessity,* I have concluded that, with 2 exceptions, TOLA is or is likely to be necessary. The first exception is that Schedule 1 must be amended to extend Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) to integrity agencies, including any future Commonwealth Integrity Commission. The other exception is in Schedule 5: one aspect of the voluntary assistance power and corresponding civil immunity in s 21A(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) is unnecessary and should be amended.

1.6. *As to proportionality and proper rights protection*, TOLA will be compliant if, but only if, the central recommendations in this report are implemented. Most importantly, Schedule 1 should be amended to:

a. remove the power from agency heads to issue TANs and from the Attorney-General to approve TCNs[2]

b. vest those issuing and approval powers in the Administrative Appeals Tribunal (AAT) in a way which will preserve and protect both classified and commercial-in-confidence material and allow independent rulings on technical questions such as 'systemic weakness' (definitions which, among others, should be amended)

c. create a new statutory office – the Investigatory Powers Commissioner (IPC). The IPC should be a retired judge who will be appointed to the AAT and have access to technical advice. The IPC will assist in approving the issue of TANs and TCNs (as above) while monitoring the operation of Schedule 1 and issuing guidelines. (This can be done with minimal expense.)

1.7. I have recommended that there be no change to the way that TARs are currently agreed between an interception agency head and a Designated Communications Provider (DCP) and the way the agreement then enables the relevant agency head to issue a TAR (although I have recommended the use of a prescribed form). This is in contrast with my recommendations on TANs and TCNs. It was almost unanimously agreed in non-government submissions that these notices should be authorised by either an independent tribunal member or a judicial officer and subject to meaningful judicial review once issued. Indeed, a number of stakeholders indicated that their main concern with the provisions in Schedule 1 was that no independent person is involved in the decision to issue a notice. The Australian Human Rights Commission raised human rights concerns on this point. Government submitters contended that there are already a number of conditions that apply to the issuing of compulsory notices, and these operate effectively and with sufficient oversight. My recommendations for TANs and TCNs build on these existing mechanisms to guarantee consideration of human rights, privacy and technical implications by the issuing authority.

1.8. A related key point is the distinction between TANs and TCNs, which provide technical 'access'; and warrants (and other similar instruments), which provide 'content'. TANs and TCNs do not provide the authority to obtain content from a DCP without an underlying warrant, and the Government has submitted that these notices are merely a mechanism to ensure that whatever data is obtained under a lawful warrant is accessible and comprehensible to the interception agency. I have not accepted the Government's argument as to the distinction in this regard.

[2] With the concurrence of the Minister for Communications.

1.9. I consider that there is a greater need for safeguards in the virtual world than in the physical world, for both reasons of trust and the wide and unknown impact of technology. At a public hearing of this review, Professor Peter Leonard, from the Law Council of Australia, stated in relation to trust:

> *In the digital world, digital trust of citizens is affected by activities that may not relate to their specific digital activities. So we always need to consider, as we look at the digital world, the effect on broader digital trust of citizens, and potentially undermining that trust. Now, often a degree of undermining that trust will be justified in national security or law enforcement, but I do think that you can't take the digital world as an exact analogue of the physical world, because of that different nature of the digital system*.[3]

1.10. This chapter provides an overview. It should be read with the whole of the report.

The review

1.11. TOLA was enacted in December 2018 after targeted government consultation and limited time for parliamentary scrutiny. Many communications providers regarded this as unsatisfactory.

1.12. By s 7A of the *Independent National Security Legislation Monitor Act 2010* (Cth) (INSLM Act), the Parliamentary Joint Committee on Intelligence and Security (PJCIS) may refer to me any matter which it 'becomes aware of in the course of performing its functions … and … considers should be referred'.

1.13. In March 2019, having issued 2 reports on TOLA, the PJCIS requested that I consider the necessity and proportionality of that legislation in view of the threats it seeks to meet, and its effects on human rights, and to report back by June 2020.[4]

1.14. The review has held extensive consultations in Australia, the United Kingdom (UK) and the United States (US); held public and private hearings; and received many submissions, which are listed in Appendix B and summarised in Appendix E of this report.

1.15. This report complies not only with the request from the PJCIS but also with the requirements contained in s 6(1D) of the INSLM Act[5] to review TOLA. The report's

[3] Law Council of Australia, Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5-6

[4] A copy of the referral letter and related press release is at Appendix A.

[5] (1D) The Independent National Security Legislation Monitor must:

aim is both to assist the PJCIS in its pending review of TOLA and also, as the INLSM Act's object states, to 'assist Ministers'. I have had access to the as yet unpublished Comprehensive Review of the Legal Framework of the National Intelligence Community and taken it into account.

1.16. This report is suitable to be, and should be, made public save for a small but necessarily classified annexure, which I am only able to provide to the PJCIS and ministers.

1.17. If, as I recommend, TOLA and related Acts are included in my 'own motion' powers of review in the INSLM Act, my successors will be able to update this review as necessary and as they see fit.

1.18. TOLA is a lengthy and complex Act which itself amends many laws, extends beyond national security and counter-terrorism concerns to crime generally, and operates in an environment of ever-changing technology. Also, as extensive engagement with this review has shown, it could affect many important and legitimate businesses both in Australia and overseas.

1.19. Because of these matters, and the need for extensive consultation, it has been the most complex and difficult report I have produced. I am therefore grateful for the indispensable support I have received from those providing briefings, submissions and feedback; and, of course, those assisting me.

TOLA's 5 schedules

1.20. TOLA is an Act with 5 schedules which runs to over 200 printed pages. Apart from the *Telecommunications Act 1997* (Cth) itself, TOLA amends, sometimes extensively, complex and frequently amended Acts such as the ASIO Act, the *Crimes Act 1914* (Cth), the *Customs Act 1901* (Cth), and the *Surveillance Devices Act 2004* (Cth) (SD Act). I analyse TOLA in detail later. Here I note its essence.

1.21. *Schedule 1* is the main focus of this report. It contains amendments that enable police and intelligence agencies (but not integrity agencies) to either request or compel by notice a DCP – a term which deliberately covers a broad range of persons and companies in the communications supply chain – to provide technical assistance, thereby overcoming the problem of 'going dark', and making intelligible digital content and data.

(a) review the operation, effectiveness and implications of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018; and
(b) do so as soon as practicable after the 18-month period beginning on the day that Act receives the Royal Assent.

1.22. The assistance which may be required from or agreed with a DCP is not only access to content and metadata but also technological assistance such as removing electronic protection, providing technical information, formatting information and facilitating access to devices and other *listed acts or things*.[6] Schedule 1 provides for:

a. a TAR, which is a request agreed by an agency and a DCP

b. a TAN, which is issued by an agency head

c. a TCN, which is issued by the Attorney-General with the concurrence of the Minister for Communications.

1.23. TARs (now being used), TANs and TCNs (not yet used but very likely to be used) cannot be specifically disclosed publicly or to DCP customers. They provide civil and criminal immunity according to their terms. There are a number of technical concepts or limits in Schedule 1, including whether a TAN or TCN is *reasonable and proportionate*, *technically feasible* or would result in a *systemic weakness or systemic vulnerability*.

1.24. The 3 most significant complaints about Schedule 1, which I largely accept as valid, concern:

a. the absence of independent authorisation for the notices

b. the inadequacy of various definitions of technical matters

c. the absence of independent technical assessment of proposed notices.

1.25. *Schedule 2* establishes powers which enable federal, State and Territory law enforcement agencies to obtain covert computer access warrants when investigating certain federal offences. It amends a number of Acts to reform the existing computer access warrants available to ASIO, introduces computer access warrants for law enforcement agencies, and establishes an avenue for foreign governments and international courts and tribunals to request assistance in accessing data via a computer access warrant.[7] Warrants are issued by the Attorney-General (for ASIO computer access warrants), or by an eligible judge or a nominated AAT member (for

[6] Parliamentary Library, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Bills Digest No 49 of 2018–19, 3 December 2018) 6.

[7] Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access Act) 2018* (2019).

SD Act computer warrants requested by a law enforcement officer or on behalf of foreign governments).[8]

1.26. *Schedule 3* amends the existing search warrant framework under the Crimes Act to expand the ability of criminal law enforcement agencies to collect evidence from electronic devices.[9] Other amendments include authorising the adding, copying, deleting or altering of other data if that is necessary to give effect to a warrant, while making it clear a search warrant cannot authorise police to do anything likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use of a computer or cause other material loss or damage.[10] Warrants are issued by judicial officers or AAT members, acting as *persona designata* rather than as representatives of the courts or tribunals of which they are members. Further, Schedule 3 expands the scope of the Australian Federal Police's (AFP's) power to obtain an assistance order to compel an individual to provide certain information or assistance to police; and amends the criminal penalties for failing to comply with an assistance order.

1.27. *Schedule 4* amends the search warrant framework under the Customs Act to 'enhance the ability of the Australian Border Force (ABF) to collect evidence from electronic devices under warrant in person or remotely'.[11] TOLA expands the types of actions that a warrant may authorise under the Customs Act. It authorises ABF officers to search premises for evidential material in relation to a specified offence, including using electronic equipment to access 'relevant data' that is held in a computer or data storage device found during a search, to determine whether the data is evidential material of a kind specified in the warrant.[12] Similar new provisions apply as under the Crimes Act (amended by Schedule 3), including with regard to adding and copying data and remote access, material interference and increased penalties for noncompliance.[13] Approvals are the same as for Schedule 3. Further, Schedule 4 makes amendments to the ABF's power to obtain an assistance order, including by amending the criminal penalties for failing to comply with an assistance order.

1.28. *Schedule 5* provides 2 new powers or capacities to ASIO.

---

[8] *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), s 25A; *Surveillance Devices Act 2004* (Cth) (SD Act) s 27A(7).

[9] See additional powers in Crimes Act, s 3F(2A)–(2B).

[10] Ibid s 3F(2B)–(2C).

[11] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth), 5 [19].

[12] TOLA, Schedule 4, Item 4A.

[13] TOLA, Schedule 4, Items 2, 4A, 5, 6, 7, 18.

1.29. First, the Director-General of Security may issue a voluntary assistance request to a (legal or natural) person to engage in 'conduct' to assist ASIO in the performance of its functions (ASIO Act, s 21A(1)), and a person may volunteer to provide more limited assistance in relation to documents (ASIO Act, s 21A(5)). Where a person provides assistance requested by ASIO or volunteers assistance, immunity from civil liability ordinarily attaches to that conduct.

1.30. Secondly, at the request to the Director-General of Security the Attorney-General may issue a compulsory assistance order compelling a person to assist in accessing data held on a computer or data storage device (ASIO Act, s 34AAA).

1.31. My main concern with Schedule 5 is that s 21A provides a limited and certain capacity for assistance to be volunteered under sub-s (5) but a wider and uncertain power for ASIO to request conduct under sub-s (1). Given ASIO's other powers to obtain information and assistance, I consider it is only necessary for ASIO to have power under s 21A(1) to request what equally could be volunteered under s 21A(5).

Key principles and findings

1.32. The stated purpose of TOLA is to amend a range of Commonwealth legislation to allow law enforcement and national security and intelligence agencies to 'better work in the increasingly complex digital environment' and 'introduce measures to better deal with the challenges posed by ubiquitous encryption'.[14] Some of the many issues raised in these notions are discussed in more detail in Chapter 5, dealing with technology, Chapter 6, dealing with privacy, and in the detailed and helpful submissions I have received (see Appendix B for a list of submissions). Here I set out the key findings I have made and principles I have acted on.

The threat landscape

1.33. In assessing the necessity of the provisions of TOLA, I must consider the current threat landscape.

1.34. In previous reports, I have noted that the level of threat of a terrorist act occurring in Australia remains at 'probable', and the evidence I have considered for the present review indicates that this position remains unchanged.

1.35. This review has caused me to consider broader security and other threats to the political, commercial and societal interests of the nation. There are real threats of foreign interference in facets of our lives that we may take for granted. The extent of the use of the internet by hostile foreign states and their agents to engage in

[14] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access Bill) 2018 (TOLA Bill), 2 [1].

espionage and foreign interference is still not fully appreciated, partly because of the covert and disguised means these actors use in their online activity.

1.36. Because the World Wide Web and the related Internet of Things (together, the internet) have a large and growing role in all aspects of life around the globe, but particularly in a technologically advanced democracy such as Australia, the threats TOLA seeks to meet extend beyond the counter-terrorism and national security activities that I normally consider as INSLM, to the behaviour of criminal and other bad actors more generally.

1.37. There is an ever-present threat of criminals engaging in online activities to perpetrate general but serious crimes, such as child sexual exploitation and sophisticated frauds. The breadth of these threats is facilitated by means which are increasingly complex and difficult to detect. As the Minister for Home Affairs recently said, 'almost every crime type and national security concern has an online element'.[15]

1.38. To counter what is called 'going dark' by reason of encryption, agencies must adapt their techniques, and laws must be updated. I am satisfied from the evidence I have received from intelligence, police and integrity agencies that encryption of content and, to a lesser extent, metadata has made their essential tasks significantly more difficult, and in some instances impossible. I accept the necessity of a legislative response to 'going dark'.

Proportionality

Context

1.39. Necessity is one aspect of my review. The other is proportionality. Any legislative response to threats must be adapted, and proportionate, to the risk of them occurring. International human rights law and the INSLM Act both require consideration of proportionality and the related question of human rights protections.

1.40. What makes this review unusually challenging is not only the complexity of the law but also the technological context, which includes events that can be viewed, metaphorically, as the shifting tectonic plates of our times. As Professor Sir David Omand[16] has recently written, in terms I gratefully adopt:

> *We are living through the beginning of a revolution in human affairs enabled by*

[15] Explanatory Memorandum, Telecommunications Legislation Amendment (International Production Orders) Bill 2020.

[16] University College, London. Formerly head of Government Communications Headquarters (GCHQ) and the United Kingdom's Security and Intelligence Coordinator.

the digitization of information and the means of communication through the Internet, the World Wide Web, and mobile devices (with the Internet of Things rapidly growing). We are now dependent on this technology for economic and social progress, for international economic development, and for national security and public safety. Trust has to be built both in the open Internet as a safe place to innovate, to do business, to shop, and to interact socially, and in the ability of the authorities to be able to uphold the law in cyberspace. That trust cannot be taken for granted. The Internet, and the World Wide Web that it carries, were not originally designed with security in mind, and many seek to exploit this weakness for their own antisocial, criminal, or aggressive ends. A global coincidence over the last fifteen years has shaped the rapid development of digital intelligence and heightened ethical concerns: the post–Cold War growth in demand for information about individuals to manage the threats from terrorists (especially after 9/11), international criminals, and other individuals of concern has coincided with the ability of the Internet and Web-based technologies, developed for commercial purposes, to supply detailed data about individuals in ways never before possible. Demand for and supply of such data have been interacting dynamically, and the process continues.[17]

The internet, privacy and trust: key conclusions

1.41. Although many matters which arose in this review are open for debate, in my opinion at least the following matters are clearly established.

1.42. As the internet became indispensable to the legitimate operations of, and interactions between, governments, corporations and other organisations, and individuals, it was also used by criminals and other bad actors for their illicit purposes.

1.43. The internet was not designed with security in mind. To remedy this inherent weakness, widespread data content encryption and, to an increasing extent, metadata encryption has been used. Encryption seeks to maintain general confidence in the security of the internet. It is not only appropriate but also essential that it seeks to provide effective security and protection for:

a. internet communications and transactions

b. government, commercial and private data

c. the maintenance of legitimate personal rights to privacy, and its near relative, anonymity.

[17] Sir David Omand and Mark Phythian, *Principled Spying: The Ethics of Secret Intelligence*, (Georgetown University Press, 2018) Ch 5.

1.44. *Privacy* can be an elusive concept and each legal jurisdiction has its own approach. Thus:

a. international law recognises a right to privacy, while giving some leeway to nation states in how they respond

b. European Union (EU) law enables the right to be forgotten

c. the 4th Amendment to the *Constitution of the United States* is of significance to Australia in obtaining mutual assistance for the purposes of intelligence and countering crime

d. although Australia has enacted a *Privacy Act 1988* (Cth), neither the Australian Constitution nor the common law of Australia recognises a specific right to privacy. Instead, the common law mainly protects privacy through the requirement that, absent consent, there must be a legal basis for interference with personal property.

1.45. In particular, Australia has inherited from English law and still maintains:

a. *a common law rule* that holders of public office can only seize or access private property as authorised by law

b. *the historically entrenched practice* that this is typically done by warrant, issued by persons independent of the agency which seeks to exercise the warrant.[18]

1.46. This rule:

a. applies to accessing and copying data content and metadata on personal devices such as computers and mobile phones, just as much as it does to searches of people or premises

b. has rightly been said to recognise the 'link between protection of personal property and protection of freedom of thought and political expression'[19]

c. as it states a fundamental right, is protected by the principle of legality, so that a statute which seeks to overcome it will only be effective in doing so by clear statement of intent or by necessary implication.

---

[18] *Smethurst v Commissioner of Police* [2020] HCA 14 [23] (Kiefel CJ, Bell and Keane JJ): 'The power to search has always been regarded as an exceptional power, to be exercised only under certain justifying conditions**.** One essential condition, found in statutes authorising the issue of warrants for search and seizure, both Commonwealth and State and Territory, is that the object of the search be specified by reference to a particular offence.'

[19] Ibid [155] (Gageler J, citing Lord Camden in *Entick v Carrington* (1765) 19 St Tr 1029).

1.47. With rare exceptions – most notably, some ASIO warrants issued by the Attorney-General[20] – independent serving judges and tribunal members issue these warrants to executive agencies and police in Australia. They act in a personal capacity, '*persona designata*'. This practice is rightly seen as a vital democratic safeguard in Australia – so much so that departing from it requires justification.

1.48. Pre-TOLA, coercive statutory powers for access to intelligible data content and metadata were heavily relied on by intelligence, police and integrity agencies. (I should note that I do not generally see it as my role in this review to revisit the justification for such powers, many of which have operated for some time.) As encryption steadily deprived them of this access, the effectiveness of those powers diminished. A key justification put forward for TOLA is that it will reverse this trend.

1.49. A fundamental principle guiding me in this review is that, just as we do not accept lawlessness in the physical world, we should not accept lawlessness in the virtual world. Therefore, in principle, the surveillance powers that apply in the physical world should also apply to the virtual world unless there are good reasons that they should not.

1.50. In this report, I apply this fundamental principle together with a *companion principle* – that of 'trust but verify', which I have adopted from *A Question of Trust* as the theme of this work. The companion principle is that in the sceptical world in which Australian democracy operates:

> *trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency.*[21]

1.51. In this report I reject the notion that there is a binary choice that must be made between the effectiveness of agencies' surveillance powers in the digital age on the one hand and the security of the internet on the other. Rather, I conclude that what is necessary is a law which allows agencies to meet technological challenges, such as those caused by encryption, but in a proportionate way and with proper rights protection. Essentially this can be done by updating traditional safeguards to meet those same technological challenges – notably, those who are trusted to authorise intrusive search and surveillance powers must be able to understand the technological context in which those powers operate, and their consequences. If, but

[20] Leaving aside warrants issued as part of the judicial function.

[21] David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (UK Government, London, 2015) [246].

only if, the key recommendations I set out in this report in this regard are adopted, TOLA will be such a law.

Safeguards updated for new technology

1.52. My UK counterpart, Jonathan Hall QC, in his most recent report[22] has rightly written of terrorism legislation as follows:

> *[2.30] Modern technology calls into question legislation written in an earlier era, and terrorism legislation is no exception. Interrogating a phone can reveal more data than searching a house; information is electronic, and accessed, rather than physical, and seized; contact is encrypted and routed around the world; worldwide publication is open to every person with a smartphone.*

1.53. The same holds true for TOLA, whose scope and purpose extends well beyond countering terrorism. Take the familiar example of the personal mobile phone/device, which:

a. is an essential aspect of modern life: its use is not really optional for anyone seeking to fully participate in Australian life

b. amalgamates the functions that were once performed by several devices: telephone, address book, calendar, emails, internet browser, camera, video camera, calculator, thermometer, pedometer, heart monitor, dictaphone and more

c. is a 'data rich' environment – it contains not only an unprecedented amount of data content that its user may be broadly aware of, but also highly revealing metadata about the user's movements, communications and thoughts that the user may be unaware of and, in some cases, is not capable of being aware of

d. is the paradigm example of monetisation of our personal data, usually with technical consent but rarely, if ever, with our informed consent

e. when its contents are revealed, can be devastating for the user's privacy. As the US Supreme Court recently said of movement metadata of one man due to his phone's tracking capacity, it was 'revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations"'.

[22] Jonathan Hall QC, Independent Reviewer of Terrorism Legislation, *The Terrorism Acts In 2018: Report of the Independent Reviewer of Terrorism Legislation on the Operation of the Terrorism Acts 2000 and 2006* (UK Government, 2020) <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2020/03/Terrorism-Acts-in-2018-Report.pdf> [27]

1.54. DCPs are able to analyse and then profit from personal and commercial information that we reveal when we use the web – for example, they can 'data mine' using proprietary algorithms. This has resulted in some 'tech titan' DCPs having enormous (although opaque) power that is in some ways greater than many nation states.

1.55. All of that information, frequently unknown and even unknowable to the user of a mobile but entirely new in its size, scope and type, if it is available to a DCP, is available to the Government and its agencies if there is a law permitting intelligible access (if that is technically possible). TOLA is such a law.

Schedule 1

A double-lock for TANs and TCNs – a proportionate and more technically sound decision-making process

1.56. In relation to Schedule 1, for the reasons set out in greater detail in the report, TANs and TCNs should be authorised by a body which is independent of the issuing agency or government. These are powers designed to compel a DCP to reveal private information or data of its customers and therefore the usual practice of independent authorisation should apply.

1.57. I reject the argument advanced by agencies that 'a key safeguard in Schedule 1 powers is that they cannot authorise access to data', access being granted by separate warrant issued by a tribunal member or judge. This argument elevates form over substance; after all, Schedule 1 states that its purpose is to reverse the effect of going dark by making intelligible or otherwise useful the content of data already, or in future to be, accessed by warrant. Having accepted that as a key justification in the context of necessity, I cannot ignore it when considering proportionality and rights protection.

1.58. A key safeguard in Schedule 1 is the general limitation that TANs and TCNs must be reasonable and proportionate. The factors to be weighed up in making that decision are comprehensive and, appropriately, cover such key issues as the interests of the issuing agency and the DCP, the necessity and objectives of the notice, its impact on third parties, the availability of other means to achieve the objectives of the notice, and the legitimate expectations of the Australian community relating to privacy and cybersecurity. But those factors should be weighed up by someone independent of the Government or the agency. That should also be so when determining whether complying with the notice is not 'practicable', not 'technically feasible', or would create a 'systemic weakness' or 'systemic vulnerability'.

1.59. I accept that the decision-makers who make decisions under TOLA (be they agency heads or the Attorney-General) will receive advice on technical matters, but the real question is one of independence and the appearance of it. This independence

engenders the necessary trust in the minds of members of the public that the powers are being exercised in a manner that is no more than is necessary. A proper appreciation of the impact of an intrusive TOLA power depends upon the issuer being independent of the agency concerned and, importantly, having technical knowledge. The powers under TOLA cannot be exercised, let alone their impact understood, in the absence of independent technical expertise.

1.60. It was a consistent and, indeed, unanimous theme across non-government submissions that TANs and TCNs should be authorised by either an independent tribunal member or a judicial officer with the benefit of expert technical advice. A number of submissions drew upon the UK's double-lock model of judicial authorisation which, as I explain later, involves an independent exercise of decision-making with the assistance of technical advisers.

1.61. Law enforcement agencies, intelligence agencies and the Department of Home Affairs submitted that TOLA already contains safeguards as to independence and technical advice.

1.62. The desirability of a decision-maker independent of the executive and its agencies is recognised in the Government's Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (IPO Bill), which is a critical step that enables Australia to seek a bilateral agreement with the US under their *Clarifying Lawful Overseas Use of Data Act 2018* (CLOUD Act). The IPO Bill would enable Australia to give effect to such a bilateral agreement by creating a new international production order framework that allows Australian law enforcement and intelligence/security agencies to issue or obtain extraterritorial orders for electronic data on foreign DCPs (where there is an agreement in place).

1.63. Under the regime proposed under the IPO Bill, the Director-General of Security, a Deputy Director-General or ASIO employee may approve an application for an International Production Order (IPO), which then goes to the Attorney-General for consent, after which the application is sent to a nominated member of the Security Division of the AAT to approve *persona designata*. In view of the extensive powers already conferred upon the AAT, the mechanisms outlined in the IPO Bill and the other conclusions I have come to, I recommend the following:

a. A new statutory office – the IPC – should be created to monitor the operation of the system of TANs and TCNs. The IPC should be a retired judge of the Federal Court or the Supreme Court of a State or Territory. The IPC would be appointed by the Governor-General, on the advice of the Attorney-General, following mandatory consultation on the appointment with the Leader of the Opposition.

b. The IPC should be 'dual hatted' – the IPC should be appointed as a part-time Deputy President within the AAT and designated as the head of a new Investigatory Powers Division (IPD) of the AAT, with powers and procedures based upon the existing Security Division. One of the first tasks of the IPC, following wide consultations with interested persons, would be to recommend in detail how that system should work.

c. The IPC would be required to concur in the appointment by the Governor-General of a suitable number of eminent, independent technical experts, who would also be assigned to the new IPD as part-time Senior Members.

d. On the advice of the technical advisers, the IPC would approve and, where necessary, conduct hearings concerning TANs and TCNs.

e. There should also be a registrar of the new IPD who would ensure proper protection of sensitive and classified material.

f. In order to encourage industry support, there should be consultation with industry groups as to who should be appointed to these roles.

g. To promote the interests of transparency and accountability, the IPC would provide the Attorney-General and the PJCIS with an annual report on the operation of Schedule 1, and any other functions that are later be conferred upon the IPC and the IPD. There should be the capacity to provide a classified annexure to these reports as necessary.

No change to TARs

1.64. For the reasons I give later in this report, I do not consider that there is any need to alter the present arrangements relating to TARs (except to recommend that a prescribed form be used). The TAR is not a coercive instrument. A DCP may freely choose to comply or not comply with a TAR without any legal consequence.

Extension to integrity and anti-corruption agencies

1.65. Integrity and anti-corruption agencies should have the same access to Schedule 1 TOLA powers as police do. These agencies are already empowered under other legislative schemes to exercise various investigative powers.

The definitions of 'systemic weakness' and 'systemic vulnerability'

1.66. I have been persuaded that the definitions of 'systemic weakness' and 'systemic vulnerability' are overlapping, create confusion and are not fit for purpose.

1.67. There is little difference conceptually, or in normal or technical usage, between a 'systemic weakness' and 'systemic vulnerability'. These terms are already used

interchangeably in industry and public discourse; there is no further need to use both in the TOLA.

1.68. I have made other recommendations to amend the definition of 'systemic weakness' to bring it into line with the many helpful submissions I received from industry as to the application of those definitions to the technologies at hand. I am satisfied that these amendments, when considered and applied by the IPC, with the assistance of technical advisers, will best ensure that the integrity of the technology and systems used by DCPs is not compromised or the effects limited.

Schedule 2

1.69. I am satisfied that the computer access warrant and associated powers conferred by Schedule 2 are both necessary and proportionate, subject to some amendments.

1.70. I am satisfied that agencies should retain the power to engage in telecommunications interception for the purposes of a computer access warrant without being required to obtain a separate warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) authorising that interception.

1.71. However, to the extent that computer access warrants permit steps to be taken to conceal the activities of the agency in accessing the relevant computers outside of a 28-day period following the expiry of the warrant, I consider that the agency should be required to obtain external approval for those steps. These warrants authorise actual, or potentially significant, incursions into privacy and property, whether it is in the accessing of the computer or the premises on which the computer is located. The decision-maker should be given the opportunity to consider and approve the steps that the agency proposes to take to conceal its activities where they occur a month or more after the warrant has expired.

1.72. To the extent that a computer needs to be removed, I do not consider it a satisfactory limitation that the computer be returned 'within a reasonable period'.[23] Instead, I recommend the item's return 'as soon as is reasonably practicable'.

Schedules 3 and 4

1.73. I am generally satisfied that the powers conferred by Schedules 3 and 4 are both necessary and proportionate, but there are some matters that should be addressed and further monitored.

[23] ASIO Act, ss 25A(4A), 27E(3A). See also SD Act, s 27E(2A). Where the computer access warrant has been obtained by ASIO, this is subject to a situation in which the return of the item would be prejudicial to security. Where that is the case, it is permissible to retain the item until it is no longer the case.

1.74. It should be declared that the powers under Schedules 3 and 4 do not authorise the detention of a person to whom the order applies *where the* agency *in question does not otherwise have any lawful basis on which to do this.* A simple statutory recognition of this would go a long way toward appeasing fears frequently expressed to me.

1.75. I note that Schedules 3 and 4 introduced significant new offences and increased the penalties for noncompliance with an assistance order. The introduction of a monetary penalty as an alternative to imprisonment appears to be an appropriate and proportionate addition, but I consider it appropriate that the prospect of imprisonment for the new offences remains. Despite some concerns about the broadening of offences and increases in penalties, I accept the necessity and proportionality of the increase in criminal penalties for failure to comply with an assistance order and of the introduction of aggravated offences in relation to the more general offences. However, I do recommend that agencies and external stakeholders continue to monitor any prosecutions or penalties.

Schedule 5

1.76. I have concluded that Schedule 5 should be amended to limit its breadth and clarify its scope.

1.77. Section 21A(1) of the ASIO Act empowers the Director-General of Security to 'request a person or body to engage in conduct' that assists ASIO. In my view, as 'conduct' is undefined, it may operate too broadly and, as so drafted, has not been shown to be necessary. I recommend that s 21A(1) be limited to the types of voluntary assistance that are specified in s 21A(5).

1.78. Several stakeholders submitted that the powers conferred on the Director-General of Security under s 21A(1) represent a significant step, as previously the power to confer immunity from civil liability on a person assisting ASIO was limited to the Attorney-General.[24] That function may be further sub-delegated to a 'senior position-holder' under s 16A of the ASIO Act, and I recommend that this power now be exercised by an officer not lower than a Deputy Director-General.

1.79. The legislation is silent on the interaction between the new powers introduced in Schedules 1 and 5. The power to issue a TAR, includes a number of important safeguards and it is necessary to make clear that s 21A does not empower the Director-General to circumvent those protections by making the request under s 21A instead.

[24] See IGIS submission

1.80. Submitters raised the question of whether a person subject to an assistance order (under s 34AAA) is effectively being detained during the period in which they are required to provide the assistance, by being effectively prevented from leaving a specified place prior to the completion of the designated assistance task, under pain of criminal penalties. The Director-General of Security expressly rejected this proposition and the AFP likened its s 3LA power to other powers that compel production or attendance, including production orders, summonses and subpoenas. I am comforted by the agencies' clear assurances on this matter and therefore do not recommend amendments to introduce protections for a person under detention. I still consider it necessary to make it clear, in the ASIO Act, that an assistance order under s 34AAA does not authorise detention of a person to whom this order applies.

Reporting and record-keeping and own motion review powers

1.81. In a number of respects the TOLA reforms fail to provide for adequate, or sometimes any, reporting or record-keeping. Trust is essential to the exercise of the powers conferred by TOLA and the public's acceptance of them. Trust is eroded where the public has inadequate insight into or knowledge of the exercise of the powers. While confidential and sensitive information must be appropriately protected, that is not a licence to keep all such information from the public if it can be conveyed within limits.

1.82. Finally, my successors should be able, of their own motion, to revisit these complex and important matters when they consider it necessary, and the INSLM Act should be amended accordingly.

Structure of this report

1.83. The report is set out in 2 parts. The first part, 'Context', explains the legislation, the threat the legislation responds to and the impact that technology has had on business practice, as well as detailed legal analysis covering common law privacy protections, Australia's international obligations and relevant international comparative approaches. The second part, 'Findings', provides a detailed explanation for my recommendations.

List of recommendations

Schedule 1

Recommendation 1

I recommend that State and Territory anti-corruption commissions be given power to agree to or apply for all 3 types of industry assistance notice – that is, TARs, TANs and TCNs. This power should also be given to the foreshadowed Commonwealth Integrity Commission, when and if it is established.

Recommendation 2

I recommend no change to the capacity of the relevant agencies and a DCP to freely agree a TAR with each other, other than that a prescribed form be used.

Recommendation 3

I recommend that the powers of approval of TANs and TCNs, presently vested in agency heads (for TANs) and the Attorney-General (for TCNs), instead be vested in the AAT and assigned to a new Investigatory Powers Division (IPD). The new IPD, building on the powers and procedures in the Security Division, would operate in a similar way to protect classified material of agencies that are applying for TANs and TCNs and the commercial-in-confidence material of DCPs that are resisting the issue of those notices. The IPD should be able to sit in private as necessary. It would be able to utilise existing AAT powers and procedures, including alternative dispute resolution, to decide for itself whether to issue a TAN or TCN. It would hear submissions and receive evidence from the applying agency and the DCP and be in a position to promptly determine technical questions, such as whether a notice is practicable, reasonable and proportionate or would create a systemic weakness. The Attorney-General's approval would be required for a federal agency to lodge an application for a TCN with the AAT, but this should not be required for any State or Territory body or the Commonwealth Integrity Commission, if and when it is established.

Recommendation 4

I recommend that the IPD consist of a new part-time Deputy President, who would also be the Investigatory Powers Commissioner (IPC), and other eminent lawyers and technical experts as needed. So that they can build up the necessary specialised expertise, and because these powers will not be exercised ex parte, the exercise of these powers should *not* be *persona designata*.

Recommendation 5

I recommend the creation of the IPC as a new statutory office holder, whose functions would be:

a. monitoring the operation of TOLA Schedule 1, including by sharing information with other oversight bodies (such as the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman) and reporting annually on its operation to the Attorney-General and the PJCIS

b. as an additional, part-time Deputy President of the AAT, taking part in the issue of TANs and TCNs as head of the IPD

c. concurring in the appointment of other part-time technical and legal decision-makers assigned to the new IPD who will also be able to assist the IPC in the monitoring roles

d. developing and approving the prescribed form for TAR, TAN and TCN applications and issuing guidelines

e. with the concurrence of the AAT President, issuing practice notes for the IPD.

Recommendation 6

In recognition of the importance of the IPC and the need for the role to be, and be seen to be, filled by someone who is independent of government, is eminent in the law and its application, enjoys bi-partisan support and is not diverted by judicial duties, I recommend that the IPC be a retired judge of the Federal Court or the Supreme Court of a State or Territory, appointed by the Governor-General, on the advice of the Attorney-General, following mandatory consultation on the appointment with the Leader of the Opposition. I would expect there would also be consultation with industry, but I would not mandate it.

Recommendation 7

I recommend amending the definitions in TOLA of 'serious Australian offence' and 'serious foreign offence' so that they align with the definition in existing s 5D of the TIA Act. The effect of this is that, by and large, it would not be open to an agency to obtain an industry assistance notice in respect of an offence punishable by only 3 years' imprisonment.

Recommendation 8

As to *systemic weakness and vulnerability*, I recommend removing all references to 'systemic vulnerability' in Schedule 1, as it is redundant.

Recommendation 9

I recommend that s 317ZG(4A) state prohibited effects as follows:

(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection means a reference to any act or thing that creates a material risk that otherwise secure information will be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.

I further recommend the introduction of the following definitions:

a. 'Otherwise secure information' means 'information of, any person who is not the subject, or is not communicating with the subject of, an investigation'.

b. 'Unauthorised third party' means 'anyone other than a party to the communication, the agency requesting the relevant TAR, TAN or TCN and/or integrity agencies'.

Recommendation 10

I recommend clarification of definitions through the use of non-exhaustive statutory examples:

a. Clarify that 'target technology' in s 317B refers to the specific instance used by the intended target.

b. Include non-exhaustive examples of what is excluded from the meaning of 'electronic protection' in s 317B.

Recommendation 11

I recommend that a 'Designated Communications Provider' not be taken to include a natural person (where that natural person is an employee of a DCP) but only apply to natural persons insofar as required to capture sole traders.

Recommendation 12

I recommend that the AFP no longer have any role in the consideration of industry assistance notices requested by or issued on behalf of State and Territory police.

Schedules 2, 3 and 4

Recommendation 13

I recommend that agencies retain the power to engage in limited telecommunications interception, for the purposes of a computer access warrant, without the need to obtain a separate warrant under the TIA Act authorising that interception.

Recommendation 14

I recommend that an agency be required to seek external authorisation to exercise a concealment of access power if it proposes to take that step more than 28 days after the warrant has expired.

Recommendation 15

I recommend that the legislation be amended to require that a computer or thing which is removed from warrant premises during the execution of a computer access warrant (or related authorisation) be returned to warrant premises if returning the computer or thing is no longer prejudicial to security or, otherwise, as soon as is it reasonably practicable to do so.

Recommendation 16

I recommend that agencies and external stakeholders continue to monitor the prosecutions and convictions (to the extent that information is made publicly available) so as to permit any trends to be discerned as more time passes.

Recommendation 17

I recommend that both s 3LA of the Crimes Act and s 201A of the Customs Act be amended to state, for the avoidance of doubt, that neither authorises the detention of a person to whom the order applies where the agency in question does not otherwise have any lawful basis to detain the person.

Recommendation 18

I recommend that a monetary penalty be retained as an alternative to a penalty of imprisonment for failing to comply with an industry assistance order.

Schedule 5

Recommendation 19

I recommend that the power to request conduct in s 21A(1) be limited in scope to the conduct which can be volunteered under s 21A(5).

Recommendation 20

I recommend that s 21A(1)(e) and s 21A(5)(e) be amended to confine the scope of that immunity from civil liability by requiring instead that 'the conduct does not result in *serious personal injury or death to any person or* significant loss of, or serious damage to, property' (emphasis added).

Recommendation 21

I recommend that s 21A arrangements be approved by the Director-General of Security or a Deputy Director-General.

Recommendation 22

I recommend that s 21A of the ASIO Act be amended to make clear that nothing in s 21A authorises the Director-General of Security to make a request of a person that is properly the subject of a TAR.

Recommendation 23

I recommend that the ASIO Act be amended so as to expressly state, for the avoidance of doubt, that the power does not authorise the detention of a person to whom the order applies where ASIO does not otherwise have any lawful basis on which to do this.

INSLM Act

Recommendation 24

I recommend that the definition of 'counter-terrorism and national security legislation' in s 4 of the INSLM Act be amended to include TOLA so that future INSLMs may review it of their own initiative as necessary.

Reporting, disclosure and oversight

Recommendation 25

I recommend that relevant agencies keep a record of the number of industry assistance orders that are executed and provide them annually to the IPC.

Recommendation 26

I recommend that the various industry assistance order provisions be amended to mandate that the agency in question report to its oversight agency (such as the Commonwealth Ombudsman or the IGIS) as to the number of assistance orders that it executes each year and, other than for ASIO, publish those figures in the public annual reports of the relevant agencies and the oversight bodies. I recommend that statistics on the use of TOLA powers, including a broad description of the acts or things implemented, be made public annually by the IPC (tabled in Parliament within 15 sitting days of receipt) provided that publication would not reveal operationally sensitive or classified information.

Recommendation 27

I recommend that agencies be required to keep records of the number of requests they make of carriers or carriage service providers under s 313 of the Telecommunications Act and to report on those matters annually to the IPC.

Recommendation 28

I recommend that the capacity of the Commonwealth Ombudsman to undertake a joint investigation with State Ombudsmen or Independent Commission Against Corruption oversight bodies such as Inspectors-General be made explicit within s 317ZRB of the Telecommunications Act.

Recommendation 29

As to the Commonwealth Ombudsman's powers of reporting, I recommend that s 317ZRB(7) be repealed so that the Minister cannot remove material from an Ombudsman report under that provision.

Recommendation 30

I recommend that Commonwealth officials be authorised to disclose TAR/TAN/TCN information to the public and to State, Territory and Commonwealth officials when that disclosure is in the national or public interest. A decision to disclose based on those factors may be made by the relevant agency or departmental head or the relevant minister.

Recommendation 31

I recommend that the information disclosure provisions be amended so as to permit DCPs to obtain not merely legal advice but also technical advice in relation to the request or potential request of TARs and the issue or potential issue of TANs and TCNs.

Recommendation 32

As to Schedules 3 and 4, I recommend that there is no need to keep any record of any industry assistance order that an agency issues but which is ultimately not executed.

Recommendation 33

I recommend that ASIO's exercise of powers under Schedule 5 be detailed in its annual report (in a classified appendix as necessary) and that this information be provided to the PJCIS, the Leader of the Opposition, the IGIS, the INSLM, the Attorney-General and the Minister for Home Affairs.

2. CONDUCT OF THE REVIEW

2.1. This review was the most complex I have undertaken in this role. The complexity arose in large part because of the technical nature of the provisions, the keen public interest in these laws and their far-reaching impact across government, industry and civil society, not only in Australia but in partner jurisdictions – notably, the UK and the US.

2.2. As a result of the ongoing sensitivity with regard to the use of these powers by law enforcement and security intelligence agencies, for only the second time as INSLM and the third time since the role was established in 2010 I have produced a classified annexure to this unclassified report. The highly classified and operationally sensitive documents I have viewed during this review are vital in the formation of my recommendations. The INSLM Act specifies what should remain classified and I have complied with its requirements. I note for completeness that all of my recommendations from this review are unclassified and therefore included in this public report.

2.3. I issued requests for information, pursuant to my coercive INSLM Act powers, to relevant agencies. I duly received classified and unclassified responses, and I have included information from the unclassified responses in this public report. Designated Communications Providers (DCPs) and other non-Government submitters were unhappy with the truncated parliamentary process of reviewing the TOLA Bill. At least one objective of my review was to allow those submitters to make detailed submissions and to participate in a more lengthy process.

Legislative history

2.4. On 14 July 2017, the then Prime Minister, the Hon Malcolm Turnbull MP, announced the development of legislation to assist Australian agencies to meet the challenges of modern communications, including the prevalence of encrypted messages. Following this announcement, the Attorney-General's Department, being the policy agency responsible for the reforms at the time, began to develop draft legislation. Responsibility for the draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (TOLA Bill) was transferred to the Department of Home Affairs upon its creation in June 2018, along with a number of other national security policy functions.

2.5. I am informed that:

a. Targeted industry consultations continued throughout 2017 and 2018, culminating in a confidential industry roundtable event on 28 June 2018 hosted

by the then Minister for Law Enforcement and Cyber Security. Key domestic and international providers considered most likely to be affected by the legislation participated in these consultations and were invited to provide comments on a private exposure draft of the TOLA Bill.

b. On 14 August 2018 an exposure draft of the TOLA Bill was released by the then Minister for Law Enforcement and Cyber Security for public comment. The Department of Home Affairs received approximately 15,990 submissions on the exposure draft. The Department of Home Affairs considered that the majority of these submissions (some 15,130) were standardised campaign emails. In the department's view, 55 submissions raised substantive issues from industry, civil society, government bodies and individuals. The overwhelming majority of public submissions related to the proposed industry assistance framework in Schedule 1 of the TOLA Bill.

2.6. On 20 September 2018, the Minister for Home Affairs introduced the TOLA Bill into the House of Representatives. The Bill, as introduced, incorporated minor changes following the exposure draft consultation process. This same day, the Attorney-General referred the TOLA Bill to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for inquiry and report. The PJCIS received 105 submissions and 32 supplementary submissions.

2.7. On 22 November 2018, the Minister for Home Affairs wrote to the PJCIS requesting an accelerated consideration of the Bill, with a view to the Bill being passed before the end of the parliamentary year. The PJCIS held a series of public and private hearings on the question of the necessity of the Bill over the Christmas – New Year period, as referenced by the Minister. On 5 December 2018, the PJCIS tabled a brief advisory report addressing the most pressing issues raised by the TOLA Bill.

2.8. The report consisted of 17 recommendations, including provision for a statutory review of the Bill's operation by the INSLM *within* 18 months of operation. The remaining recommendations were primarily aimed at improving the efficacy and oversight of the industry assistance measures outlined in Schedule 1 of the TOLA Bill.[25] The report did not consider Schedules 2 to 5 of the Bill.

2.9. On 6 December 2018, approximately 173 amendments, both substantive and consequential, were introduced and passed by the Parliament following the PJCIS

[25] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Australian Government, Canberra, 2018) Ch 2, 'Committee comment and recommendations' <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1/section?id=committees%2freportjnt%2f024247%2f26913>.

recommendations. These included a provision for a referral to the PJCIS for a further review of the Act by 3 April 2019 but also a change in the amending Act from the PJCIS recommendations for INSLM review *within* 18 months of enactment, to a provision requiring INSLM review to commence *after* 18 months.

2.10. The PJCIS commenced its next review of TOLA on 17 December 2018. Its particular focus was on clarifying the intent of the PJCIS recommendations made in its 2018 report and to advise on the extent to which those recommendations were addressed. That review received 71 submissions and 7 supplementary submissions. In an oral statement to the House of Representatives on 12 February 2019, the Chair of the PJCIS advised the House that the PJCIS supported 2 further amendments to the Act.

2.11. These amendments extended to:

a. revising the time frame for the INSLM's statutory review of TOLA

b. extending the industry assistance powers provided for under the Act to Commonwealth and State anti-corruption bodies.

2.12. I received a referral to review TOLA from the Chair of the PJCIS, Andrew Hastie MP, by letter dated 26 March 2019. He requested, on behalf of the PJCIS, that the review be completed in time to inform the PJCIS's own statutory review of the legislation, then due by 30 September 2020. This was the first referral to the INSLM in the PJCIS's history. This referral complemented the requirement in s 6(1D) of the INSLM Act that I review and report on TOLA.

2.13. A copy of the letter of referral is at Appendix A.

Intelligence reviews

2.14. In the past half-century a number of distinguished persons have undertaken inquiries into or reviews of aspects of what is now known as the National Intelligence Community.

2.15. Thus, in the 1970s and 1980s there were royal commissions into intelligence agencies conducted by the late Justice Robert Hope AC. There was a further royal commission in the 1990s conducted by the Hon Gordon Samuels AC and Mr Mike Codd AC.

2.16. In the 21st century, governments of the day have appointed reviewers rather than royal commissioners to conduct intelligence reviews, notably:

a. in 2004, an Inquiry into Australian Intelligence Agencies by Mr Philip Flood AO

b. in 2011, an Independent Review of the Intelligence Community by Mr Robert Cornall AO and Dr Rufus Black[26]

c. in 2017, an Independent Intelligence Review by Mr Michael L'Estrange AO and Mr Stephen Merchant PSM[27]

d. at the end of 2019, a Comprehensive Review of the Legal Framework Governing the National Intelligence Community by Mr Dennis Richardson AC.[28]

2.17. I have considered all relevant parts of Mr Richardson's report. It is not yet released. However, I can say that:

a. he understood and respected my independent role both generally and in relation to this current review
b. to the extent that he made comments – or, more rarely, recommendations of relevance to this review – although I am unable to quote from his as-yet unpublished report, I have considered them all in making my findings and recommendations.

Submissions

2.18. Following completion of my previous review on 15 August 2019, on 20 August 2019 correspondence was sent to relevant agency and departmental heads to advise them of my review and that I would shortly be seeking information from them or their organisation in relation to the review (which I generally did by way of compulsory notice under the INSLM Act) and invited classified and unclassified submissions. These relevant agencies comprised Commonwealth, State and Territory law enforcement, integrity, intelligence and policy-oriented functions. On 21 August 2020, I wrote to non-Government organisations, academics, industry representative bodies and other civil society representatives to advise them of my review and invited submissions. On 22 August 2020, I wrote to private sector

[26] Robert Cornall AO and Dr Rufus Black, *2011 Independent Review of the Intelligence Community Report* (Department of the Prime Minister and Cabinet, Canberra, 2011) <https://pmc.gov.au/resource-centre/national-security/2011-independent-review-intelligence-community>.

[27] Michael L'Estrange AO and Stephen Merchant PSM, *Report of the 2017 Independent Intelligence Review* (Australian Government, Canberra, 2017) <https://www.pmc.gov.au/resource-centre/national-security/report-2017-independent-intelligence-review>.

[28] Dennis Richardson AC, Comprehensive Review of the Legal Framework Governing the National Intelligence Community, 2019, Terms of Reference <https://www.ag.gov.au/NationalSecurity/Documents/Terms-of-reference-comprehensive-review.pdf>.

companies and industry to advise of my review and invited submissions. A media release was disseminated to Australian media organisations on 19 August 2019 asking for public submissions to the review. This release was also posted on the INSLM website. A list of submissions is at Appendix B.

Hearings

2.19. In all correspondence, I highlighted the importance of conducting a comprehensive review of the legislation and reiterated provisions in the INSLM Act that give me the power to hold private and confidential hearings. As evident from public debate of the legislation, I recognised that industry has legitimate commercial-in-confidence concerns about the operation of the legislation. Organisations were therefore encouraged to provide a confidential submission or a confidential supplement to a public submission if necessary. I also started an intensive round of industry consultation, including holding one-on-one private meetings with key industry representatives and senior executives from affected private companies.

2.20. On 29 September 2019, I also held a 'town hall' meeting where I engaged directly with industry professionals and representatives and heard their concerns and suggested reforms. This early industry engagement also provided a basis for international engagement. This consultation with industry, a first for INSLM reviews, was important in building trust in the review.

2.21. As with other reviews, I also held private hearings early on with Commonwealth departments and agencies so that I could be provided with classified, as well as unclassified, information in response to my questions.

2.22. These meetings with government and industry occurred before the public hearing in Canberra on 20 and 21 February 2020 so that I had a full appreciation of the issues before the public hearing, but (as has been my general practice as INSLM) also so that the agencies and industry had an idea of my preliminary thoughts and could consider providing any further information I required at the public hearing, including how to express it in a public form, if possible.

2.23. The public hearing was attended by:

a. representatives from many of the relevant agencies and departments (including the Director-General of Security and senior officials from the Australian Federal Police (AFP) and the Department of Home Affairs)

b. representatives from State integrity agencies

c. representatives from industry (including Mozilla and Atlassian)

d. industry advocates (including Access Now and The Allens Hub)

e. the Australian Human Rights Commission

f. the Law Council of Australia.

2.24. This public hearing was live-streamed and, in a first for me as INSLM, it was the subject of a continuous live blog by a representative of ZDNet.

2.25. The audio and transcripts of the hearing are available on the INSLM website. The program for the public hearing is at Appendix C.

2.26. Supplementary information was received from agencies and the private sector following the public hearing, and I engaged in ongoing consultation in Australia with relevant submitters throughout the review.

2.27. The Lowy Institute is an independent, non-partisan international policy think tank located in Sydney. Dr Roger Shanahan of the Lowy Institute was good enough to invite me to speak about my citizenship review in June 2019 and about my TOLA review on 6 March 2020, immediately after my public hearings. The March 2020 speech is available on the INSLM website.

International engagement

2.28. The TOLA provisions do not operate in isolation. As I explore throughout this report, the ubiquity of encryption, the global nature of cyberspace and malicious actors, and the novelty of aspects of TOLA have resulted in TOLA gaining some international attention.

2.29. Similarly, other countries have sought to address the increasingly digitised nature of crime, terrorism and security through their own legislation and operational policy. In November 2019, I travelled to the UK and the US to gain insights into the approaches taken by industry, government agencies and oversight bodies and to ascertain international perspectives on Australia's approaches. I met over 100 people in a very worthwhile two-week round trip.

A Question of Trust and IPCO

2.30. In 2015, my then UK counterpart David Anderson QC presented to then UK Prime Minister the Rt Hon David Cameron his report *A Question of Trust: Report of the Investigatory Powers Review* (*A Question of Trust*). Among other matters, the report considered laws concerning government access to data and metadata and, in that context, what powers and protections should be the subject of legislation. It had much in common with this review and remains a valuable resource to me. In particular:

a. its scope extended well beyond counter-terrorism laws, given that, as the report noted:

> *public authorities intercept communications, and collect information about communications, for a host of other purposes including counter-espionage, counter-proliferation, missing persons investigations and the detection and prosecution of both internet enabled crime (fraud, cyber-attacks, child sexual exploitation) and crime in general.*[29]

b. it considered threats and also, of continuing relevance to the review:

- *the capabilities required to combat those threats,*
- *the safeguards to protect privacy,*
- *the challenges of changing technologies, and*
- *issues relating to transparency and oversight*.[30]

2.31. *A Question of Trust* was highly influential. Among other matters, it led to the enactment of the *Investigatory Powers Act 2016* (UK). It also led to the creation of the Investigatory Powers Commissioner's Office (IPCO). For warrants authorising intrusive powers of access equivalent to those conferred by Schedules 1 and 2 of TOLA, in addition to administrative or ministerial approval, there is a 'double-lock' so that retired judges, with access to high level technical advisers, must also approve the exercise of the powers by reference to those judges' assessments of the lawfulness, proportionality and intrusiveness of the proposed warrant. IPCO also performs the complaint and audit functions undertaken in Australia by the Inspector-General of Intelligence and Security (IGIS), the Hon Margaret Stone AO FAAL, and the Commonwealth Ombudsman, Michael Manthorpe PSM. This model has been influential in my thinking, and I consider it in more detail later in this report.

I have been able to consult with Lord Anderson throughout my tenure, including in relation to this review. Having met the inaugural Investigatory Powers Commissioner, Lord Justice Fulford, in a previous visit, in November 2020 I spent nearly 2 days with the IPCO – notably, with the new Commissioner, the Rt Hon Sir Brian Leveson, formerly President of the Queens's Bench Division and Head of Criminal Justice in the High Court of England and Wales, various judicial commissioners and members of IPCO's Technology Advisory Panel, including its Chair, Sir Bernard Silverman FRS.

2.32. While in the UK I also met with, among others, representatives from:

---

[29] David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (UK Government, London, 2015) [2].

[30] Ibid [1].

a. privacy law and counter-terrorism experts

b. the Metropolitan Police Service (MPS)

c. the Security Service (MI5)

d. the Secret Intelligence Service (MI6)

e. the Government Communications Headquarters (GCHQ)

f. telecommunications industry representatives

g. my counterparts in the current and some former Independent Reviewers of Terrorism Legislation: Jonathan Hall QC, Max Hill QC and the Rt Hon Lord Carlile of Berriew CBE QC FRSA

h. Professor Sir David Omand GCB

i. senior judges.

2.33. In the US, I met with, amongst others, representatives from:

a. the Department of Justice

b. the Federal Bureau of Investigations (FBI)

c. the Senate Intelligence and Judiciary Committees

d. the House Intelligence and Judiciary Committees

e. the Department of Homeland Security

f. the Office of the Director of National Intelligence

g. the State Department

h. the National Security Agency

i. the Privacy and Civil Liberties Oversight Board (which has somewhat similar functions to mine as INSLM)

j. the Carnegie Institute, the US Chamber of Commerce, Cisco, Apple, Atlassian and Facebook.

2.34. I also held roundtable discussions with civil society and industry in Washington DC (hosted by the US Chamber of Commerce) and in California (hosted by Facebook).

2.35. This travel gave me confidence that the recommendations I now make are based on a full understanding of the operation of the US *Clarifying Lawful Overseas Use of Data Act 2018* (CLOUD Act) and the crucial importance of IPCO, both in raising public trust in the exercise of powers similar to those in TOLA and, in the UK, obtaining an agreement with the US Government in relation to the CLOUD Act.

2.36. More generally, the consultation and submissions referred to in this chapter, the appendices and elsewhere in this report, have been vital in the conduct of this review and the recommendations I have come to. I thank all concerned for their contributions.

Those assisting me

2.37. In carrying out the review I was assisted by:

a. my Principal Adviser, Mr Mark Mooney

b. my Counsel Assisting, Mr Yaseen Shariff and Ms Laura Johnston, both of the New South Wales Bar

c. my Solicitors Assisting, Mr James Anderson and Ms Ellen Smith, both from the Australian Government Solicitor

d. my then Acting Deputy Principal Adviser and my Advisers

e. my Executive Officer, Ms Karen Thornton.

2.38. The technological complexities that arose in the review required that I engage Technical Counsel Assisting for the first time as INSLM. I therefore also thank them for their assistance and keen analysis.

2.39. I express my deep gratitude and appreciation to all for their work but particularly the indispensable work of Mr Mooney. Any errors remain mine.

At the public hearing. Left to right: Mr Mark Mooney, Principal Adviser; Dr James Renwick CSC SC, INSLM; Ms Laura Johnston, Counsel Assisting; and Mr James Anderson, Solicitor Assisting

3. CONTEXT: THE THREAT LANDSCAPE

3.1. Before considering whether TOLA remains proportionate to the threat of terrorism or threat to national security or simply to the threat of criminal actors, and remains necessary, I must consider the current threat landscape.

3.2. The threats noted below, coupled with greater awareness of how privacy of internet users may be lost, explain why there is an increasing move to use encryption to protect the legitimate activities of private individuals and corporations.

3.3. Unsurprisingly, encryption is used by criminals and other bad actors. As I wrote in the *Australian Financial Review* last year when requesting submissions for this inquiry:[31]

> *Today, law abiding Australians are highly dependent on digital communications and devices, and digitised services, to conduct personal, corporate and government business: indeed, to live their lives. Effective encryption is critical to ensuring the security and integrity of those activities, protecting us against criminal and other malicious actors whose motives may range from blackmail, to theft of money or identity, to espionage. Equally, the security offered by encryption is being used by the same actors to shield them from investigation by our intelligence and law enforcement agencies.*

3.4. In my opening statement at the public hearings I said this:

> *To give a few examples of illicit activities on the internet, not limited to Australia:*
>
> *a. ISIL has made very effective use of it to publicise, proselytise, and direct terrorism;*
>
> *b. The Christchurch shooter live streamed his atrocities on social media;*
>
> *c. There is large scale theft of private data and corporate intellectual property;*
>
> *d. There is local and transnational organised crime, money-laundering, trafficking of illicit drugs and arms and child sexual exploitation, including on*

[31] Dr James Renwick CSC SC, 'Time for Industry to Speak Up on Australia's Encryption Legislation', *Australian Financial Review*, 21 October 2019 <https://www.afr.com/technology/time-for-industry-to-speak-up-on-australia-s-encryption-legislation-20191017-p531qq>.

> *the dark web, which facilitates the commission of such crimes anonymously and thus with impunity.*
>
> *e. Nation states and their proxies continue to engage in espionage and foreign interference: as former Director-General of Security, Duncan Lewis remarked last year 'the current scale and scope of foreign intelligence activity against Australian interests is unprecedented'. But they also work on their capacities to engage in cyber-attacks such as Computer Network Attacks not only, say, to disable access by another country's military to its computers and web servers, but also to have kinetic effects, for example by releasing dam water, turning off power to hospitals, or attacking a stock exchange's records. It is no accident that such conduct is capable of amounting to a 'terrorist act' under the Criminal Code. The New York Times' 'Privacy Project' provides many examples of such behaviour, and also of the large scale theft of private data and corporate intellectual property – as do the unsealed indictments filed by the US Department of Justice against, for example, members of the Chinese People's Liberation Army.*[32]

The current threat level

Terrorism

3.5. Currently, the level of threat of a terrorist act occurring in Australia remains at 'probable', and the evidence before me suggests that this position will remain unchanged for some time. The threat is mainly from radical violent Islamists[33] – notably, the Islamic State of Iraq and the Levant (ISIL) – but there is also some radical right-wing activity. Although the comprehensive travel ban currently in place to deal with the COVID-19 pandemic largely prevents people from arriving in Australia from territory formerly occupied by ISIL, the capacity to influence online is undiminished. In contrast, radical right-wing activity tends to be 'homegrown', although it is significantly inspired by events overseas.

3.6. In my 2018–2019 annual report, tabled in February 2020, I noted links between terrorism and the internet as follows:

> *An added risk emerged during the reporting period. The attack by an Australian in Christchurch, New Zealand in March 2019 brought to the fore the dangers of violent extremists drawing on ethno-nationalist, racist or fringe right-wing*

[32] Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 3–4 (footnotes omitted).

[33] Violent Islamist action is to be contrasted with the major world religion of Islam, which practises peace.

> *narratives and ideologies. The perpetrator conducted the attack alone. However, he drew inspiration from a global network of like-minded individuals who often disseminate and discuss their views online. The phenomenon is not new. Similar, albeit relatively less lethal, attacks inspired by the same narrative both preceded and followed from the Christchurch attack. Still, Christchurch turned into a seminal event in the history of such terrorism for its lethality and use of technology to maximise impact, in particular the live streaming of the attacks on social media.*[34]

3.7. In the 2018 version of CONTEST[35] – The United Kingdom's strategy for countering terrorism – the following is noted:

> *[69] The threat from terrorism is constantly evolving. Globally, terrorist groups and networks of all ideologies continue to develop organically, exploiting social media, technology and science to further their aims and ambitions.*
>
> *[78] Evolving technology creates new challenges, risks and opportunities in fighting terrorism. Terrorists use new technologies, like digital communications and unmanned aerial vehicles, to plan and execute attacks, and tend to adopt them at the same pace as society as a whole. For terror groups, the internet is now firmly established as a key medium for the distribution of propaganda, radicalisation of sympathisers and preparation of attacks.*
>
> *[79] Evolving technology, including more widespread use of the internet and ever-more internet-connected devices, stronger encryption and cryptocurrencies, will continue to create challenges in fighting terrorism. Data will be more dispersed, localised and anonymised, and increasingly accessible from anywhere globally.*[36]

3.8. My UK counterpart, Jonathan Hall QC, in his most recent report, has rightly written:

---

[34] Dr James Renwick CSC SC, Independent National Security Legislation Monitor, *Annual Report 2018–2019* (Australian Government, Canberra) 6 [2.9] <https://www.inslm.gov.au/node/182>.

[35] This has 4 strands – namely, Pursue (to stop terrorist attacks); Prevent (to stop people from becoming terrorists or supporting violent extremism); Protect (to strengthen protection against terrorist attack) and Prepare (where an attack cannot be stopped, to mitigate its impact).

[36] UK Government, *CONTEST: The United Kingdom's Strategy for Countering Terrorism* (2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf>.

> *[2.30] Modern technology calls into question legislation written in an earlier era, and terrorism legislation is no exception. Interrogating a phone can reveal more data than searching a house; information is electronic, and accessed, rather than physical, and seized; contact is encrypted and routed around the world; worldwide publication is open to every person with a smartphone.*[37]

Espionage and foreign interference

3.9. In relation to counter-espionage and foreign interference, I noted in my recent annual report the remarks of the then Director-General of Security, Duncan Lewis AO DSC CSC:

> '*The counter-espionage and foreign interference issue … is something which is ultimately an existential threat to the state, or it can be an existential threat to the state. It has the capacity to do that.' This threat is not confined to 'one particular nation', although sophistication and intent varied greatly among other countries. ASIO assessed that 'the current scale and scope of foreign intelligence activity against Australian interests is unprecedented … Unlike the immediacy of terrorism incidents, the harm from acts of espionage may not present for years or even decades. These sort of activities are typically quiet, they're insidious and they have a long tail.*[38]

3.10. The full extent of the use of the internet by hostile foreign States and their proxies to engage in espionage and foreign interference is still not fully appreciated – in part because of their technical skill and the related problem of correctly identifying those hostile actors.

3.11. The most recent public version of the Australian Security Intelligence Organisation (ASIO) annual report states:

> *Foreign intelligence services seek to exploit Australia's businesses for intelligence purposes. That threat will persist across critical infrastructure, industries that hold large amounts of personal data, and emerging sectors with unique intellectual property that could provide an economic or strategic edge. Foreign states continue to undertake acts of cyber espionage targeting Australian Government, academic, industrial and economic information*

---

[37] Jonathan Hall QC, Independent Reviewer of Terrorism Legislation, *The Terrorism Acts in 2018: Report of the Independent Reviewer of Terrorism Legislation on the Operation of the Terrorism Acts 2000 and 2006* (UK Government, 2020) <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2020/03/Terrorism-Acts-in-2018-Report.pdf>.

[38] James Renwick CSC SC, Independent National Security Legislation Monitor, *Annual Report 2018–2019* (Australian Government, Canberra) 7 <https://www.inslm.gov.au/node/182>

> *technology networks and individuals, to gain access to sensitive and commercially valuable information – these threats to Australia's security continue to increase in scale and sophistication. Cyber espionage is a relatively low-risk and scalable means of obtaining privileged information, which adds another potent method to the array of espionage techniques through which foreign intelligence agencies and other hostile actors can target Australians and Australian interests.*[39]

Criminal activities more generally

3.12. As noted earlier, this review extends well beyond counter-terrorism and national security threats to crime more generally. That is not to say that the links between organised crime and terrorists are not real and frequent. Thus, the United Nations Security Council (UNSCR) Resolution 1373, passed immediately after the events of 11 September 2001, noted with concern 'the close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials'.[40]

3.13. Further, criminals frequently misuse the internet to commit particularly heinous crimes such as child sexual exploitation, as well as 'general' crime. These have no counter-terrorism and national security aspect. As the Minister for Home Affairs recently said when introducing the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (IPO Bill):

> *Almost every crime type and national security concern has an online element – agencies require electronic information and communications data not only for cyber investigations but also for investigations and prosecutions regarding violent crimes, human trafficking and people smuggling, drug trafficking, financial crimes, terrorism and child sexual abuse.*[41]

Encryption helps both bad and good actors

3.14. The internet is used by almost everyone in Australia, including for work and private communication and commercial and social activities. Given its ubiquity, users need to be able to use it securely to ensure privacy and deter theft and misuse of our information and other data from the spectrum of threats noted above.

---

[39] Australian Security Intelligence Organisation, *Annual Report 2018–19* (Australian Government, Canberra, 2019) <https://www.asio.gov.au/sites/default/files/2018-19%20Annual%20Report%20WEB2.pdf>.

[40] SC Res 1373, UN SCOR, S/RES/1373 (28 September 2001) [4].

[41] Explanatory Memorandum, Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth).

3.15. But bad actors, especially but not only the more sophisticated, increasingly use encryption of both data and metadata to disguise their activities. Therefore, the work of law enforcement agencies, intelligence agencies and anti-corruption bodies is liable to be thwarted or at least made more difficult.

3.16. The position of the Australian Federal Police (AFP), although not unique, is a good example of the problems faced.

3.17. In its submission to the review the AFP noted that encrypted forms of communication are an increasingly significant issue for law enforcement agencies. It submitted that:

a. *more than 90 percent of content currently being lawfully intercepted by the AFP uses some form of encryption;*

b. *encryption has directly impacted around 200 operations conducted by the AFP in the last 12 months, all of which related to the investigation of serious criminality including terrorism offences carrying a penalty of seven years or more; and*

c. *by late 2020, it is 'expected that nearly all communications content of investigative value will be encrypted.'*[42]

3.18. The AFP explained the impact of this as follows:

> *Communication technology and encryption underpins everyday modern communications and is advancing at an incredible rate and is contributing to the creation of ungovernable space, free from the rule of law.*
>
> *…*
>
> *Serious criminals (including terrorists and child sex offenders) who have an understanding of law enforcement's technical impediments are known to deliberately use encryption technologies to prevent police from lawfully accessing their criminal communications. This makes it increasingly difficult for the AFP to prevent, deter, disrupt and investigate criminal activity.*
>
> *…*
>
> *The AFP understands the benefits of modern technology and the telecommunication industry's objective to provide a secure online environment for users. However this same technology is increasingly used by criminals to conceal illicit activities and evade investigative efforts. Criminal entities are astute to gravitating toward safe havens in which to undertake their criminality,*

[42] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, 10.

whether these be defined by societal, legal or technical opportunities. While enhanced security and privacy should be the foundation on which all technology and communications are developed, these foundations also significantly enhance the opportunities for criminality to flourish without fear of detection and disruption by law enforcement.[43]

3.19. The AFP also provided statistics and examples to demonstrate the impact of encrypted forms of communication on their operations:

Since 2016, the AFP has prosecuted 20 individuals for a range of terrorism-related offences where encrypted technology was used in an attempt to inhibit law enforcement investigation.

In March 2018, the AFP in collaboration with the FBI (US) and RCMP (Canada) executed 25 warrants internationally (19 in Australia) relating to the sale and disruption of encrypted communications provider Phantom Secure, resulting in 5 individuals being indicted in the US on Racketeering charges.

- *In May 2019, the CEO was sentenced to 9 years jail and US$80M in assets was seized from Phantom Secure as the proceeds from knowingly supporting transnational criminal organisations through the provision of encrypted communications.*
- *AFP analysis identified more than 10,000 handsets in Australia, all of which were immune to traditional lawful access technology.*[44]

3.20. The Independent Broad-Based Anti-Corruption Commission (IBAC) of Victoria also provided advice on the increasing prevalence of encrypted communication:

In recent years, the value of traditional telecommunications interception, in particular, has waned as more of IBAC's targets use encrypted messaging applications to communicate. Over the past three financial years, 67 per cent of IBAC's intercepted data was identified as encrypted. In the past financial year alone, this figure was 92 per cent. This has the certain effect of hampering IBAC's efforts to gather evidence of corrupt conduct for criminal prosecution. This marked increase in encrypted communications, and user's awareness of limitation to decrypt them has led to a number of occasions where investigations were extended by several months and/or required the use of more intrusive investigative methods to identify offending behaviour.[45]

---

[43] Ibid 9–11.

[44] Ibid 10.

[45] Independent Broad-based Anti-corruption Commission (Victoria), Submission No 3 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 12 September 2019, 2.

3.21. Further, ASIO provided advice about the particular challenges it has experienced:

> *The contemporary digital landscape is characterised by increasing complexity, the ubiquitous use of encryption, and a rapid expansion in new methods of communication and communication providers. This environment has increasingly challenged the ability of ASIO to fulfil its functions under existing legislation. The new mechanisms provided under the Act allow ASIO to maintain a level of parity with respect to its operational effectiveness within this context.*
>
> *Over 95 per cent of ASIO's most dangerous counter terrorism targets use encrypted communications. It is estimated that by 2020 all electronic communications of investigative value will be encrypted. There is no evidence that this trend will be reversed into the future. In this environment ASIO's ability to access data of security relevance has been increasingly frustrated by the same encryption that benefits society more broadly. Within this context ASIO will increasingly need to call upon the assistance of communications providers to gain access to data, and to do this in a cooperative way that does not weaken the protections that encryption offers to the benefit of all Australians.*[46]

3.22. A number of authors and submitters have suggested that the current views on the impact of encryption on law enforcement and intelligence must take into account that the past few decades have in many ways been a golden age for those bodies because of the widespread unencrypted use of the internet for communications.[47]

3.23. In its submission to the review the Office of the Australian Information Commissioner (OAIC) acknowledged the challenges to law enforcement presented by technological developments and encrypted forms of communication:

> *The OAIC recognises the challenge facing law enforcement, national security and intelligence agencies combating threats to national security in the digital age. The OAIC recognises there is a need to provide these agencies with greater access to information to address today's complex threats, and to enable timely international cooperation. … The powers permitted under the Act have the potential to significantly weaken important privacy rights and protections under the Privacy Act. The encryption technology that can obscure criminal*

[46] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, [2]–[3].

[47] See, for example, Riana Pfefferkorn, Submission No 4 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 12 September 2019, 6.

> *communications and pose a threat to national security is the same technology used by ordinary citizens to exercise their legitimate rights to privacy.*[48]

Conclusion

3.24. In summary, I accept the evidence from intelligence, police and integrity agencies that near-universal encryption of content and, to a lesser extent, metadata has made their essential tasks significantly more difficult and in some instances impossible. Given the current threat levels for terrorism, foreign interference and crime more generally, some legislative response was justified. No country which operates under the rule of law, as Australia does, can countenance the creation of ungovernable space, free from the rule of law.

3.25. However, encryption simultaneously preserves legitimate as well as illicit activities. This means that any legislated response to 'going dark' must not undermine the security for legitimate communications or communications systems upon which so much in every society, including our own, depends. As the Minister for Home Affairs acknowledged in TOLA's second reading speech, TOLA may indirectly make some people more reluctant to use communications services:

> *It is plausible that a person may minimise their use of communications services if they believe government agencies can ask providers to facilitate access to communications carried through these service, for example by removing forms of electronic protection applied to their communications if they are capable of doing so*.[49]

3.26. Hence it is imperative that we have clear law, in proportionate terms, with effective oversight of a type which provides reassurance in a democratic society and, in particular, independent, technically informed, issue of Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs).

---

[48] Office of the Australian Information Commissioner, Submission No 20 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 20 September 2019, [3]–[4].

[49] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 14 [40].

4. CONTEXT: ANALYSIS OF TOLA

4.1. This chapter provides an overview and detailed analysis of the impact that TOLA made. This analysis is fundamental to understanding the issues presented by stakeholders and is the basis for my recommendations.

4.2. TOLA confers a variety of powers and capacities upon the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD), the Australian Criminal Intelligence Commission (ACIC), police and integrity agencies. Broadly speaking:

a. ASIO is Australia's security intelligence agency. Its key focus is to 'obtain, correlate and evaluate intelligence relevant to security'. It is not a law enforcement body.

b. ASIS is Australia's overseas secret intelligence agency.

c. ACIC is Australia's national criminal intelligence agency.

d. ASD is Australia's signals intelligence collection body. It has a cybercrime disruption role.

e. The Australian Federal Police (AFP) and State and Territory police forces and services investigate and seek to prevent the commission of crime and assist those who prosecute it.[50]

f. Integrity agencies investigate unlawful and inappropriate behaviour by Government agencies. Some focus on police or intelligence agencies; others focus on public officials more broadly.

Pre-TOLA powers

4.3. The following investigatory powers existed prior to TOLA and, unless otherwise indicated, still exist.

4.4. Under the *Crimes Act 1914* (Cth), the AFP can obtain evidence using warrants in respect of either *premises* or *persons*, executed by police constables. Under those warrants it can search for and seize 'evidential material', which includes things 'in

[50] The AFP's functions under the *Australian Federal Police Act 1979* (Cth) (AFP Act) include such 'police services' as the investigation of federal offences and the 'prevention of crime and the protection of persons from injury or death, and property from damage, whether arising from criminal acts or otherwise': AFP Act, s 4.

electronic form' as well as physical things. Sometimes those are 'delayed notification' warrants.

4.5. Under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), the AFP and State and Territory police can obtain access to telecommunications data or stored communications that already exist and they can intercept communications in real time. That access might be given by a telecommunications provider without the need to obtain the actual mobile phone. They could also obtain a surveillance device warrant under the *Surveillance Devices Act 2004* (Cth) (SD Act).

4.6. Under the Crimes Act, the SD Act and the TIA Act, search warrants for police are issued by magistrates, other judges and Administrative Appeals Tribunal (AAT) members acting as *persona designata*. The propriety and lawfulness of applications for warrants and their execution are reviewable by Ombudsman's offices in each jurisdiction. They are also reviewable by courts – this often occurs when a warrant is challenged at the point of execution[51] or when something seized by warrant is tendered in proceedings, typically a criminal trial.

4.7. Under the TIA Act and the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), ASIO can obtain telecommunication interception (TI) warrants and also, under the ASIO Act, warrants to search premises and postal articles and access the contents of computers (computer access warrants). All of these can be obtained and executed covertly (that is, without ever having to notify the persons whose property or communications are being examined, copied or seized).

4.8. Historically, all ASIO warrants were issued by the Attorney-General. That altered when the ASIO Act provided, in Part III, Division 3, for special powers in relation to terrorism offences, called Questioning Warrants and Questioning Detention Warrants.[52] These are issued by an independent Issuing Authority at the request of ASIO and the concurrence of the Attorney-General. The Telecommunications Legislation Amendment (International Production Orders) Bill 2020 is currently under examination by the PJCIS. The Bill contains a significant proposal that would provide a framework for Australian agencies – including ASIO – to obtain independently authorised international production orders from the AAT. This is considered later in this report.

4.9. Under the TI Act and SD Act, integrity agencies, whose remit often includes considering the conduct of police, may, like police, obtain warrants.

---

[51] The principles are discussed in *Smethurst & Anor v Commissioner of Police* [2020] HCA 14; and *Australian Broadcasting Corporation v Kane (No 2)* [2020] FCA 133.

[52] See also the Australian Security Intelligence Organisation Amendment Bill 2020.

Schedule 1

4.10. The amending Act contains 5 schedules. In the executive summary I briefly note their terms and purpose. The following sections provide further detailed analysis on the operation and impact of each schedule.

Overview of Schedule 1

4.11. Schedule 1 deals with industry assistance notices. It amends the *Telecommunications Act 1997* (Cth) by adding in a new Part 15. It also amends the ASIO Act, the *Criminal Code Act 1995* (Cth) (Criminal Code), the TIA Act and the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (ADJR Act). Part 1 of Schedule 1 entered into force on 9 December 2018.[53]

Scope of powers prior to TOLA

4.12. Since long before the reforms enacted by TOLA, the Telecommunications Act has required carriers and carriage service providers to assist law enforcement and intelligence agencies. Thus, s 313 of the Telecommunications Act requires carriers, carriage service providers and carriage service intermediaries to give Commonwealth, State and Territory officers and authorities 'such help as is reasonably necessary' for a series of listed purposes.

4.13. Those purposes relevantly include enforcing criminal laws and laws imposing pecuniary penalties, assistance in the enforcement of foreign criminal laws, and safeguarding national security. Section 313 also imposes on carriers and providers an obligation to do their best to prevent telecommunications networks and facilities from being used to commit offences against Australian law.

4.14. In broad terms, the amendments effected by Schedule 1 of TOLA grant agencies additional coercive powers which they can exercise in respect of 'Designated Communications Providers' (DCPs). Schedule 1 does so by introducing a new part, Part 15, to the Telecommunications Act. The powers that Part 15 contains are in addition to, rather than in place of, carriers' and others' obligations under s 313 of the Telecommunications Act, which continues in force despite the passage of TOLA.

4.15. The main reforms effected by Schedule 1 are as follows:

---

[53] TOLA, s 2(1), item 2 of table entitled 'Commencement Information'. The limited exception to this is Part 2 of Schedule 1, which commences at the time (if any) that the *Federal Circuit and Family Court of Australia Act 2018* (Cth) enters into force, which has not to date occurred. The sole effect of Part 2 of Schedule 1 is to alter the reference to the 'Federal Circuit Court of Australia' in certain sub-sections of Part 15 of the *Telecommunications Act 1997* (Cth), in the event that that Court merges with the Family Court of Australia.

- It introduces the concept of DCPs.
- It introduces the power to issue Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) to DCPs (each called an 'industry assistance notice').
- It introduces the concept of a 'listed act or thing'.
- It introduces the concepts of 'systemic weakness' and 'systemic vulnerability'.
- It provides immunity from civil liability (and criminal liability in respect of certain offences) for conduct that is in compliance with an industry assistance notice.
- It provides for compensation for conduct undertaken in compliance with a TAN or TCN.

Amendments effected by TOLA

Introduction of the concept of 'Designated Communications Provider'

4.16. Section 317C of the Telecommunications Act, as introduced by TOLA, defines the term 'Designated Communications Provider' (DCP). The term is significant, as it sets the bounds of those on whom an industry assistance notice may issue. The term is defined by way of the table set out below. It indicates the types of legal or natural persons that fall within the definition of DCP and the 'eligible activities' of each type of DCP. It is a deliberately wide definition. According to the Explanatory Memorandum, it is 'crafted in technologically neutral language to allow for new types of entities and technologies to fall within its scope as the communications industry evolves'.[54]

4.17. The table includes entities that were already the subject of regulation under the Telecommunications Act – namely, carriers, carriage service providers and carriage service intermediaries. The definition also encompasses (among others) a person who provides an electronic service that has end users in Australia; who develops, supplies or updates software for use in connection with a carriage service or electronic service; who manufactures or supplies components for use in Australia; or who installs or maintains equipment on behalf of customers or connects equipment to a telecommunications network in Australia.

4.18. Accordingly, the list of entities that fall within the definition of DCP is broad. It includes both natural and legal persons operating at every level of the supply chain.

[54] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth), [26].

Further, it includes not only those who operate in Australia but also anyone whose technology, software and components are likely to be used in Australia or to be connected to a telecommunications network in Australia. A list detailing examples of DCPs is now available on the Department of Home Affairs website, released under a freedom of information request.

Introduction of TARs, TANs and TCNs

4.19. The most significant aspect of the Schedule 1 reforms is the introduction of the power to issue industry assistance notices (TARs, TANs and TCNs). While they differ in scope and effect, the common feature of these 3 notices is that they are:

a. issued by or on behalf of an Australian security or law enforcement agency

b. to a DCP[55]

c. with a view to requesting (in the case of a TAR) or compelling (in the case of a TAN or TCN) the DCP's assistance by

d. having them do a listed act or thing.[56]

4.20. An industry assistance notice can request or compel a DCP to do a listed act or thing for particular purposes. In broad terms, the head of a given agency can *only*:

a. request or compel (as the case may be) a DCP to do a listed act or thing 'directed towards ensuring that the [DCP] is capable of giving help to' the agency that he or she heads

b. in relation to the performance of a function or power that Australian law confers on that agency[57]

c. insofar as that function or power relates to a 'relevant objective' of that agency.[58] The term 'relevant objective' broadly reflects the functions of the respective agencies – namely, national security and related objectives in the case of security agencies; and enforcing Australian or foreign criminal laws in the case of law enforcement (defined as 'interception') agencies.

[55] Telecommunications Act, s 317C.

[56] Ibid s 317E.

[57] Ibid s 317G(2).

[58] Ibid s 317G(5).

4.21. TARs and TANs are ordinarily given in writing. They may be given orally only in exceptional circumstances – in particular, where it is necessary to deal with 'an imminent risk of serious harm to a person or substantial damage to property'.[59]

4.22. A DCP[60] that is acting in accordance or purported accordance[61] with the request is immune from civil liability for that conduct where it is in connection with the eligible activities of that DCP.[62]

4.23. The agency head who issues or requests the industry assistance notice is, in every case, obliged to notify the body with oversight of the agency's conduct (that is, the Inspector-General of Intelligence and Security (IGIS) or the Commonwealth Ombudsman, as the case may be) within 7 days of giving the request or notice, although the request or notice remains valid whether or not that notification occurs.[63]

Technical Assistance Requests

4.24. By a TAR, an agency head requests that the DCP do one or more specified acts or things in connection with any or all of the eligible activities of the DCP where those acts or things:

a. relate to the performance of a function or power of the agency, and

b. relate to a relevant objective of the agency.

4.25. The power to agree a TAR[64] with a DCP vests in the Director-General of Security, the Director-General of the ASIS, the Director-General of the ASD or the chief officer of an 'interception agency'. The term 'interception agency' means the AFP, the ACIC or the police force or service of a State or the Northern Territory.[65]

4.26. An agency head cannot issue a TAR unless satisfied as to the statutory decision-making criteria.[66] These include that 'the request is reasonable and proportionate' and that the DCP's compliance with the request is both 'practicable' and 'technically feasible'. The agency head is required to have regard to a number of criteria in

[59] Ibid ss 317H, 317M.

[60] And its relevant officers, employees and agents.

[61] For example, where an apparently valid notice is later set aside by a court.

[62] Telecommunications Act, ss 317G(1), 317ZJ.

[63] Ibid ss 317HAB, 317MAB, 317TAB.

[64] Ibid s 317G(1).

[65] Ibid s 317B.

[66] Ibid s 317JAA.

assessing whether the request is reasonable and proportionate, including such important matters as:[67]

a. the legitimate interests of the DCP to whom the request relates
b. the availability of other means to achieve the objectives of the request
c. whether the request is the least intrusive form of industry assistance – that is, when compared to other forms of industry assistance known to the head of the issuing authority, as the case requires – so far as the persons whose activities are not of interest to that authority are concerned
d. whether the request is necessary
e. the legitimate expectations of the Australian community relating to privacy and cybersecurity.[68]

4.27. There are no equivalent criteria to determine whether or not the request is technically feasible.

4.28. The agency head who issues the TAR is under an obligation to notify the DCP that compliance with the request is voluntary.[69]

Technical Assistance Notices

4.29. By a TAN, an agency head requires a DCP to do one or more specified acts or things in connection with any or all of the eligible activities of the provider where those acts or things:

a. relate to the performance of a function or power of the agency, and

b. relate to a relevant objective of the agency.

The acts or things the TAN specifies cannot be directed towards ensuring that the DCP is capable of giving help to the agency in question[70] (which is the function of a TCN).

4.30. The power to issue a TAN[71] to a DCP vests in the Director-General of Security or the chief officer of an interception agency (it does not extend to ASIS or ASD). Where the interception agency in question is a State or Territory police force, the AFP Commissioner must approve the head of the interception agency that is issuing the

[67] Ibid s 317JC.

[68] Ibid s 317JC, sub-sections (c), (e)–(h).

[69] Ibid s 317HAA.

[70] Ibid s 317L(2A).

[71] Ibid s 317L(1).

notice.[72] That is significant in Australia's federal system, where State and Territory police are not otherwise subordinate to the AFP.

4.31. A DCP that does not comply with a requirement under a TAN, to the extent that the DCP is capable of doing so, is liable to a civil penalty. In the case of a body corporate that can be up to approximately $10,000,000. The DCP has a defence to that liability by proving that compliance with the requirement involves doing an act or thing in a foreign country which would contravene a law of that country.[73]

4.32. An agency head cannot issue a TAN unless satisfied as to the statutory decision-making criteria.[74] These include that 'the requirements imposed by the notice are reasonable and proportionate' and that the DCP's compliance with the notice is both 'practicable' and 'technically feasible'. In assessing whether the request is reasonable and proportionate, the agency head is required to have regard to a number of criteria that are similar to those applicable in the case of a TAR.[75] Section 317RA is critical. It states:

> *In considering whether the requirements imposed by a technical assistance notice or a varied technical assistance notice are reasonable and proportionate, the Director-General of Security or the chief officer of an interception agency, as the case requires, must have regard to the following matters:*
>
> *(a) the interests of national security;*
>
> *(b) the interests of law enforcement;*
>
> *(c) the legitimate interests of the designated communications provider to whom the notice relates;*
>
> *(d) the objectives of the notice;*
>
> *(e) the availability of other means to achieve the objectives of the notice;*
>
> *(ea) whether the requirements, when compared to other forms of industry assistance known to the Director-General of Security or the chief officer, as the case requires, are the least intrusive form of industry assistance so far as the following persons are concerned:*

[72] Ibid s 317LA.

[73] Ibid s 317ZB(5).

[74] Ibid s 317P.

[75] Ibid s 317RA.

(i) persons whose activities are not of interest to ASIO;

(ii) persons whose activities are not of interest to interception agencies;

(eb) whether the requirements are necessary;

(f) the legitimate expectations of the Australian community relating to privacy and cybersecurity;

(g) such other matters (if any) as the Director-General of Security or the chief officer, as the case requires, considers relevant.

4.33. Further, before issuing a TAN, the agency head is required to consult the DCP that is the intended recipient of the notice, except in circumstances of urgency.[76]

Technical Capability Notices

4.34. By a TCN, an agency head requires a DCP to do one or more 'specified acts or things' in connection with any or all of the eligible activities of the provider where those acts or things:

a. relate to the performance of a function or power of the agency, and

b. relate to a relevant objective of the agency.

In the case of a TCN, as distinct from a TAN, the listed act or thing must 'be directed towards ensuring that the designated communications provider *is capable of* giving listed help to' the agency in question (emphasis added).[77]

4.35. The Attorney-General alone has the power to issue a TCN to a DCP, on application of the Director-General of Security or the chief officer of an interception agency (but neither ASIS nor ASD).[78] The notice must be in writing. In deciding whether to issue a TCN, the Attorney-General must be satisfied that 'the requirements imposed by the notice are reasonable and proportionate' and that compliance with the notice is 'practicable' and 'technically feasible'.[79] The Attorney-General is required to have regard to a number of criteria in assessing whether the request is reasonable and

[76] Ibid s 317PA.

[77] Ibid s 317T(2).

[78] Ibid s 317T(1).

[79] Ibid s 317V.

proportionate, which essentially ensures the same requirement as for TARs and TANs.[80]

4.36. Before issuing a TCN, the Attorney-General must open a period of consultation with the DCP that is the intended recipient of the TCN. Section 317W provides that the Attorney-General must not issue a TCN to a DCP unless he or she has given the DCP a 'consultation notice' which invites the DCP to 'make a submission to the Attorney-General on the proposed technical capability notice'.[81] The Attorney-General cannot issue the TCN unless he or she has 'considered any submission that was received within the time limit specified in the consultation notice'. That time limit cannot be less than 28 days (except in certain circumstances).[82]

4.37. Section 317WA provides that, during that period, the DCP may give the Attorney-General a written notice requesting the carrying out of an assessment of whether the TCN should be given. If it does so, the Attorney-General is to appoint 2 'assessors' to carry out that assessment. The first must be a technical expert and the second a former judge of at least 5 years' standing.[83] The assessors are required to report to both the Attorney-General and the DCP on various things that include essentially the same criteria as the original decision-maker is required to consider.[84] The assessors' report is not binding on the Attorney-General, but he or she is bound to take it into account before issuing the TCN.[85]

4.38. Similar consultation provisions apply where a variation to a TCN is proposed.[86]

4.39. A DCP that does not comply with a requirement under a TCN, to the extent that the DCP is capable of doing so, is liable to a civil penalty.[87] As with a TAN, the DCP has a defence to that liability by proving that compliance with the requirement involves the doing of a thing in a foreign country which would contravene a law of that country.[88]

---

[80] Ibid s 317ZAA.

[81] Ibid s 317W(1)(a).

[82] Ibid ss 317W(1)(b), (2), (3).

[83] Ibid ss 317WA(4), (5).

[84] Ibid s 317WA(7).

[85] Ibid s 317WA(11).

[86] Ibid s 317YA.

[87] Ibid ss 317ZA, 317ZB.

[88] Ibid s 317ZB(5).

Introduction of the concept of a 'listed act or thing'

4.40. Section 317E of the Telecommunications Act defines the term 'listed act or thing'. The definition is exhaustive and broad. It is set out in full at Appendix D. It includes, among other things:

a. 'removing one or more forms of electronic protection' applied to a product or service

b. 'providing technical information'

c. 'installing, maintaining, testing or using software of equipment'

d. 'facilitating or assisting access' to facilities, equipment, devices, services and software

e. 'modifying' or 'substituting' products or services

f. 'assisting with the resting, modification, development or maintenance of a technology or capability'.

4.41. It also includes doing an act or thing to conceal that something has been done to perform a function or exercise a power under Australian law, but not insofar as that amounts to 'making a false or misleading statement' or 'engaging in dishonest conduct'.[89]

Introduction of the concepts of 'systemic weakness' and 'systemic vulnerability'

4.42. A key limitation on the issue of TARs, TANs and TCNs is that none of them can have the effect of 'requesting or requiring' the DCP on whom it issues 'to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection' or of preventing a DCP from rectifying such a weakness or vulnerability.[90] That expressly includes building a new decryption capability into a form of electronic protection, which in turn includes anything that would render systemic methods of encryption less effective.[91] The terms 'systemic weakness' and 'systemic vulnerability' are defined in s 317B of the Act as follows:

> ***systemic vulnerability*** *means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*

[89] Ibid s 317E(1)(j), (2).

[90] Ibid s 317ZG(1).

[91] Ibid ss 317ZG(2), (3).

> ***systemic weakness*** *means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*

4.43. A TAR, TAN or TCN has no effect where it would have the effect of implementing, or preventing a DCP from rectifying, a systemic weakness or vulnerability.[92] Part 15 also contains other limitations on what an industry assistance notice can lawfully require.[93] For example, where a warrant was originally required to obtain the relevant information or data, such a warrant is still required in addition to any requirement under Part 15.

Immunity from criminal responsibility for conduct that complies with a TAR, TAN, or TCN

4.44. Schedule 1 of TOLA amends the Criminal Code to provide that that, where certain conduct would otherwise be an offence, a person is not criminally responsible for that conduct if the person is acting in accordance with a TAR or in compliance with a TAN or TCN. It does so by exempting that conduct from the scope of the offence of operating any apparatus or device that hinders the normal operation of a carriage service;[94] and from the meaning of 'unauthorised access, modification or impairment' for the purpose of certain computer offences.[95]

---

[92] Ibid s 317ZG(5).

[93] Ibid ss 317ZGA, 317ZH.

[94] Being an offence under *Criminal Code Act 1995* (Cth) (Criminal Code), s 474.6(5), which provides:

> *(5) A person commits an offence if:*
> *(a) the person uses or operates any apparatus or device (whether or not it is comprised in, connected to or used in connection with a telecommunications network); and*
> *(b) this conduct results in hindering the normal operation of a carriage service supplied by a carriage service provider.*
> *Penalty: Imprisonment for 2 years.*

[95] See Criminal Code, Divisions 477 and 478, which create the following offences:

> ***Division 477 – Serious computer offences***
> *477.1 Unauthorised access, modification or impairment with intent to commit a serious offence*
> *477.2 Unauthorised modification of data to cause impairment*
> *477.3 Unauthorised impairment of electronic communication*
> ***Division 478 – Other computer offences***
> *478.1 Unauthorised access to, or modification of, restricted data*
> *478.2 Unauthorised impairment of data held on a computer disk etc.*

Compensation for conduct in compliance with the TAN or TCN

4.45. Normally, the acts or things a DCP does under a TAN or TCN are to be done on the basis that the DCP neither profits from nor bears the reasonable cost of complying with the notice.[96] There are various exceptions to this, including where the head of the interception agency or security agency (in the case of a TAN) or the Attorney-General (in the case of a TCN) is satisfied that it would be contrary to the public interest for the provision to apply.[97]

4.46. A DCP must comply with the requirement on such terms and conditions as it agrees with the applicable costs negotiator. The 'applicable costs negotiator' is the Director-General of Security, the head of the interception agency in question or the person specified in the TCN.[98] If the DCP and applicable costs negotiator cannot agree, the legislation provides for an arbitrator to be appointed.[99] If the DCP and the applicable costs negotiator cannot agree on the arbitrator, another nominated person (depending on the type of notice in question) is to appoint the arbitrator.[100] There are further conditions for the type of person who is eligible to be appointed an arbitrator.[101]

Schedule 2

Overview of Schedule 2

4.47. Schedule 2 deals with computer access warrants. It amends the ASIO Act and the TIA Act to expand ASIO's existing powers in respect of computer access warrants and related authorisations. It also grants Commonwealth, State and Territory law enforcement agencies the power to obtain computer access warrants, by way of amendment to the SD Act. Schedule 2 entered into force on 9 December 2018.[102]

478.3 Possession or control of data with intent to commit a computer offence
478.4 Producing, supplying or obtaining data with intent to commit a computer offence.

[96] Telecommunications Act, s 317ZK.

[97] Ibid s 317ZK(1).

[98] Ibid s 317ZK(16).

[99] Ibid s 317ZK(4).

[100] Ibid s 317ZK(4).

[101] Ibid s 317ZK(7).

[102] TOLA, s 2(1), items 4 and 5 of table entitled 'Commencement Information'.

Scope of powers prior to TOLA

4.48. ASIO has had the power to apply for computer access warrants since 1999.[103] Until the TOLA reforms, it was the only Australian security or law enforcement agency that had the power to do so. With the exception of Questioning Warrants and Questioning Detention Warrants, and urgent warrants issued by the Director-General, all intrusive warrants issued under the ASIO Act are issued by the Attorney-General rather than a judge or tribunal member acting as *persona designata*. The Attorney-General may issue a computer access warrant to ASIO at the request of the Director-General of Security, where there are reasonable grounds to believe that ASIO's access to data held in a target computer will substantially assist in collecting intelligence about a matter that is important to security.[104]

4.49. Where expressly authorised to do so, ASIO also has the power to execute the powers of a computer access warrant in connection with a foreign intelligence warrant[105] or an identified person warrant.[106] Accordingly, powers in respect of computer access are available to ASIO not only under a computer access warrant but also under these other types of warrant.

4.50. But before TOLA came into force, a computer access warrant (or similar) did not empower ASIO to intercept a communication passing over a telecommunications system operated by a carrier or carriage service provider. This is because that conduct amounted to 'telecommunications interception' under the TIA Act. Therefore, ASIO was required to obtain a TIA Act warrant *and* a computer access warrant, in each case satisfying a different statutory test, in order to lawfully intercept communications for the purposes of doing something under the latter warrant.

Amendments effected by TOLA

4.51. The main reforms effected by Schedule 2 are as follows:

a. The Attorney-General can issue a computer access warrant that authorises ASIO to intercept communications for the purpose of doing anything specified in the

---

[103] *Australian Security Intelligence Organisation Legislation Amendment Act 1999* (Cth), Schedule 1, which amended the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) to introduce the power. The power was subsequently amended by the *National Security Legislation Amendment Act (No 1) 2014* (Cth), Schedule 2.

[104] ASIO Act, s 25A.

[105] Ibid s 27A(1).

[106] Ibid s 27E(2).

warrant. This removes the need for ASIO to obtain a separate warrant under the TIA Act for the interception.

b. The Attorney-General can authorise ASIO, in a computer access warrant, to remove a computer or other thing from premises to do to the computer or thing anything specified in the warrant.

c. ASIO can remove a computer or thing from premises for the purpose of executing a computer access warrant.

d. ASIO can do anything reasonably necessary to conceal the fact that something has been done in relation to a computer under a computer access warrant or related authority.

e. Commonwealth, State and Territory law enforcement officers can obtain computer access warrants.

f. The Attorney-General can authorise a law enforcement officer to apply for a computer access warrant at the request of a foreign government.

g. A law enforcement officer can apply to an eligible judge or nominated AAT member for an assistance order that compels a person to provide certain assistance in respect of a computer that is the subject of a computer access warrant.

Expanding the scope of ASIO's powers in respect of computer access warrants

4.52. Schedule 2 of TOLA amends the ASIO Act to permit ASIO to intercept telecommunications under a computer access warrant.

4.53. First, it repeals a provision that had previously limited the scope of powers under a computer access warrant to exclude the interception of communications.[107]

4.54. Secondly, it introduces a provision that allows the Attorney-General to specify in a computer access warrant that the warrant authorises the interception of communications passing over a telecommunications system if the interception is for the purposes of doing anything lawfully specified in the warrant.[108]

4.55. The effect is that, while a computer access warrant does not automatically authorise the interception of communications for the purpose of doing something under the warrant, it is capable of doing so where the Attorney-General considers it

[107] Ibid s 33(1), as in force immediately prior to the reforms effected by Schedule 2 of TOLA.

[108] Ibid s 25A(4)(ba). This legislation also authorises interception for the purposes of exercising a concealment of access power: see ibid s 25A(8)(h), s 27A(3C)(h).

appropriate. In such cases, the Director-General of Security will no longer need to obtain a separate warrant under the TIA Act to lawfully intercept the communications in question.

4.56. A consequence of these amendments is that, in contrast to what ordinarily applies to a warrant for telecommunications interception, a different, lower, threshold now applies to the lawful interception of communications where that interception is for the purposes of doing something authorised under the computer access warrant. However, the higher protection accorded to intercepted product is reflected in TOLA's amendments to Part 2-6 of the TIA Act, which limit the use and disclosure of 'ASIO computer access intercept information'.[109]

Removing a computer or thing from warrant premises for the purpose of executing a computer access warrant

4.57. Under Schedule 2, when the Attorney-General issues a computer access warrant, he or she can specify that ASIO has the power to remove a computer (or other thing) from premises, so as to do to it anything specified in the warrant, and to later return it to the premises.[110] The same power exists where reasonably necessary to conceal what ASIO has done to a computer under a computer access warrant.[111] A thing taken from premises under any of these powers must be returned to the premises within a reasonable period or at a time when this would no longer be prejudicial to security.[112]

Concealing things done under a computer access warrant

4.58. Schedule 2's amendments to the ASIO Act also empower ASIO to do anything reasonably necessary to conceal the fact that something has been done in relation to a computer under a computer access warrant.[113]

4.59. ASIO's powers to conceal its steps under a computer access warrant or related authorisation are not absolute. ASIO does not have power to authorise anything that would interfere with *another person's* lawful use of a computer or cause that person material loss or damage.[114]

---

[109] *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), s 63AC.

[110] ASIO Act, ss 25A(4)(ac), 25A(8)(f), 27E(6)(f).

[111] Ibid ss 25A(4)(ac), 25A(8)(f), 27E(6)(f).

[112] Ibid ss 25A(4A), 25A(10), 27A(3E), 27E(3A), 27E(8).

[113] Ibid ss 25A(8)(c), 27A(3C)(c), 27E(6)(c).

[114] Ibid ss 25A(9), 27A(3D), 27E(7).

4.60. ASIO may take the steps to conceal its activities while the relevant warrant or authority is in force, within 28 days following its expiry or at the earliest time after that time that it is practicable to do so.[115]

Law enforcement agencies' powers to obtain computer access warrants

4.61. Previously, the SD Act had authorised the granting of surveillance device warrants (including, as a subset, tracking device authorisations) regarding:

a. criminal investigations
b. the location and safe recovery of children to whom recovery orders relate[116]
c. in certain cases where a control order is in force, counter-terrorism purposes.

4.62. Schedule 2 of TOLA amended the SD Act to grant law enforcement agencies the power to apply for computer access warrants.[117]

4.63. A computer access warrant grants a law enforcement agency access to a 'target computer'. This can include 'a particular computer', 'a computer on particular premises' or 'a computer associated with, used by or likely to be used by a person', whether or not that person's identity is known.[118] The TOLA reforms replaced the previous definition of 'computer' under the SD Act with the ASIO Act's broader definition, so that it now includes one or more 'computers', 'computer systems', 'computer networks' or any combination of these.[119]

4.64. An application for a computer access warrant is made by a 'law enforcement officer'. 'Law enforcement officer' is defined to include officers of both federal and State and Territory police forces, crime commissions, integrity commissions and, in contrast with Schedule 1, anti-corruption agencies.[120] Applications may be made by the law enforcement officer or by 'another person on the law enforcement officer's behalf'.[121]

---

[115] Ibid s 25A(8)(j) and (k).

[116] The *Surveillance Devices Act 2004* (Cth) (SD Act), s 6, defines 'recovery order' to mean:
(a) an order [a recovery order as defined in s 67Q] under section 67U of the Family Law Act 1975; or
(b) an order for a warrant for the apprehension or detention of a child under subregulation 15(1) or 25(4) of the Family Law (Child Abduction Convention) Regulations 1986.

[117] Ibid Part 2, Division 4.

[118] Ibid s 27A(15).

[119] Ibid s 6(1).

[120] Ibid s 6A.

[121] Ibid s 27A(1).

4.65. The grounds on which a law enforcement officer may apply for a computer access warrant include for:

a. investigations into relevant offences[122]

b. child recovery orders

c. international assistance investigations

d. integrity operations (but only in the case of federal law enforcement officers)

e. control orders.[123]

4.66. The application is made to an eligible judge or an AAT member.[124] The judge or member must be satisfied of various factors,[125] having regard to other factors,[126] before issuing the warrant. The judge or member must specify in the warrant what actions the warrant authorises.[127] These can be any of a list of specified actions that he or she considers appropriate in the circumstances.[128] Those actions include:

a. entering premises

b. using the target computer or other equipment or devices to access relevant data held on the target computer

c. in certain circumstances, adding, copying, deleting or altering data on the target computer

---

[122] 'Relevant offence' means:

(a) an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of 3 years or more or for life; or
(b) an offence against a law of a State that has a federal aspect and that is punishable by a maximum term of imprisonment of 3 years or more or for life; or …
(db) if a surveillance device warrant, a computer access warrant, or a tracking device authorisation, is issued or given (or is sought) for the purposes of an integrity operation in relation to a suspected offence against the law of the Commonwealth, or of a State or Territory, that is punishable by a maximum term of imprisonment of 12 months or more or for life—that offence; or …

[123] SD Act, s 27A(1), (3), (4), (5), (6).

[124] Ibid s 27A(7).

[125] Ibid s 27C(1).

[126] Ibid s 27C(2), including:

(c) the extent to which the privacy of any person is likely to be affected; and
(d) the existence of any alternative means of obtaining the evidence or information sought to be obtained.

[127] Ibid s 27E(1).

[128] Ibid s 27E(2).

d. intercepting a communication for the purposes of doing anything specified in the warrant.

4.67. The amendments also include the power to obtain computer access by way of emergency authorisation or other order where there is not sufficient time to obtain a warrant.[129]

4.68. The computer access warrant regime established for law enforcement officers under the SD Act contains provisions equivalent to those noted above for ASIO computer access warrants and related authorisations. These include, for instance, the power to remove a computer or other things from warrant premises for processing;[130] to add, copy or delete data;[131] to intercept a communication passing over a telecommunications system for limited purposes;[132] and to take steps to conceal things done under a computer access warrant.[133]

Obtaining a computer access warrant at the request of a foreign country

4.69. Schedule 2 of TOLA also amends the *Mutual Assistance in Criminal Matters Act 1987* (Cth) to permit applications for computer access warrants at the request of a foreign country. The amendments to that Act provide that the Attorney-General may, at his or her discretion, authorise an eligible law enforcement officer to make an application under the SD Act[134] for a computer access warrant.

4.70. The Attorney-General may do so where satisfied that:

a. there is an investigation underway in the requesting country into an offence under the law of the foreign country punishable by a maximum penalty of imprisonment for 3 years or more, life imprisonment or the death penalty

b. the requesting country has requested access to data held in a computer

c. the requesting country has given prescribed undertakings as to the use of any data obtained from that access and any other matter the Attorney-General considers appropriate.[135]

---

[129] Ibid s 35A(4) or (5).

[130] Ibid s 27E(2)(f).

[131] Ibid s 27E(2)(d).

[132] Ibid s 27E(2)(h).

[133] Ibid s 27E(7).

[134] Ibid s 27A(1).

[135] *Mutual Assistance in Criminal Matters Act 1987* (Cth), s 15CC(1).

Obtaining an assistance order in respect of a computer the subject of a computer access warrant

4.71. Schedule 2 of TOLA also introduces a new assistance order power in respect of computer access warrants.[136] In broad terms, this assistance order permits a law enforcement officer (or person acting on his or her behalf) to request of a person such assistance as the law enforcement officer considers reasonable or necessary to access, copy or convert data held in a computer the subject of a computer access warrant or related authorisation.

4.72. An order is only available where the eligible judge or AAT member to whom the application is made is satisfied of prescribed criteria. These criteria broadly include that there are reasonable grounds to suspect that accessing that information will assist, or substantially assist, the investigation in question.[137] Failure to comply with an order exposes a person to a maximum penalty of 10 years imprisonment or 600 penalty units or both.[138]

4.73. This power resembles other assistance order powers that predate TOLA, including in connection with the execution of a search warrant in respect of premises.[139]

Schedule 3

Overview of Schedule 3

4.74. Schedule 3 amends the warrant powers in Part IAA of the *Crimes Act 1914* (Cth) – in particular, in respect of data held in or accessible from electronic devices. Schedule 3 does not amend any other parts of the Crimes Act or any other legislation.

4.75. In general terms, the powers in Part IAA of the Crimes Act may be exercised by an 'executing officer' or a 'constable assisting' (together, a constable executing a warrant).[140] Each of those terms refers to a 'constable', who participates in the execution of a warrant and (in the case of an executing officer) has particular

---

[136] SD Act, s 64A.

[137] The precise terms of the test depend on the type of warrant, authorisation or order to which it relates: see ibid ss 64A(2)(c), 64A(3)(c), 64A(4)(a), 64A(5)(a), 64A(6)(a), 64A(7)(a).

[138] Ibid s 64A(8).

[139] See *Crimes Act 1914* (Cth), s 3LA, and *Customs Act 1901* (Cth), s 201A, each of which predates TOLA but which were amended by Schedules 3 and 4 of TOLA respectively; and the new power in s 34AAA of the ASIO Act, which was introduced by Schedule 5 of TOLA. I discuss each of these powers in my analysis of those respective schedules.

[140] In each case, as defined in the Crimes Act, s 3C.

responsibilities in relation to the warrant. The term 'constable' includes a member or special member of the AFP and a member of a State or Territory police force.[141] Schedule 3 entered into force on 9 December 2018.[142]

Scope of powers prior to TOLA

4.76. Warrants issued under Part IAA of the Crimes Act include various powers to examine, process, copy, move and seize electronic data. Before summarising how TOLA has amended those powers, it is useful to set out, in broad terms, the scope of existing police powers in relation to electronic devices and accessing electronic data.

4.77. In broad terms, both warrants in respect of premises[143] and warrants in respect of a person[144] permit police officers to search for and seize 'evidential material'.[145] The definition of 'evidential material'[146] expressly includes things 'in electronic form'. Any police power exercisable in respect of 'evidential material' accordingly applies to any electronic item falling within the meaning of that term on the facts of a given matter.

4.78. Even prior to TOLA, a constable executing a warrant had the power to operate electronic equipment at warrant premises to access data that he or she reasonably believed was evidential material.[147] Also, a constable executing a warrant could take onto warrant premises electronic equipment that enabled the 'examination or processing of a thing' to determine whether it might be seized under the warrant;[148] and to move a thing found at warrant premises 'to another place for examination or processing' in certain circumstances.[149]

4.79. The power to operate electronic equipment taken to, or moved from, warrant premises to access data already expressly includes the power to access 'data not held at (warrant) premises',[150] and in the case of a warrant in respect of a person,

---

[141] Every 'executing officer' or 'constable assisting', as defined in the Crimes Act, s 3C, is a 'constable', which is itself defined in s 3 of the Crimes Act as set out above.

[142] TOLA, s 2(1), item 6 of table entitled 'Commencement Information'.

[143] Crimes Act, s 3C(1).

[144] Ibid s 3C(2).

[145] Ibid s 3F(1)(c), in respect of a warrant in force in relation to premises.

[146] Ibid s 3C(1).

[147] Ibid s 3L.

[148] Ibid s 3K(1).

[149] Ibid s 3K(2).

[150] Ibid s 3L(1).

data held at *any* premises.[151] This empowers constables executing a warrant to access electronic data stored offsite and even offshore – for instance, in 'cloud' storage. While the executing officer is obliged to notify the 'occupier' of the other premises where that data is held when accessing the data, they are only obliged to do that where it is 'practicable' to do so.[152]

4.80. Another power that predates TOLA is the power to compel a person to provide information that enables access to electronic data. This includes, for instance, providing a password for a phone or laptop computer. Section 3LA of the Crimes Act permits a constable to apply to a magistrate for an order compelling a person to provide 'any information that is reasonable and necessary' to access, copy or convert into electronic form data held in a computer or data storage device (an assistance order),[153] provided that the computer or data storage device is sufficiently connected with a warrant, and the person in respect of whom the order is made falls within a particular category.[154] The power does not automatically follow from the issue of a warrant. Rather, it is available only on application to, and by order of, a magistrate.[155]

Amendments effected by TOLA

4.81. Schedule 3 of TOLA expands the scope of powers that may be exercised in relation to electronic devices, and data held on or accessible from electronic devices, in connection with the execution of a warrant. The main reforms effected by Schedule 3 are as follows:

a. It introduces the concept of 'account-based data'.
b. It expands the scope of actions police can take to access electronic data.
c. It permits remote access to data from a place other than warrant premises.
d. It increases the time during which an electronic device moved from warrant premises under s 3K may be retained for processing or examination.
e. It amends both the circumstances in which an assistance order is available and the penalties for failing to comply with that order.

4.82. The TOLA amendments apply only to 'overt' search warrants – warrants in respect of which an occupier is notified at the time of execution of the warrant – and not to

[151] Ibid s 3LAA(1), as in force prior to 9 December 2018.

[152] Ibid s 3LB(1)(c).

[153] Ibid s 3LA, as in force at all relevant times.

[154] Ibid s 3LA.

[155] Ibid s 3LA(1).

delayed notification search warrants, which are dealt with separately in the Crimes Act.[156]

Account-based data

4.83. TOLA introduced the concept of 'account-based data' in relation to the execution of warrants. That term is expressly defined.[157] In essence, 'account-based data' is data accessible through an account held or used by a person, including (in the case of a deceased person) an account formerly held or used by that person.[158] It is not necessary for police to establish the person *has* used the account; it is enough that the person is or was 'likely to be' a user of the account. Also, it is not necessary that the person be the *only* user of the account; it is enough that the person is '*a* user' of the account.

4.84. The term 'account-based data' is distinguished from data more broadly, although police have broadly equivalent powers in respect of both account-based data and other data.

4.85. TOLA has expanded the scope of actions that a constable may take in respect of data, including both 'account-based data'[159] and data more broadly.[160] The new powers include:

a. powers 'to add, copy, delete or alter other data' in a computer or device for the purpose of obtaining access to data to determine whether it is 'evidential material'[161]
b. the power to use other computers or communications in transit to access the data, if 'it is reasonable in all the circumstances to do so', and 'to add, copy, delete or alter' other data in that computer or communication in transit[162]
c. the power to do anything 'reasonably incidental to' the above.[163]

4.86. Those powers are subject to the limitation set out in s 3F(2C) of the Crimes Act. That is, they do not authorise police to do anything likely to interfere with lawful use of a computer or communications beyond what is necessary to do the things specified

[156] As contained in Crimes Act, Part IAAA.

[157] TOLA, Schedule 3, item 1, amending the Crimes Act, s 3C(1).

[158] Crimes Act, s 3CAA.

[159] Ibid s 3F(2B).

[160] Ibid s 3F(2A).

[161] Ibid s 3F(2A)(a), (b); s 3F(2B)(a), (b).

[162] Ibid ss 3F(2A)(c), 3F(2B)(c).

[163] Ibid ss 3F(2A)(e), 3F(2B)(e).

in the warrant.[164] Also, they do not authorise police to do anything that would cause material loss or damage to some other person lawfully using the computer.[165]

Permitting remote access to data

4.87. Prior to the reforms enacted by TOLA, a police officer could only access data held at some place other than warrant premises if he or she were accessing that data from warrant premises.[166] The TOLA amendments now permit police officers to exercise the extended powers in the Crimes Act, s 3F(2A) and (2B), at warrant premises or 'at any other place'[167] and at any time while the warrant is in force.[168] In the case of a warrant in force in respect of a person, the powers can be exercised either in the person's presence or 'at any other place'.[169]

Increasing the time during which an electronic device may be retained

4.88. As noted above, s 3K(2) permits an electronic device to be moved from warrant premises 'for examination or processing'. TOLA:

a. increased the time that a computer or data storage device can be retained from 14 days to 30 days[170]
b. increased the period by which that time can be extended, by order of an issuing officer, from 7 days to 14 days.[171]

Assistance orders

4.89. As noted above, prior to TOLA, the Crimes Act empowered a constable to apply for, and a magistrate to issue, an 'assistance order' compelling a person with a particular connection to the device in question to provide 'any information or assistance that is reasonable and necessary' to access, copy or convert into electronic form data held in a computer or data storage device.[172] Following TOLA, that power continues to exist, with 3 main amendments to the way it operates.

4.90. *First*, TOLA has expanded the circumstances in which it is possible to obtain an assistance order. It is now possible to obtain an order for a person to give assistance

---

[164] Ibid s 3F(2C)(a).

[165] Ibid s 3F(2C)(b).

[166] Pursuant to the Crimes Act, s 3L.

[167] Crimes Act, s 3F(2D).

[168] Ibid s 3F(2A)(a).

[169] Ibid s 3F(2E).

[170] Ibid s 3F(3A).

[171] Ibid s 3F(3D).

[172] Ibid s 3LA, as in force at all relevant times.

in respect of an item found during an ordinary search or frisk search conducted under a warrant issued under s 3E. This applies not only to a search of a person conducted by authority of a person warrant;[173] it also applies to a warrant in respect of premises where its terms include a power to conduct an ordinary search or a frisk search of a person.[174]

4.91. *Secondly*, the Crimes Act now specifies with greater particularity the circumstances in which a person is liable for an offence of failing to comply with an assistance order. While s 3LA(5) had previously provided that 'a person commits an offence if the person fails to comply with the order', that sub-section is now more prescriptive. In particular, it now focuses attention on the particular requirements an assistance order imposes. A prosecutor will now be required to prove that the person was 'capable of complying with a requirement in the order' – not previously an element of the offence – that he or she omitted to do an act and that that omission contravenes the requirement.[175]

4.92. *Thirdly*, the TOLA reforms expanded and increased the maximum penalties for a failure to comply with an assistance order. The maximum penalty was previously limited to imprisonment for a maximum period of 2 years. The maximum penalty is now 5 years' imprisonment or 300 penalty units in an ordinary case, or 10 years' imprisonment or 600 penalty units where the offence to which the warrant in question relates is 'a serious offence' or 'a serious terrorism offence'. Each of those terms is defined in the Crimes Act.[176]

Schedule 4

Overview of Schedule 4

4.93. Schedule 4 amends certain investigative powers of Australian Border Force (ABF) officers in respect of electronic devices. It does so by way of amendments to the *Customs Act 1901* (Cth) – in particular, to Part XII, Subdivision C, of that Act.

4.94. In general terms, the warrant powers in that subdivision may be exercised by an 'executing officer'.[177] In the case of Schedule 4 powers, that means an officer of the ABF. The amendments effected by Schedule 4 broadly increase the powers available to an executing officer, or person assisting him or her, in relation to computers, data

[173] Ibid s 3E(2); s 3F(2)(a).

[174] Ibid s 3F(1)(f).

[175] Ibid s 3LA(5).

[176] Ibid s 3C.

[177] As defined in s 183UA(1) of the Customs Act to mean, insofar as relevant to the reforms effected by Schedule 4 of TOLA, an officer of the ABF.

storage devices, other electronic items and access to data. Schedule 4 entered into force on 9 December 2018.[178]

Scope of powers prior to TOLA

4.95. Prior to the TOLA reforms, ABF officers had power to obtain a search warrant in respect of 'premises' but not in respect of a 'person'. This contrasted with the position of AFP officers, who could apply for either category of search warrant.

4.96. An ABF officer executing a search warrant in respect of premises had limited powers in respect of the access to data accessible from the warrant premises. Further, where an item was moved from warrant premises for examination or processing, the ABF was permitted to retain the item for only 72 hours.

4.97. In addition, prior to TOLA, the ABF had the power to obtain an assistance order to compel a person to provide such assistance as is reasonable or necessary to permit access and other steps in relation to electronic data. However, if a person did not comply with that order, the maximum penalty was 6 months' imprisonment.

Amendments effected by TOLA

4.98. The main reforms effected by Schedule 4 are as follows:

a. It introduced a power for ABF officers to obtain a search warrant in respect of a person.
b. It expanded the ABF's powers in respect of electronic items and access to data in connection with the execution of a search warrant in respect of premises.
c. It increased the time during which a computer or data storage device moved from warrant premises by the ABF for examination or processing may be retained for that purpose.
d. It amended offence provisions and maximum penalties that apply where a person fails to comply with an assistance order.

Search warrants in respect of a 'person'

4.99. The TOLA amendments give ABF officers, for the first time, the power to obtain a warrant to conduct an ordinary search or a frisk search in respect of a person (a person warrant). A person warrant is available where there are reasonable grounds to suspect a person has in his or her possession (or will have within the following 72 hours) 'any computer, or data storage device, that is evidential material'.[179]

[178] TOLA, s 2(1), item 6 of table entitled 'Commencement Information'.

[179] Customs Act, s 199A(1).

4.100. An ABF officer has various powers under a person warrant.[180] In addition to more general powers to search the person, seize computers and data storage devices, record fingerprints and take forensic samples,[181] a person warrant contains specific powers in respect of electronic equipment.[182]

Expansion of ABF's powers in respect of electronic items and access to data

4.101. The amendments effected by Schedule 4 of TOLA expand the ABF's warrant powers in respect of electronic items and access to data, including search warrants in respect of premises and person warrants.[183] These new powers are broadly equivalent to those accorded to the AFP in respect of Crimes Act warrants in the amendments effected by Schedule 3 of TOLA.[184] However, unlike Crimes Act search warrants, Customs Act search warrants as amended by Schedule 4 of TOLA do not include any power to access account-based data.

4.102. As in the case of Crimes Act search warrants, Customs Act search warrants are limited in that these additional powers do not authorise an ABF officer to do anything likely to interfere with lawful use of a computer or communications beyond what is necessary to do the things specified in the warrant.[185] Also, they do not authorise police to do anything that would cause material loss or damage to some other person lawfully using the computer.[186]

The time during which an ABF officer can retain an electronic item moved from warrant premises

4.103. As noted above, prior to TOLA, ABF officers had the power to move an electronic item found in the execution of a search warrant from warrant premises to another place for examination or processing. TOLA:

a. increased the time that a computer or data storage device moved under that power can be retained from 72 hours to 30 days[187]
b. provided that the period by which that time can be extended, by order of a judicial officer, is on each occasion 14 days.[188]

---

[180] Ibid s 199B.

[181] Ibid s 199B(1).

[182] Ibid s 199B(2).

[183] Ibid ss 199(4A), 199B(2).

[184] As set out in the summary of Schedule 3.

[185] Customs Act, ss 199(4B)(a), 199B(3)(a).

[186] Ibid ss 199(4B)(b), 199B(3)(b).

[187] Ibid s 200(3A).

[188] Ibid s 200(3B), (3D).

Assistance orders

4.104. As noted above, prior to TOLA, the Customs Act empowered an ABF officer to apply to a magistrate for an 'assistance order' compelling a person with a particular connection to a computer to provide 'any information or assistance that is reasonable and necessary' to access, copy or convert into electronic form data held in a computer or data storage device.[189] Following TOLA, that power continues to exist, subject to some amendments.

4.105. *First*, TOLA expanded the scope of assistance orders under the Customs Act so that they are now available in respect of not only 'computers' but also 'data storage devices'.

4.106. *Secondly*, as is the case with reforms to the equivalent provision of the Crimes Act, the Customs Act now specifies in more detail the circumstances in which a person is liable for an offence of failing to comply with an assistance order. While s 201A previously provided that 'a person commits an offence if the person fails to comply with the order', the prosecution is now required to prove that the person the subject of the order was 'capable of complying with a requirement in the order', which was not previously an element of the offence; that he or she omitted to do an act; and that the omission contravenes the requirement.[190]

4.107. *Thirdly*, the reforms have significantly increased the penalty for failing to comply with an assistance order. The penalty for failing to comply with an order is now 5 years' imprisonment or 300 penalty units in the ordinary case, whereas previously it was 6 months' imprisonment. Further, where the warrant in question relates to a 'serious offence', the maximum penalty for failing to comply with an assistance order is now 10 years' imprisonment or 600 penalty units.

Schedule 5

Overview of Schedule 5

4.108. Schedule 5 deals the provision of assistance to ASIO, either voluntarily or under compulsion. The Schedule 5 amendments protect against civil liability those who assist ASIO by engaging in certain conduct, either at the request of the Director-General of Security or by voluntary disclosure. Further, it empowers the Director-General of Security to request the assistance. Schedule 5 entered into force on 9 December 2018.[191]

---

[189] For the pre-TOLA form, see s 201A as at 1 September 2018.

[190] Customs Act, s 201A(3), (4).

[191] TOLA, s 2(1), item 6 of table entitled 'Commencement Information'.

Scope of powers prior to TOLA

4.109. Prior to the TOLA amendments, the ASIO Act empowered the Attorney-General to confer on a person protection from civil or criminal liability where the person was engaged in authorised 'special intelligence conduct'.[192] However, ASIO did not have any more general power to confer immunity from civil liability on a person assisting ASIO in any other capacity or for any other purpose.

4.110. Further, until the reforms effected by TOLA, ASIO did not have a power to compel a person to provide assistance in relation to a computer to which it has obtained access in connection with a warrant. Both AFP officers[193] and ABF officers[194] had those powers, but ASIO officers had no equivalent.

Amendments effected by TOLA

4.111. Schedule 5 of TOLA:

a. confers protection against civil liability on any person who provides voluntary assistance by 'conduct' at the request of the Director-General of Security, or makes an unsolicited disclosure of certain information to ASIO[195]
b. provides a mechanism by which ASIO can compel a person to assist it in relation to a computer to which ASIO has already obtained access in connection with a warrant.[196]

Immunity from civil liability for those the Director-General requests to engage in conduct

4.112. TOLA amends the ASIO Act by introducing s 21A. That section provides that, where the Director-General requests a person or a body 'to engage in conduct' which he or she 'is satisfied, on reasonable grounds … is likely to assist the Organisation in the performance of its functions', the person or body will be immune from civil liability for the conduct. 'Conduct' is not defined.

4.113. Those requests must ordinarily be made in writing.[197] It is open to the Director-General to enter into a contract, agreement or arrangement with the person or body in question in relation to the conduct the subject of the request.[198]

---

[192] ASIO Act, s 35K.

[193] Crimes Act, s 3LA.

[194] Customs Act, s 201A.

[195] ASIO Act, s 21A(1), (5).

[196] Ibid s 34AAA.

[197] Ibid s 21A(2), (2A), (3).

[198] Ibid s 21A(4).

4.114. The immunity that s 21A confers on a person is not absolute. It only applies to conduct which the person engages in 'in accordance with the request' of the Director-General.[199] Further, no protection against liability applies to conduct that involves an offence against Commonwealth, State or Territory law.[200] Also, it does not apply to conduct that results in significant loss of or damage to property.[201]

4.115. The Director-General is obliged to report to IGIS the fact of a s 21A request within 7 days of making the request.[202]

Protection against liability for unsolicited disclosure of information

4.116. Section 21A(5) also provides protection against civil liability for a person who engages in voluntary conduct that the person or body reasonably believes is likely to assist ASIO 'in the performance of its functions'.[203] The conduct that falls within the scope of that provision is narrower than what may be requested under s 21A(1) – namely, giving information to ASIO, giving or producing to ASIO a document, or copying and giving to ASIO a document.[204] By s 2B of the *Acts Interpretation Act 1901* (Cth):

> ***document*** *means any record of information, and includes (a) anything on which there is writing; and (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; and (d) a map, plan, drawing or photograph.*

4.117. As in the case of conduct at the request of the Director-General, the section provides no protection against liability where the conduct involves a person committing an offence against a Commonwealth, State or Territory law,[205] or which results in significant loss of or damage to property.[206]

Order to provide information and assistance

4.118. TOLA also introduces s 34AAA to the ASIO Act. That section provides that the Director-General may request the Attorney-General to make an order that a

---

[199] Ibid s 21A(1)(c).

[200] Ibid s 21A(1)(d).

[201] Ibid s 21A(1)(e).

[202] Ibid s 21A(3A).

[203] Ibid s 21A(5).

[204] Ibid s 21A(5).

[205] Ibid s 21A(5)(c).

[206] Ibid s 21A(5)(d).

specified person 'provide any information or assistance that is reasonable and necessary' to allow ASIO to do certain things. Those things include accessing data held in or accessible from a computer or data storage device, copying data held in or accessible from the computer or device, or converting such information into documentary form.

4.119. The computer or data storage device the subject of an order must have a prescribed connection to a warrant. For instance, the computer or storage device must be the subject of a warrant, or on warrant premises, or be removed or seized under warrant, or found in the course of a search of a person authorised by warrant. The effect of this is that s 34AAA is only available in respect of a computer or device that is already lawfully available to ASIO.

4.120. The Attorney-General may make an order under s 34AAA where satisfied of various things, including the purpose and importance of obtaining the data; that the person the subject of the order has a sufficient connection with the computer or device (or, if not, that he or she is suspected of 'being involved in activities that are prejudicial to security'); and that the person has the knowledge to comply with the order.

4.121. It is an offence for a person subject to an order under s 34AAA who is capable of complying with a requirement of the order to fail to do so. The offence is punishable by imprisonment for 5 years or 300 penalty units.[207]

Meeting with the UK Investigatory Powers Commissioner and Chair of the Technical Advisory Panel, London, November 2019. Left to right: Dr James Renwick CSC SC, INSLM; Rt Hon Sir Brian Leveson, Investigatory Powers Commissioner; and Sir Bernard Silverman FRS FAcSS, Chair of the Technical Advisory Panel

[207] Ibid s 34AAA(4).

5. CONTEXT: TECHNOLOGY – DEFINITIONS AND CHALLENGES

5.1. It is both true and deceptively simplistic to say that a fundamental reason for the enactment of TOLA was the ubiquitous use of encryption. In fact, there are many technical developments and policy factors at play. As Sir David Omand notes:

> *Civil liberties organizations report increasing ethical concerns by individuals for their right to privacy and for the protection of their personal information from hackers, from carelessness on the part of corporations, from unrestrained government surveillance, from new techniques such as predictive analytics, and from the very business model of the Internet that rests on the monetization of personal data. As a result demand is increasing for end-to-end encryption, for anonymization software, for secure apps and mobile devices, and for stronger data protection law and stronger enforcement of it.*[208]

5.2. The purpose of this chapter is to define some key terms, to place the debate in its proper technological context and to state some key challenges. I acknowledge with gratitude the support of my technical adviser in writing this chapter.

5.3. Day-to-day communication in Australia relies almost wholly on technology that is complex and constantly evolving. Australians have been among the fastest adopters of new communication technologies in the world. We have become almost entirely dependent on these technologies for everyday activities: business operations, financial transactions, economic development, social interactions and public engagement.

5.4. Indeed, new and emerging technologies have been at the forefront of burgeoning industries, and enabled the growth and vitality of others, in Australia and around the world. It is believed that in future technologies will be developed that have business, private, military and intelligence applications – for example, neuromorphic hardware, artificial general intelligence, fully autonomous vehicles and robots, and nanotube electronics.

5.5. The frequently amended *Telecommunications Act 1997* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) contain fundamental protections of Australians' privacy and confidentiality of communications and communications services. But communications between

[208] Sir David Omand and Mark Phythian, *Principled Spying: The Ethics of Secret Intelligence*, (Georgetown University Press, 2018) 145.

individuals, governments and organisations rely on technology that is complex and constantly evolving. Therefore, to answer the questions raised on this review – proportionality, necessity and safeguards – I must consider aspects of the technological context in which TOLA and related acts are to operate.

A changing communications environment

5.6. Rapid technological change over recent decades has dramatically changed how we are communicating. This change has increased not only the variety of communication methods but also the number of devices, the volume of information communicated and the pace of adoption of new technologies. I now consider some of the key trends:

a. increased mobility

b. increased number and variety of connected devices

c. digitisation and growth of data networks

d. different modes of communication.

Increased mobility

5.7. Traditional voice calls using landlines were for a long time made on the analogue Public Switched Telephone Networks (PSTN). Voice calls relied on a device – the telephone – connected by a wire to a physical socket in the user's premises.

5.8. The first mobile or cellular networks came in the 1980s. However, it was not until the 1990s and the introduction of digital Global System for Mobile Communications (GSM) networks that mobile phones became widely used.

5.9. Approximately every 10 years a new generation of mobile networks is developed. In 2020 the change from 4th generation (4G) to 5th generation (5G) networks is occurring. The latest data from the Australian Communications and Media Authority (ACMA)[209] shows more than half of Australian adults do not have a fixed phone line connected at home and rely instead on mobile devices. That trend is likely to continue.

Increased number and variety of connected devices

5.10. The traditional telephone is no longer the only or even the main device used for telecommunications. We use a wide variety of devices to communicate, including

[209] ACMA <https://www.acma.gov.au/sites/default/files/2020-04/Communications%20report%202018-19.pdf>

mobile phones, tablets, computers, smart watches and more. Data from Deloitte[210] shows that in the US there is an average of 11 connected devices per household. This number is forecast to increase in coming years.

5.11. One of the changes that the latest 5G mobile networks will allow is many more devices connected in a small area. This will enable the Internet of Things (IoT), in which many more devices, like fridges, electricity meters and doorbells, will be connected to the internet and therefore to telecommunications networks, communicating with their owners' mobile phones. IoT will also allow for M2M communications. M2M connections will allow for 'smart cities', where bins, traffic lights, street lights and so on are connected to the internet. Also, there will be industrial applications: sensors and manufacturing systems will also be connected.

What do our mobile phones say about us?

5.12. Like others,[211] I find it useful to approach these policy issues by reference to the personal mobile phone, which effectively everyone now uses. Many in Australia use mobile phones (which are, really, very powerful computer devices) not only for calling but also for email, web searches and purchases, banking, taking and storing photos, dating and use of a large range of 'apps'. We rarely put them down or stop using them.

5.13. Yet very few fully know what the information on our mobile phones says about us. In fact, they are the paradigm example of monetisation of our personal data, usually with our technical consent but rarely, if ever, with our informed consent.

5.14. A recent article by John Naughton[212] makes the point in a way which is worth setting out at some length:

> *Suppose you walk into a shop and the guard at the entrance records your name. Cameras on the ceiling track your every step in the store, log which items you looked at and which ones you ignored. After a while you notice*

---

[210] Kevin Westcott, Jeff Loucks, Dan Littman et al, 'Build It and They Will Embrace It: Consumers are Preparing for 5G Connectivity in the Home and On the Go', *Deloitte Insights* (Deloitte Center for Technology, Media & Telecommunications, UK, 2019) <https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html>.

[211] Encryption Working Group, 'Key Takeaways from the Encryption Working Group's Paper on "Moving the Encryption Policy Conversation Forward" (Carnegie Endowment for International Peace and Princeton University, 10 September 2019) <https://carnegieendowment.org/programs/technology/cyber/encryption>.

[212] Senior research fellow at the Centre for Research in the Arts, Social Sciences and Humanities, University of Cambridge, and author of *From Gutenberg to Zuckerberg: What You Really Need to Know About the Internet* (Quercus, UK, 2012).

that an employee is following you around, recording on a clipboard how much time you spend in each aisle. And after you've chosen an item and bring it to the cashier, she won't complete the transaction until you reveal your identity, even if you're paying cash.

Another scenario: a stranger is standing at the garden gate outside your house. You don't know him or why he's there. He could be a plain-clothes police officer, but there's no way of knowing. He's there 24/7 and behaves like a real busybody. He stops everybody who visits you and checks their identity. This includes taking their mobile phone and copying all its data on to a device he carries. He does the same for family members as they come and go.

When the postman arrives, this stranger insists on opening your mail, or at any rate on noting down the names and addresses of your correspondents. He logs when you get up, how long it takes you to get dressed, when you have meals, when you leave for work and arrive at the office, when you get home and when you go to bed, as well as what you read. He is able to record all of your phone calls, texts, emails and the phone numbers of those with whom you exchange WhatsApp messages. And when you ask him what he thinks he's doing, he just stares at you. If pressed, he says that if you have nothing to hide then you have nothing to fear. If really pressed, he may say that everything he does is for the protection of everyone.

A third scenario: you're walking down the street when you're accosted by a cheery, friendly guy. He runs a free photo-framing service – you just let him copy the images on your smartphone and he will tidy them up, frame them beautifully and put them into a gallery so that your friends and family can always see and admire them. And all for nothing! All you have to do is to agree to a simple contract. It's 40 pages but it's just typical legal boilerplate – the stuff that turns lawyers on. You can have a copy if you want.

You make a quick scan of the contract. It says that of course, you own your photographs but that, in exchange for the wonderful free framing service, you grant the chap 'a non-exclusive, transferable, sub-licensable, royalty-free and worldwide licence to host, use, distribute, modify, copy, publicly perform or display, translate and create derivative works' of your photos. Oh, and also he can change, suspend, or discontinue the framing service at any time without notice, and may amend any of the agreement's terms at his sole discretion by posting the revised terms on his website. Your continued use of the framing service after the effective date of the revised agreement constitutes your acceptance of its terms. And because you're in a hurry and you need some pictures framed by this afternoon for your daughter's birthday party, you sign on the dotted line.

> *All of these scenarios are inconceivable in what we call real life. It doesn't take a nanosecond's reflection to conclude that if you found yourself in one of them, you would deem it preposterous and intolerable. And yet they are all simple, if laboured, articulations of everyday occurrences in cyberspace. They describe accommodations that in real life would be totally unacceptable, but which in our digital lives we tolerate meekly and often without reflection.*[213]

5.15. All of that information – entirely new in its size, scope and type – is now available to Government and its agencies if there is a law permitting access. It would be surprising if they did not seek laws permitting them to use it to the full, hence the importance of the fundamental and companion principles in this review, set out in the executive summary.

Digitisation and growth of data networks

5.16. Since the 1990s most telecommunications have moved from analogue systems to digital systems in which everything is represented by 0s and 1s. While the practical difference is buried in the technical details of how electrical devices work at a fundamental level, the main change for users is that they can now send data as well as voice traffic. Almost all networks today use the Internet Protocol (IP) to send data between users. When users are making voice calls, the sound of their voices is converted into data – that is, digitised – and sent over IP networks using a technique called Voice over Internet Protocol (VoIP). The volume of data is growing exponentially – ACMA data shows an increase of over 400% from 2015 to 2019.

Different modes of communication

5.17. Traditional voice calls between 2 parties talking in real time have been supplemented and in many cases replaced by other modes of communication – text, pictures and video.

5.18. Communication is often asynchronous – one person sends an email to someone who is not even online at the time, and the recipient picks it up and reads it later.

5.19. People also communicate indirectly and in groups – for example, using Facebook posts and WhatsApp groups. So it is not just a case where Person A communicates directly with Person B; a group of people communicate directly and indirectly with each other.

---

[213] John Naughton, 'Why We Click "Accept" Without Reading the Terms', *Australian Financial Review*, 6 March 2020.

A complex web of communications infrastructure and service providers

5.20. In order to provide the variety of communications services and features that are now available, there is a complex combination of physical equipment, software and services 'running on top'. Until the 1980s, all of these services were typically provided by a single integrated company – Telecom Australia issued a single bill and it owned everything needed to connect us to any of their other customers, including even the home phone. Today ownership of this infrastructure has fragmented.

5.21. Conceptually, the telecommunications systems can be divided into network infrastructure, network services and application services.[214]

Network infrastructure

5.22. The most obvious piece of infrastructure that we interact with daily is the end user device – typically a mobile phone.

5.23. That device needs to connect to something. The first thing might be something else the user owns (for example, their home wireless router or a cable in the car), but at some point in the chain it will connect to an access network. This might be a fixed access network, such as the NBN home connection, or a radio access network, such as a connection to a mobile phone mast and base station operated by Telstra, Optus or Vodafone.

5.24. From there, depending on what there is communication with and where, the information can travel across a wide range of network infrastructure. Thus:

a. International PSTN voice calls were first interconnected to the world via satellite, then later via undersea cables connected between continents.

b. The modern internet and high-speed networks still use a mixture of cabled connections (these can be electrical signals on a copper cable, but today they are more often light signals on a fibre optic cable) and radio connections (satellites, microwave links and others).

c. Cabled connections tend to be more reliable. In particular, light-based data networks have the advantage of being able to carry very large amounts of information and many voice, video and data services simultaneously.

d. Radio connections are easier and cheaper to set up, but they suffer from more interference – for example, from other radio connections, storms and other

[214] This is a simplified version – technical experts actually talk of 7 layers.

atmospheric conditions. They are also more limited in the volume of data they can reliably carry.

5.25. As noted, when data is communicated it often does not go directly across the network from the sender to the recipient. Instead, it first goes to a computer server. These are normally located in the vast global infrastructure known as data centres – large, dedicated facilities with good power supplies; lots of cables connecting them to the outside world; and 'business continuity' features, including good fire and flood protection, to keep them up and running.

5.26. But the servers are not always owned by the same company that runs the software on them. They may be rented as needed as cloud computing services from providers such as Amazon or Microsoft.

5.27. The complexity of how data and information flows from A to B is generally hidden from users, but today data is often fragmented across different equipment owned by different providers and often in different countries. The proliferation of new methods of communication and the number of devices has resulted in huge increases in the amount of data travelling across global infrastructure, unconstrained by national borders. While many countries have sought to impose regulations on where data is stored, the global nature of networks makes it much more difficult to constrain data flows.

5.28. *A Question of Trust* provided the following explanation of data in transit across national jurisdictions:

> *A network is a group of devices which are linked and so able to communicate with one another. The internet is often described as a 'network of networks', all of which are interconnected. Communications over the internet take place through the adoption of protocols which are standardised worldwide. A single communication is divided into packets (units of data), which are transmitted separately across multiple networks. They may be routed via different countries as the path of travel followed will be a mix of the quickest or cheapest paths; not necessarily the shortest path. The quickest path will depend upon bandwidth capacity and latency (the amount of data which can be sent through an internet connection and the delay). The result of this method of transmission is increased data flows across borders. For example, an email sent between two persons in the UK may be routed via another country if that is the optimum path for the CSPs involved. The route taken will also depend on the location of*

servers. The servers of major email services like Gmail, Yahoo and Hotmail are based outside the UK.[215]

Network service providers

5.29. Data going in and out of personal devices follows different and complex routes across equipment owned by many different providers. This is unseen and largely unnoticed by private users of devices. Often it is possible to ignore this by buying a service from a network provider who uses a combination of their own equipment and services obtained from others to provide the overall network we effectively use for our telecommunications. These companies are Communications/Carriage Service Providers (C/CSPs), although under TOLA they are called Designated Communications Providers (DCPs). While the engineers will have more accurate definitions, basically C/CSPs make sure our data – the 0s and 1s on our devices – get to where it needs to when it needs to.

5.30. Often the C/CSP is the company that provides the access network we first connect to – for example, Telstra or Optus. However, other companies can provide this service – for example, retail service providers like TPG and Exetel provide home broadband services across the NBN; and virtual mobile operators provide mobile phone services using the Telstra network.

Application service providers

5.31. When network service providers move data from A to B, that does not, of itself, provide something that is useful for a private mobile phone or computer user. That requires application service providers, who add extra services to turn such data flows into something useful.

5.32. In traditional 'circuit switched' voice calls, the C/CSP turned voices into electrical signals, set up a connection to the 'other person' and sent these signals until the phone was hung up. In that situation the C/CSP was the application service provider.

5.33. However, direct voice calls between 2 people provided by the C/CSP, often referred to as 'circuit-switched' calls, are now a very small part of telecommunications. Now, IP data networks are used to communicate in other ways, such as email or chat services.

5.34. In the early days of the internet, the C/CSP still often provided the application service – for example, Telstra provided BigPond email for its customers. However, today people use a vast range of different applications provided by different

[215] David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (UK Government, London, 2015) [4.12].

companies. While BigPond email is still available, many use services from other providers, such as Google or Hotmail. When the application service to provide something useful to the user is provided by someone other than the C/CSP, this is referred to as Over-The-Top (OTT) services. As well as messaging and email, these can take many other forms, such as TV streaming services, social media platforms and so on. An operator of these other communication platforms can range from an individual developing software for fun to a large multinational enterprise, or it may be some other entity/organisation between these in scale.

5.35. OTT services can even replace traditional voice calls. There are a number of providers such as Skype, WhatsApp and others who provide voice call services as VoIP services. However, VoIP is not the exclusive preserve of OTT providers – an NBN connection is only a data connection; and the network service provider is using VoIP to allow the landline phone to still work.

5.36. Also, application service providers may be involved in more than just an 'app' on your phone; they often have software running in different places across the network and even special arrangements with the C/CSP. For example, TV providers such as Netflix set up 'content delivery networks' with network providers to ensure their data can get to their customers quickly.

Overview of communications infrastructure

5.37. Apart from the overall complexity of the different infrastructure components outlines above, the other notable factor is the involvement of multiple service providers who together make up the telecommunications services that are used every day and taken for granted. The fact that C/CSPs are now only a small part of the telecommunications infrastructure in a way not envisaged when the TIA Act was drafted in 1979 was one of the stated reasons for the introduction of TOLA. TOLA introduced the much broader concept of the DCP to cover as many of these other types of provider as possible.

Encryption

5.38. Encryption is a branch of cryptography designed so that transmitted data is only intelligible to those authorised to decrypt, and thus make intelligible, that data, whether that is ultimately viewed as text, voice, images or in some other format.

5.39. Although it has come to prominence in recent years, particularly in relation to encrypted communication platforms such as WhatsApp and Signal, for many years encryption has been a key part of communication systems, protecting the data being transported and stored on telecommunications networks from unauthorised access.

5.40. For example, encryption aims to ensure the security of online banking and the privacy of sensitive data stored by Government departments, such as Services Australia, formerly the Department of Human Services; and to stop others seeing personal information or images on a personal mobile phone or device.

5.41. The benefits of encryption, and the risks that it mitigates, have been noted by the Australian Signals Directorate (ASD) and its Australian Cyber Security Centre.[216]

5.42. The main change in recent years has been that more and more data is being encrypted by default to improve security and privacy – a change sometimes referred to as ubiquitous encryption.

5.43. Originally, most encryption was 'symmetric encryption': both parties used the same secret 'key' to both encrypt and decrypt messages. The key therefore needs to be shared before starting to communicate using encryption. So, if an adversary can intercept the key, they can then decrypt the communications.

5.44. In an attempt to counter the risks associated with the use of one key, asymmetric encryption was developed in the 1970s. Asymmetric encryption involves the use of 2 linked keys – a public key and a private key. A user who wants to send an encrypted message can get the recipient's public key from a public directory. This key is used to encrypt the message, which is sent to the recipient. The recipient can then decrypt the message with a private key. Asymmetric encryption was traditionally considered to be more difficult and slower to implement. However, with improvements in computing power, it is now commonplace.

5.45. Asymmetric encryption aims to remove the opportunity for an unauthorised person to intercept the transmission of the private key that would allow them to decrypt messages. Public keys are, by definition, publicly available, but the encryption algorithms are designed to make it (almost) impossible to derive the private key from the public key. However, there is a branch of mathematics known as cryptanalysis that is dedicated to finding weaknesses in such algorithms, with varying degrees of success.

5.46. This illustrates a key point: encryption, as with any other security measures, is never 100% guaranteed to be secure. Any system has to be designed to allow authorised people to access the data, and this will always provide a potential route for others

[216] Australian Signals Directorate, *Australian Government Information Security Manual* (Australian Government, Canberra, December 2019); Australian Cyber Security Centre, Australian Signals Directorate, *Cloud Computing Security* (Australian Government, Canberra, July 2018) <https://www.cyber.gov.au/advice/cloud-computing-security>; Mike Burgess, Director-General, Australian Signals Directorate, 'Director-General ASD Statement Regarding the TOLA 2018', 12 December 2018 <https://www.asd.gov.au/publications/statement-tola-act-2018>.

to get access as well. The reference to encryption 'keys' links to some good analogies to keys for physical locks – if someone can get a copy of the key for a specific lock they can open the lock. Similarly, if they get the encryption key for a particular piece of data, they can decrypt it. If a whole series of locks is designed to be opened with a master key then, if someone gets a copy of that master key, they can open all the locks. Equally, if an encryption system is designed with a master key then, if someone gets hold of that key, they can access all of the data it protects. There are often good reasons to build a system with a master key – for ease of maintenance, to be able to help users that get locked out and so on. But a system with a master key has additional security risks if an unauthorised person gets access to that key.

Encryption of different types of data

5.47. Encryption can take many forms and be applied in many different places, but for the present purpose I consider, firstly, the data to be encrypted – namely, *data at rest vs data in transit* – and, secondly, where the encryption is controlled – on the device, on the network or by the application service provider.

Data at rest

5.48. 'Data at rest' is data stored on a device, computer server or other equipment. Data at rest is encrypted so as to prevent someone who physically accesses the device from being able to see the data.

5.49. The most common example of 'data at rest' is a certain type of data on a mobile device such as a smartphone. The data stored there will include the user's emails, messages, contacts, photos, other application data and more. It is a 'data rich' environment. If a user is attacked successfully by cyber criminals to obtain this data, it can be devastating for the user's privacy and confidentiality. Recognising the importance of security to the market, and the importance of privacy to users, in 2014 device manufacturers such as Apple and Google moved to include encrypted data as a default setting on devices. Users had to enter a passcode to unlock the device and access the data. Today, to increase security, encryption software on these devices is now 'user-controlled' – that is, only the user can unlock their device. Previously, Apple, for example, could unlock any device using a key that it controlled, but now it is unable to unlock the devices it sells. This increases security, but it does mean that Apple cannot help the user to recover their data if they forget their passcode.

5.50. Data at rest is also stored by application service providers – for example, mail messages are stored on an email server. This data is typically protected by other means such as 'authentication' and 'access control', so that another user cannot access the mail message. Encryption of this data is less common, as there may be little risk of someone getting unauthorised physical access to a server in a secure

data centre, but the application service provider can implement it to improve security. In this case, the encryption is controlled by the service provider, as they typically need to control the encryption and decryption to provide their services to the end users.[217]

Data in transit

5.51. 'Data in transit' is data that is being moved from one place to another across a telecommunications network and other systems. This data may be encrypted to stop unauthorised people who may have access to the intermediate systems from being able to see the content of the data that is being sent. In the physical world an analogy would be to send mail in a locked box so that anyone who gets into the delivery van or sorting office cannot see what is in there.

5.52. Encryption of data in transit has become more common in recent years due to increasing awareness of security and improved computing power, which enables encryption of data even at the high data rates and volumes now present. The fact that data may be sent across different infrastructure owned by different companies that the user may be completely unaware of is also a motivation for encrypting such data in transit.

5.53. This encryption can be implemented at a number of levels:

a. **Encryption by the network service provider**: This can be implemented on the access network – for example, when a mobile phone communicates with the mobile phone mast, the data sent across the airwaves is encrypted. This stops someone with a radio scanner sitting nearby and hearing all the content of phone calls. Before this encryption was implemented in the 1990s, some public figures were embarrassed by exactly this technique. It can also be implemented through to the core network that the service provider operates. But in all these cases it is under the control of the network provider – they are able to access and decrypt the data, because they need to in order to then send the data to where it needs to go.
b. **Encryption by application service provider**: This may be implemented between the end user and the servers operated by the application service provider. For example, it is common nowadays for almost all websites to communicate with users using a technique known as 'Secure Sockets Layer' (SSL) – the 'https' in the website address. Indeed, some browsers warn that sites not using this are insecure. This encryption is controlled by the application service provider, who

[217] It is possible for users to implement 'client-side' encryption where they control encryption of their data stored on remote servers but consider this is effectively an example of device-based encryption.

needs to be able to decrypt the data from the user in order to provide the web page content requested or, in the case of a system such as Facebook, to store the content of 'posts' from users so that other users can read them.

c. **End-to-end encryption**: In this case, the data is encrypted all the way from the sender to the intended recipient of the communication. Popular examples are WhatsApp and Signal messaging applications, but there are many others. For example, some financial institutions use 'secure mail services' to send email messages that can only be read by the recipient. Depending on how the application service provider sets up the encryption, it is possible that it may be completely user controlled and the service provider has no access to it.

Summary: different types and levels of encryption of communication

5.54. There are different types and levels of encryption. Most communications involve one or more of these. Depending on how they are implemented and where, a law enforcement authority may require collaboration from a number of different service providers, or it may not be possible at all. This again shows that, because of encryption used by other parties outside the control of network service providers, the traditional lawful interception approach of only mandating assistance from the network service provider may not allow law enforcement authorities to see any intelligible data content.

Different types of data

5.55. Traditionally, when voice calls on the PSTN were the main method of communication, communications data consisted of the audio content of the call along with the basic data the phone company generated for billing (number dialled, start time and duration). That is very different now due to the pace of uptake of digital technologies, growing numbers of internet connected devices, and data volumes going across the network. This means that there is a much broader range of data being generated and sent. As the Internet of Things becomes more commonplace, this proliferation will increase. A key distinction in data is between content and metadata.

Communications content versus metadata

5.56. 'Content' involves all the information that the user has intentionally developed or received from another person or system. This is usually the actual message users read, hear or look at. 'Metadata' is information about the content that facilitates the communication, formats the content and can provide additional value to user communications. Examples are the location of a photo, the email server 'to' and 'from' information in an email and the 'formatting' and 'tagging' information of web

pages. It can include a data-description of the user services to enable the network communications systems function.

5.57. Conceptually, metadata enables the user content of the communications, but is not the content.

5.58. But sometimes the distinction is not clear-cut, and there are also some grey areas. For example, some systems consider email subject headers as metadata and some as content. In fact, at one time mobile phone systems considered SMS contents as metadata, as they were originally intended to be used for network service information. However, now they are mainly used for personal communication content.

Communications content

5.59. Australian law does not define content of communications, but it does define metadata negatively[218] as *excluding* any:

a. information that is the contents or substance of a communication
b. documents (to the extent they contain the contents or substance of a communication).

5.60. UK law has a more positive definition of content. It is considered to include any element of the communication, or any data attached to or logically associated with the communication, that reveals anything that might reasonably be considered the meaning (if any) of the communication, but it excludes any meaning arising from the fact of the communication.[219]

5.61. Communications content is more than just the audio content of phone calls. Sometimes content is sent across the network, but in other cases it may be stored as data at rest by application service providers. Obvious examples are the content of emails or messages that are stored on a server run by the application service provider. Another example that may be less obvious is the data from backing up mobile devices. In many cases the mobile device is 'backed up' to a globally hosted

[218] *Telecommunications (Interception and Access) Act 1979* (Cth) (TI Act), s 172.

[219] *Investigatory Powers Act 2016* (UK), s 261(6), provides:

> *'Content', in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but – (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and(b) anything which is systems data is not content.*

'cloud' service where all messages, contact directories, calendars, keys, photos, audio and video, metadata and host device configuration are stored. Examples of these include iCloud,[220] Google Account,[221] and HUAWEI Mobile Cloud.[222]

Richness of metadata

5.62. In the days of landline PSTN calls, metadata consisted simply of what was needed to enable the call – start time, end time and number dialled. In the modern world of telecommunications, there are often huge volumes of other data generated and stored, either directly needed to provide the service or generated incidentally.

5.63. Network service providers often need to generate and collect extra metadata to provide their services. For example, mobile phone networks always generated the location of the user, as this was needed to send the right voice content to them. In today's world of OTT services, these providers often also collect and generate metadata. This may be data needed to enable service provision, but it may also be linked business models that rely on the collection and exploitation of data. This means users often share much data without being fully aware of it.

5.64. Some examples are:

a. **Location data**: This can go to much greater detail than the mobile phone cell that a user is in. A person checking the weather forecast tells the provider their current location. When checking route guidance on Google Maps, Google knows where the user is, calculated using GPS to an accuracy of a few metres. When a user is following a route, regular updates are sent on destination while tracking the user's progress over time. Location information can also be generated from seemingly unconnected sources, including connecting to public Wi-Fi networks or mobile phone cameras embedding location data in image files.
b. **Biometric data**: Advances in technology have also introduced greater use of biometric data to verify and grant access. Examples include fingerprint recognition used to log in to Android phones, and the 3D facial recognition that

[220] iCloud TM 'is a cloud computing solution by Apple Computer Inc. that provides cloud storage and apps for desktop, tablet and mobile devices. iCloud provides the ability to store documents, videos, photos, music and other data online and the ability to sync it between iOS-powered devices'.

[221] Google Account: 'You can back up content, data, and settings from your phone to your Google Account. You can restore your backed-up information to the original phone or to some other Android phones.'

[222] HUAWEI Mobile Cloud 'allows you to back up your data to a secure cloud which prevents data loss in the event that you lose your phone as well as allowing you to conveniently transfer your data to a new device anytime, anywhere'.

recent Apple phones use. There are even experiments taking place that allow someone to be uniquely identified from their gait – the way they walk. This could come from camera observations or even just the motion sensors on a mobile phone carried in the pocket.

c. **Machine-to-machine communication**: The growth of the Internet of Things has led to a massive growth in automatic measurements of data that are regularly sent to service providers. For example, smart electricity meters measure electricity usage levels in real time, internet-connected fridges check levels of stock, and sensors in bins report how much rubbish has accumulated over time.

Security and privacy challenges

5.65. Generally, user content is considered most sensitive, and it is protected more strongly using technical measures and in legislation. However, metadata can still be sensitive. Obvious examples are email addresses showing who the user is communicating with; and the search queries a user puts into search engines such as Google. Looking at the richness of metadata, there are some less obvious risks.

5.66. Location data is one example of this. As discussed, users often wittingly or unwittingly share the location information with service providers all the time. While these features may be designed to optimise convenience (such as advising routes to avoid traffic congestion), much of this location data is routinely tracked and stored on default settings, frequently without the full knowledge of the user.

5.67. In addition, there is an increasing market of apps that openly track users' locations. Indeed, advances in technology mean that many parents are readily able to track the location of their children using geolocation devices such as smart watches, GPS devices and smartphone apps. A recent study by the Royal Children's Hospital in Melbourne found that 18% of parents surveyed reported using a tracking device. This was more common among parents of teenagers (24%) than primary school aged children (12%). Of those parents who did not report using a tracking device, almost half (45%) said they would consider doing so in the future.[223]

5.68. From a security point of view, there can be serious risks in these sort of apps – who is collecting the data, how are they storing it and how do they use it? Data may not be properly secured – for example, it may be protected only by an easily guessable password. It may be being deliberately sold – there are examples in the US of mobile phone companies selling location data to help bounty hunters track down

[223] Dr Anthea Rhodes, *Child Health Poll – Travelling to School: Habits of Australian Families* (Royal Children's Hospital, Melbourne, February 2019) 4.

fugitives.[224] Location data can be exploited to enable stalking, and perpetrators of domestic violence are doing this at an 'unprecedented rate'.[225]

5.69. Another example is the biometric data being collected by devices. Without appropriate protection, this can have impacts on personal privacy (like being recognised every time you walk down the street) and on security (such as someone 'using' your fingerprints to assume your identity). In addition, there is an increasing market of apps that openly track users' locations.

A current example: tracking exposure to COVID-19

5.70. As I write this report, the world is facing the COVID-19 pandemic. Understandably, everyone wishes to minimise its effects. A present focus is on 'social isolation' for almost everyone and a complete quarantine for those who have the virus. Media reports on a single day in late March 2020 suggested the following types of official use of data and metadata:

a. The *New York Times* reported that 'Prime Minister Benjamin Netanyahu of Israel has authorized the country's internal security agency to tap into a vast and previously undisclosed trove of cellphone data to retrace the movements of people who have contracted the coronavirus and identify others who should be quarantined because their paths crossed … The existence of the data trove and the legislative framework under which it is amassed and used have not previously been reported. The plan to apply it to fighting the virus, alluded to only vaguely by Mr. Netanyahu, has not yet been debated by lawmakers or revealed to the public. The idea is to sift through geolocation data routinely collected from Israeli cellphone providers about millions of their customers in Israel and the West Bank, find people who came into close contact with known virus carriers, and send them text messages directing them to isolate themselves immediately'.[226]

b. The *Independent* reported that 'Taiwan, which has won global praise for its effective action against the coronavirus, is rolling out a mobile phone-based

---

[224] Joseph Cox, 'I Gave a Bounty Hunter $300. Then He Located Our Phone' *Vice* (online, 9 January 2019) <https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile>.

[225] Julie Inman Grant, eSafety Commissioner, 'When "Smart" is Not Necessarily Safe: The Rise of Connected Devices Extending Domestic Violence', *eSafety Commissioner* (blog, 13 May 2019) <https://www.esafety.gov.au/about-us/blog/when-smart-not-necessarily-safe-rise-connected-devices-extending-domestic-violence>.

[226] David M Halbfinger, Isabel Kershner and Ronen Bergman, 'To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data' *New York Times* (online, 16 March 2020) <https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html>.

"electronic fence" that uses location-tracking to ensure people who are quarantined stay in their homes. Governments around the world are combining technology and human efforts to enforce quarantines that require people who have been exposed to the virus to stay in their homes, but Taiwan's system is believed to be the first to use mobile phone tracking for that purpose. "The goal is to stop people from running around and spreading the infection," said Jyan Hong-wei, head of Taiwan's Department of Cyber Security, who leads efforts to work with telecom carriers to combat the virus. The system monitors phone signals to alert police and local officials if those in home quarantine move away from their address or turn off their phones. Mr Hong-wei said authorities will contact or visit those who trigger an alert within 15 minutes'.[227]

c. The *Wall Street Journal* reported that 'Government officials across the U.S. are using location data from millions of cellphones in a bid to better understand the movements of Americans during the coronavirus pandemic and how they may be affecting the spread of the disease. The federal government, through the Centers for Disease Control and Prevention, and state and local governments have started to receive analyses about the presence and movement of people in certain areas of geographic interest drawn from cellphone data, people familiar with the matter said. The data comes from the mobile advertising industry rather than cellphone carriers. The aim is to create a portal for federal, state and local officials that contains geolocation data in what could be as many as 500 cities across the U.S., one of the people said, to help plan the epidemic response. The data – which is stripped of identifying information like the name of a phone's owner – could help officials learn how coronavirus is spreading around the country and help blunt its advance. It shows which retail establishments, parks and other public spaces are still drawing crowds that could risk accelerating the transmission of the virus, according to people familiar with the matter. In one such case, researchers found that New Yorkers were congregating in large numbers in Brooklyn's Prospect Park and handed that information over to local authorities, one person said. Warning notices have been posted at parks in New York City, but they haven't been closed'.[228]

d. The ABC reported that 'Phone tracking used to follow movements of Chinese couple with coronavirus in Adelaide. A phone-tracking system used to better

[227] Yimou Lee, 'Coronavirus: Taiwan Tracking Citizens' Phones to Make Sure They Stay Indoors' *Independent* (online, 20 March 2020) <https://www.independent.co.uk/news/world/asia/coronavirus-taiwan-update-phone-tracking-lockdown-quarantine-a9413091.html>.

[228] Byron Tau, Government Tracking How People Move Around in Coronavirus Pandemic' *Wall Street Journal* (online, 28 March 2020) <https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202>.

> understand where 2 people infected with coronavirus roamed in Adelaide is the same system harnessed by SAPOL for criminal investigations, the state's Police Commissioner has said. Commissioner Grant Stevens said police used a program that only required a phone number to give operators "a download of where the phone had been used". "We're doing that to assist SA Health in tracking down the movements of the two people concerned so we can do our best to identify any people who might have been exposed [to coronavirus]," he told ABC Radio Adelaide. "It's used quite frequently for criminal investigations." … Phone metadata has been a contentious issue for privacy advocates worldwide, particularly in Australia where data retention laws mean phone and internet companies have to save the information for two years. This included location data that was collected every time a person used their phone for texting or calling – recording where the interaction took place and for how long. Location data was also collected every time a device connected to or pinged off a phone tower as part of its regular functionality. The data combined to create a veritable tracking device out of smartphones, roughly logging a carrier's location every 20 minutes or so. That information can be made available to government departments, police, and security agencies. SAPOL would not comment further on the methodology of its own system but said it was used under the framework of the Telecommunications (Interception and Access) Act of 1979 and gave a general indication of where the phone had been used. Commissioner Stevens said they used data that came "from the use of the phone, not the physical device" and it was not affected by whether that device had its location services switched on or off'.

5.71. The point of these examples is to show the wide scope of the use of current technology and laws, its dynamic expansion at a time of crisis, and the ever-present need for proper thresholds and safeguards. Since that March 'snapshot', the Commonwealth Government has introduced a voluntary COVID-19 app and the Parliament has enacted stringent safeguards in the *Privacy Amendment (Public and Health Contact Information) Act 2020* (Cth).

5.72. I have noted above the growth of the Internet of Things. While much of the data being collected and transmitted may seem mundane, it may be a real security threat. For example, detailed patterns of your electricity usage could allow someone to work out when your home is empty and break into it. This threat is even greater when considering aggregation of data – combining data on your electricity usage, your food shopping, your GPS-connected car and even the weight of your bin every week could reveal sensitive health-related information. Some, perhaps many, Internet of Things devices are poorly secured and operated by service providers with substandard privacy and security measures.

5.73. Although communications content is commonly encrypted, this is less common for metadata. Sometimes it is just because of the perceived lower sensitivity of the data;

sometimes it is due to resource challenges – for example, small internet-connected sensors will typically be battery powered to minimise their electricity usage, so they may not be able to run encryption processing. There are also practical problems that mean metadata cannot generally be end-to-end encrypted. The service providers need to collect and use the data somewhere. To take an example in the physical world, imagine sending a letter where the address on the envelope was unintelligible to anyone except the recipient. How would the postal service ever get it to the right place? Nevertheless, there is some evidence that sophisticated criminals do encrypt metadata when they can.

Challenges for lawful access to communications

5.74. The TIA Act, passed in 1979, prohibits interception of communications except under judicially authorised warrants. The principle of the TIA Act is that, while privacy of communications must be protected, law enforcement and security agencies can have access to the content of communications of subjects of interest if they can demonstrate reasonable cause and an appropriate warrant process. C/CSPs are required to develop and implement an Interception Capability Plan that allows them to implement these warrants and provide the content of the warranted targets communications to the authorised agency.

5.75. In 1979 the communications landscape was very different. All communications were voice calls from fixed phone lines at a particular address. Interception often involved the use of 'alligator clips' physically attached to the phone lines of targets to allow passive interception of the traffic. Such crude techniques are generally not feasible or practicable in today's telecommunication networks. Therefore, more modern electronic techniques are used. These often use 'lawful interception' functionality that is built into network switches. This technique allows suitably authorised operators to connect in a third passive user to listen to a conversation between 2 target users. This type of open, published capability to intercept communications, which may otherwise be encrypted and inaccessible, is an established standard feature and could commonly be referred to as a 'front door'.

5.76. A key challenge for law enforcement is 'end-to-end encryption' or, as noted above, encryption of data in transit at the device level. This means the C/CSP, which only provide the network service, moving the data around, only sees data when encrypted and has no ability to decrypt the data. In this case the C/CSP can comply with the warrant and intercept traffic at the level of its network, but the content provided to the agency is useless, as it is encrypted and hence unintelligible.

5.77. Another challenge concerns attribution of communications – linking a particular communication to a particular person responsible for sending it and to their intended recipient(s). Attribution of communications is increasingly difficult, as both

the design of the internet and the number of digital devices can present significant challenges. As *A Question of Trust* commented, new technologies and platforms can offer 'a cloak of anonymity' and improve the security of information. This is achieved by a combination of encryption and the anonymisation services provided by some application service providers. These can offer businesses and individuals significant security value that is fundamentally important to the broader community. But it can also enable criminal activity and assist foreign State adversaries and their proxies.

Addressing the challenges – laws keeping pace with technology

5.78. The time has long passed since the AFP could put alligator clips on a suspect's home phone line and hear the contents of every call they made. Today, criminals and adversaries use different devices. Their communications use multiple network service providers and application service providers and are often encrypted at different levels, so intelligible information cannot be obtained, hence the term 'going dark'.

5.79. It is these challenges that TOLA is designed to address. What are some of the options and approaches potentially available today? Details of the capabilities and operations of Australia's law enforcement and security agencies are necessarily classified. But the challenge is a global one, and there are a number of examples openly available regarding the work of law enforcement agencies in Australia and elsewhere, as well as from some companies commercially selling capabilities.

5.80. Sir David Omand has noted[229] that there are a range of techniques that agencies use, including trying to obtain intelligence from the unencrypted metadata. These approaches may still require network and application service providers to assist – for example, in extracting and formatting the relevant data. Agencies may also need to work with multiple network and application service providers to get enough information to be of value to the investigation, although the agency may often still need to use advanced data analytic techniques.

5.81. Metadata can be of use. However, if agencies are able to access the content of communications, this will generally be much more valuable to them, even though more sophisticated techniques are needed.

5.82. For example, the contents of communications over WhatsApp are end-to-end encrypted, but they are visible and legible to the user on the device itself. By getting physical access to the phone while it is unlocked, the messages can be read. However, if a law enforcement agency is able to seize the device – for example, on arrest of a suspect – then the device is normally locked and the content is encrypted

[229] Sir David Omand and Mark Phythian, *Principled Spying: The Ethics of Secret Intelligence*, (Georgetown University Press, 2018) Ch 5.

and not visible. Therefore, it is necessary to access the encrypted data at rest on the device.

5.83. One very simple method relies on the fact that most users use a simple PIN that can be viewed at a distance. Video surveillance could be used to obtain the PIN before seizing the device, and then this can be used to unlock the phone. Another option is to seek technical assistance to unlock the device from the manufacturer or a third party. One of the most famous examples arose after a terrorist attack in San Bernardino, California, in 2015. The Federal Bureau of Investigation (FBI) asked Apple to develop special software to allow it to unlock an iPhone 5C that it recovered. When Apple refused, the FBI got help from a company which appeared to have found some security vulnerabilities in the phone that allowed it to be unlocked.

5.84. Where a device cannot be physically accessed (for example, due to the risk to officers in gaining physical access), agencies could try to remotely exploit (or 'hack') the device to access data stored on it. This uses capabilities referred to as 'computer network exploitation' (CNE). CNE involves exploiting natural weaknesses in subjects' devices rather than increasing security vulnerabilities for multiple users by creating back doors. ASD's CNE capabilities were publicly acknowledged by the then Director-General, Mike Burgess, in March 2019.[230]

5.85. Common cyber-attacks on smart mobile devices include:

a. 'spear-phishing'[231] via email

b. 'drive-by-download'[232] via malicious web-pages

c. 'social engineering'[233] via social media tools and electronic friendships.

[230] Mike Burgess, Director-General, Australian Signals Directorate, 'Offensive Cyber and the People Who Do It' (Speech, Lowy Institute, 27 March 2019) <https://www.asd.gov.au/publications/speech-lowy-institute-speech>.

[231] 'Spear phishing' is a well-established cyber technique whereby an individual is profiled and then a tailored email or similar message is sent to the target and, by means of misrepresented trust, the target activates or installs some malicious software or behaviours.

[232] 'Drive-by-download' is a well-established technique whereby a target is encouraged to connect their device to a malicious internet website or system that installs or activates malicious software and behaviours.

[233] 'Social engineering' is a well-established technique whereby a group or person attains trust with the target and actively encourages the user and device to activate or install some malicious software or behaviours.

5.86. Target device users can be encouraged to reset passwords, install tools and apps, connect to rogue networks, and use less secure communications.

5.87. Another option could be to seek access to data at rest when it is stored on the network. This may not always be encrypted. Where it is, the service provider may still be able to have access as they control the storage and the encryption. This sort of data could include a complete backup of the phone. This could be a very valuable and rich source of information for a law enforcement or intelligence investigation. Therefore, the agency could ask the service provider to cooperate by making this data available. However, service providers recognise the importance of securing their users' data and the potential for criminals to duplicate a target user's device and information during a successful cyber attack. Given this, the service providers will often go to great lengths to protect this access or even find ways to ensure they and their staff have no ability to access the data. Even if they do potentially have the capability to provide access, the data may be stored outside the country, and a foreign company may refuse to cooperate.

Exceptional access, back doors, front doors and more

5.88. The ongoing encryption debate employs a number of terms that are commonly used but with different definitions and meanings to different people. The concepts of 'systemic weakness' and 'vulnerability' are discussed elsewhere in this report, but here I define some key terms.

Exceptional access

5.89. 'Exceptional access' refers to any function built into a communication service to allow access to the content of the communications of a specific user. Any exceptional access represents a risk to the users of the system, who have an expectation that their communications will be private and that the service provider will not have access to the contents. Any exceptional access mechanism runs the risk of misuse by criminals and adversaries – if they are able to gain control of the access, they can intercept the communications of potentially any user of the services. Thus, the security safeguards put around any such access are critical. However, exceptional access is a well-established capability – as noted above, many current telecommunications interception capabilities are implemented using such an approach.

Back doors

5.90. The metaphor of 'doors' is used frequently in discussions about such access. 'Doors' refer to access to communicated information by any unauthorised person.[234] In particular, the term 'back door' is often used, but it has connotations of something shady and unauthorised. Here I define a 'back door' as an exceptional access function that is implemented in an undocumented manner – those not authorised to use the feature are unaware of its existence, users are unaware, and it is generally protected by 'security through obscurity'. There is a lack of accountability around its use, and if its existence becomes known to an adversary the consequences are often critical.

Front doors

5.91. In contrast, a 'front door' is a documented feature. In 2014 the then Director of the FBI defined a 'front door' as a door which is 'built transparently' so that 'the chances of a vulnerability being unseen are much lower' than with a back door.[235]

5.92. Regardless of whether these access points are known as 'front doors' or 'back doors', they nonetheless exist. As Lord Anderson has said, 'a door is however a door, and the difference between front and back generally relates to the acknowledgment of its existence rather than to any technical distinction'.[236]

5.93. As I explore elsewhere in this report, many service providers have strongly opposed any kind of door, as the mere existence of doors increases the risk of unauthorised access. This affects consumer trust in their products and has a subsequent impact on market share. This unauthorised access may come from foreign governments, or their proxies, or private criminal actors. This risk undoubtedly exists and must be considered when balancing the requirements of assisting and enabling the work of Australia's security, intelligence and law enforcement agencies.

---

[234] David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (UK Government, London, 2015) [4.52].

[235] James Comey, Director, US Federal Bureau of Investigation, 'Going Dark: Are Technology, Privacy and Public Safety on a Collision Course', *Brookings Institution* (Youtube, 14 October 2014) <https://www.youtube.com/watch?v=Dkbh5fJoFhc> and quoted in David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (UK Government, London, 2015) [4.53].

[236] Ibid.

No binary choice is required

5.94. Some have said that there is a binary choice between universal decryption by police and intelligence agencies and a complete prohibition on doing so. I do not agree. As I said in my 2020 Lowy speech and now repeat:

> *not only are the topics I have mentioned vast and complex, but they sometimes attract strident overstatement based on extreme or improbable examples. So I am very grateful for the clear and informed thinkers in this field a number of whom have made submissions, and I also mention the Encryption Working Group assembled by the Carnegie Endowment and Princeton University which recently said:*
>
> > *The working group rejects two straw men – absolutist positions not actually held by serious participants, but sometimes used as caricatures of opponents. These are: (1) that we should stop seeking approaches to enable access to encrypted information (2) that law enforcement will be unable to protect the public unless it can obtain access to all encrypted data through lawful process.*

5.95. Similarly, Sir David Omand has recently written:

> *As with all hard public policy issues, there is no easy way of reconciling conflicting ethical concerns. Place the security of personal data and one's anonymity on the Internet above all else and law enforcement is shut out, the rule of law is undermined, and crime, terrorism, and cyber-attacks flourish. Insist on a right of access to all encrypted data for law enforcement and intelligence agencies – for example, through controlling or weakening encryption standards – and confidence in the Internet as a secure medium will be lost, and fragmentation of the Internet will spread.*[237]

I agree with the statements by both Sir David and the Encryption Working Group. No binary choice is required. Rather, the fundamental and companion principles I have identified earlier are the surest guide.

[237] Sir David Omand and Mark Phythian, *Principled Spying: The Ethics of Secret Intelligence*, (Georgetown University Press, 2018) 'Digital Intelligence and Cyberspace' 44.

6. CONTEXT: PRIVACY – RIGHTS AND SAFEGUARDS

Legitimate expectations of privacy

6.1. A regular theme in submissions made to me is the need for TOLA, and the agencies which utilise its powers, to respect, and be seen to respect, 'privacy' or 'the right to privacy'. It has already been noted in this report that the factors a decision-maker is to take into account in determining whether a request or notice under Schedule 1 of TOLA is 'reasonable and proportionate' include 'the legitimate expectations of the Australian community relating to privacy and cybersecurity'.[238] It is therefore important to analyse what is meant by privacy and how it may be protected.

6.2. Chapter 2 of *A Question of Trust* considers what 'privacy' entails and why it is important. It refers to a famous *Harvard Law Journal* article of long ago[239] by Samuel Warren and Louis Brandeis (later a Justice of the Supreme Court of the United States). The authors characterised privacy as 'the right to be let alone'. As *A Question of Trust* notes, privacy has alternatively been characterised as the 'right to conceal or hide information about ourselves' and something that 'can also be understood in terms of *control*. Since knowledge is power, the transfer of private information to the state can be seen as a transfer of autonomy and of control'.[240]

6.3. As *A Question of Trust* goes on to observe, in terms I would adopt, privacy, variously:

> *(a) enables the expression of individuality. Without privacy, concepts such as identity, dignity, autonomy, independence, imagination and creativity are more difficult to realise and maintain. … It facilitates an inner sanctum that others must respect. It grants us the freedom to function autonomously, without our every action being observed (or countermanded) by others. Of course, if we choose to express our individuality in criminal or anti-social ways, privacy can facilitate that too;*

---

[238] *Telecommunications Act 1997* (Cth), s 317C(h) in respect of Technical Assistance Requests (TARs); s 317RA(f) in respect of Technical Assistance Notices (TANs); s 317ZAA(f) in respect of Technical Capability Notices (TCNs).

[239] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890–1891) 4 Harv L Rev 193, 205.

[240] David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (UK Government, London, 2015) [2.7].

(b) facilitates trust, friendship and intimacy: qualities that allow us to relate freely to each other and that form the essential basis for a diverse and cohesive society. Conversely, surveillance has been shown to lead to self-censorship and the suppression of certain behaviour, though once again, antisocial as well as pro-social behaviour may be suppressed by surveillance; and

(c) is necessary for the securing of other human rights, ranging from the freedom of political expression to the right to a fair trial.

6.4. The Department of Home Affairs rightly accepts the importance of privacy and the need to proceed cautiously when interfering with it. In a submission to this review it stated:

> *It is essential that when interferences with privacy occur – online or offline – they occur consistently with the rule of law set down prospectively to ensure the application of the rules is not arbitrary or capricious, and that procedural fairness and natural justice are afforded to those under investigation. The Assistance and Access Act – in so far as it facilitates lawful interference with privacy that is authorised by other investigative powers – is one aspect of the rule of law that makes it permissible to abrogate individual privacy for legitimate purposes.*
>
> *This position finds precedent in international human rights law which recognises the right to privacy may be limited for the legitimate purposes of enforcing the criminal law, assisting the enforcement of criminal laws in a foreign country, the interests of national security, foreign relations or economic wellbeing. The Assistance and Access Act's safeguards and thresholds ensure that the law may only impose limitations on the right to privacy where it does so for one of these legitimate purposes*.[241]

6.5. The international law position is examined in the next chapter. I now turn to the Australian position.

Existing privacy laws and protections in Australia

6.6. Unlike the position in some other countries, Australia does not have any federal charter of rights that formally recognises any 'right to privacy', and a specific constitutional or tortious right to privacy has not yet been recognised. In the recent High Court decision of *Smethurst v Commissioner of Police*[242] (*Smethurst*), Gageler J

[241] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 10.
[242] [2020] HCA 14.

noted that the question whether Australian law should recognise an 'independent cause of action for infringement of a distinct right of privacy'[243] was left open by at least some members of the Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd.*[244]

6.7. Justice Gageler went on to say:

> *124. It is now more than 250 years since the celebrated judgment of Lord Camden in* Entick v Carrington *cemented the position at common law that the holder of a public office cannot invade private property for the purpose of investigating criminal activity without the authority of positive law. Lord Camden referred to the private papers unlawfully seized in that case as their owner's 'dearest property'. He said that 'though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass'. In so saying he recognised a link between protection of personal property and protection of freedom of thought and political expression.*
>
> *125. Of the judgment in* Entick v Carrington*, it has been said:*
>
> > *The principles laid down in [it] affect the very essence of constitutional liberty and security. They ... apply to all invasions on the part of the government and its [officers] of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence, – it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment.*[245]

6.8. In *Smethurst,* Kiefel CJ and Bell and Keane JJ say this about the law of search warrants:

> *22. The requirement that the offence to which a warrant relates be stated in the warrant has its origins in the common law's refusal to countenance the issue of general warrants and its strictly confining any exception to the principle that a person's home is inviolable. General warrants, as their name implies, contain no specification of the object of the search and*

[243] Ibid [155].

[244] (2001) 208 CLR 199, 248–258.

[245] [2020] HCA 14 [124]–[125] (citations omitted).

> *purport to confer a free-ranging power of search. They were described in* Wilkes v Wood *as a discretionary power given to messengers to search 'wherever their suspicions may chance to fall' and as 'totally subversive of the liberty of the subject'. They were infamously used for the purposes of controlling the writing and printing of seditious and radical political works.*
>
> *23. The power to search has always been regarded as an exceptional power, to be exercised only under certain justifying conditions. One essential condition, found in statutes authorising the issue of warrants for search and seizure, both Commonwealth and State and Territory, is that the object of the search be specified by reference to a particular offence.*
>
> *24. In* George v Rockett*, the Court observed that in prescribing conditions governing the issue of search warrants the legislature has sought to balance the need for an effective criminal justice system against the need to protect the individual from arbitrary invasion of their privacy. A person's interest in privacy is recognised in all modern bills of rights and it has achieved a status in international human rights law.*
>
> *25. It may be accepted that the balance struck by the legislature to a greater extent favours the public interest in the investigation and prosecution of crimes. Nevertheless it remains a concern of the legislature, in enacting provisions authorising warrants for search and seizure, to provide a measure of protection to persons affected by a warrant. It does so in large part by ensuring that the object of the warrant is identified by reference to a particular offence and that the limits of the authority to search may thereby be discerned. The courts' insistence on strict compliance with the statutory conditions for a warrant gives effect to this legislative purpose*.[246]

6.9. These statements from the High Court are of particular importance in considering the Department of Home Affairs' submission to me that, because data content must still be obtained by warrant, Schedule 1 powers making that content intelligible or usable do not and should not so require.

6.10. Statutory investigatory powers are required for Government agencies and officials to access, copy or retain private property, including computers, mobile devices and their contents. Further, the principle of legality protects these fundamental rights. It means that these rights are only overcome by clear statutory statement or a

[246] Ibid [22]–[25] (citations omitted).

necessary implication.[247] As was recently said in *Mann v Paterson Constructions Pty Ltd*[248] by Nettle, Gordon and Edelman JJ, 'the principle of legality … requires a clear indication of intent to conclude that legislation abrogates common law rights[249]with the required clarity increasing the more that the rights are "fundamental"[250] or "important"[251].'[252]

6.11. Australia has inherited from English law, and still maintains:

a. a *common law rule* that holders of public office can only seize or access private property as authorised by law

b. the *historically entrenched practice* that this is typically done by warrant, issued by persons independent of the agency which seeks to exercise the warrant.

This rule applies to accessing and copying data content and metadata on personal devices such as computers and mobile phones, just as much as it does to searches of people or premises.

---

[247] *Potter v Minahan* [1908] HCA 63; (1908) 7 CLR 277, 304, states it is 'in the last degree improbable that the legislature would overthrow fundamental principles, infringe rights, or depart from the general system of law, without expressing its intention with irresistible clearness; and to give any such effect to general words, simply because they have that meaning in their widest, or usual, or natural sense, would be to give them a meaning in which they were not really used'. See also *Bropho v Western Australia* [1990] HCA 24; (1990) 171 CLR 1, 18; *Coco v The Queen* [1994] HCA 15; (1994) 179 CLR 42.

[248] [2019] HCA 32.

[249] See and compare *Sargood Bros v The Commonwealth* [1910] HCA 45; (1910) 11 CLR 258, 279 (O'Connor J); [1910] HCA 45; *Pyneboard Pty Ltd v Trade Practices Commission* [1983] HCA 9; (1983) 152 CLR 328, 341 (Mason ACJ, Wilson and Dawson JJ); [1983] HCA 9; *Berowra Holdings Pty Ltd v Gordon* [2006] HCA 32; (2006) 225 CLR 364, 373 [23] (Gleeson CJ, Gummow, Hayne, Heydon and Crennan JJ); [2006] HCA 32.

[250] See, eg, *Bropho v Western Australia* [1990] HCA 24; (1990) 171 CLR 1, 18 (Mason CJ, Deane, Dawson, Toohey, Gaudron and McHugh JJ); [1990] HCA 24; *Coco v The Queen* [1994] HCA 15; (1994) 179 CLR 427, 437 (Mason CJ, Brennan, Gaudron and McHugh JJ), 446 (Deane and Dawson JJ); [1994] HCA 15; *Oates v Attorney-General (Cth)* (2003) 214 CLR 496, 513 [45] (Gleeson CJ, McHugh, Gummow, Kirby, Hayne and Heydon JJ); [2003] HCA 21.

[251] *Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission* [2002] HCA 49; (2002) 213 CLR 543, 553 [11] (Gleeson CJ, Gaudron, Gummow and Hayne JJ); [2002] HCA 49; *Lee v New South Wales Crime Commission* [2013] HCA 39; (2013) 251 CLR 196, 217–218 [29] (French CJ), 310 [313] (Gageler and Keane JJ); [2013] HCA 39.

[252] [2019] HCA 32 [159] (citations in original).

Privacy Act 1988 (Cth)

6.12. At the federal level, the *Privacy Act 1998* (Cth) establishes a series of Australian Privacy Principles (APPs).[253] Those principles regulate how 'APP entities' may deal in the 'personal information' of individuals, which includes their 'sensitive information'.[254] The term 'APP entity' includes both Commonwealth Government agencies and private sector 'organisations' (the latter of which includes, with limited exceptions, sole traders, bodies corporate, partnerships and trusts).

6.13. The Office of the Australian Information Commissioner, an independent statutory office-holder,[255] has promulgated a guideline for the interpretation of the APPs.[256] The Commissioner also performs various other functions under the Privacy Act,[257] including monitoring and advice functions in respect of privacy.

6.14. The Privacy Act recognises that privacy must be balanced with other objectives. The expressed objects of the Act[258] include both 'to promote the protection of the privacy of individuals' and 'to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities'. This is an example of a statutory recognition that the Australian community's legitimate privacy expectations must accept privacy is not an absolute value.

State and Territory charters of rights

6.15. Some Australian States and Territories have introduced their own charters of rights. For instance, both the *Charter of Human Rights and Responsibilities Act 2006* (Vic) and the *Human Rights Act 2004* (ACT) recognise a right to privacy and reputation, in essentially the same terms. Section 13 of the Victorian charter provides that a

---

[253] Contained in Schedule 1 to the *Privacy Act 1998* (Cth).

[254] In each case, as the term is defined in Privacy Act, s 6.

[255] The Office of the Australian Information Commissioner was established by the *Australian Information Commissioner Act 2010* (Cth), s 5(1). That legislation provides for a Privacy Commissioner, distinct from the Information Commissioner, who is to exercise the 'privacy functions' as defined under that Act (which include functions under the Privacy Act): see in particular Part 2, Division 3, of the Act. At the time of drafting this report, the Offices of Information Commissioner and Privacy Commissioner are held by the same person.

[256] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines: Privacy Act 1988* (OAIC, Sydney, 2019) <https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf>.

[257] Privacy Act, Part IV, Division 2.

[258] Ibid s 2A.

person has the right 'not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with' and 'not to have his or her reputation unlawfully attacked'.

Reports by the ALRC and the ACCC

6.16. In 2014, the Australian Law Reform Commission (ALRC) produced a report entitled *Serious Invasions of Privacy in the Digital Era*[259] (the ALRC Report). That report identifies 9 principles that guided its inquiry. They were drawn from 'leading cases in Australia and other comparable jurisdictions, international conventions, academic commentary on privacy and related fields' and from previous ALRC reports.[260] The principles included that:

a. privacy is a fundamental value worthy of legal protection

b. there is a public interest in protecting privacy

c. privacy should nonetheless be balanced against other important interests

d. privacy laws should be adaptable to technological change.[261]

6.17. In 2014, the ALRC Report identified various existing causes of action – some statutory, some at common law – that a person can call on for breach of privacy, including trespass, breach of confidence, improper use of a surveillance device, defamation and harassment. It made recommendations for greater privacy protection.[262] In particular, the ALRC Report recommended the introduction of a statutory tort, in a Commonwealth Act, limited to serious invasions of privacy committed intentionally or recklessly, which cannot be justified in the public interest, and which involve intrusion upon seclusion or misuse of private information.[263] The tort would arise only where the person had a reasonable expectation of privacy.[264]

6.18. That recommendation – not yet adopted – was recently echoed by the Australian Competition and Consumer Commission (ACCC) in its 2019 report on its Digital

---

[259] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Final Report* (Report No 123, 2014) <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/>.

[260] Ibid Ch 2.

[261] Ibid Ch 2, Principles 1, 2, 3 and 5 respectively.

[262] Ibid Ch 3.

[263] Ibid, as summarised at [1.4]; see also discussion and various recommendations in Chs 4 and 5.

[264] Ibid Ch 6.

Platforms Inquiry.[265] The Government's response to the ACCC inquiry indicates it will consider the introduction of a statutory tort of invasion of privacy as part of an intended broader review of the Privacy Act.[266]

6.19. In its Digital Platforms Inquiry report, the ACCC noted the significant amounts of data that consumers routinely give to technology providers.[267] While the ACCC's focus was different from mine, it nonetheless provides useful insights into the circumstances in which Australians provide data to providers.

6.20. The ACCC's 'key findings' on the relationship between consumers and providers of digital platforms (that is, 'online search engines, social media platforms and other digital content aggregation platforms'[268]) include the following:

a. 'Many digital platforms can collect a large amount and variety of data on a user's activities beyond what the user actively provides while they are using the digital platform's services. Digital platforms often have broad discretions in how they use and disclose this data.'

b. 'Several features of consumers' current relationship with digital platforms prevent consumers from making informed choices. They include bargaining power imbalances, information asymmetries between digital platforms and consumers and inherent difficulties for consumers to accurately assess the current and future costs of providing their user data.'

c. 'Many digital platforms seek consumer consents to their data practices using clickwrap agreements with take-it-or-leave-it terms that bundle a wide range of consents.'

d. 'These features of digital platforms' consent processes leverage digital platforms' bargaining power and deepen information asymmetries, preventing consumers from providing meaningful consents to digital platforms' collection, use and disclosure of their user data.'

---

[265] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (Australian Government, Canberra, 2019) Recommendation 19 <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>.

[266] Australian Government, *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Australian Government, Canberra, 2019) <https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf>.

[267] See, in particular, Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (Australian Government, Canberra, 2019) Ch 7, 'Digital Platforms and Consumers'.

[268] Ibid 4, which refers to the Terms of Reference for the inquiry.

6.21. Before reaching conclusions on privacy in Australia, it is instructive to consider aspects of how privacy is protected in the US and the European Union (EU).

Reasonable expectations of privacy in the digital age: the United States

6.22. The US Supreme Court has given detailed consideration to individuals' reasonable expectations of privacy in the digital era and whether they can be said to be voluntarily giving access to all that data simply by conducting their day-to-day business in the digital era. This arises from its ongoing consideration and application of the Fourth Amendment to the *Constitution of the United States*.

6.23. The Fourth Amendment, contained in the Bill of Rights, provides that:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

6.24. The Fourth Amendment was drafted long ago in 'response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity'.[269]

6.25. After a long period when 'Fourth Amendment search doctrine was "tied to common-law trespass"'[270] – indeed, the bedrock principles stated in the UK in *Entick v Carrington* – in 1967, in the case of *Katz v United States*[271] (*Katz*), the US Supreme Court established that the protection conferred by the Fourth Amendment does not 'turn upon the presence or absence of physical intrusion'.[272] In other words, from that point on, it was not necessary to establish a physical trespass in order to make out a violation of the Fourth Amendment.

6.26. Rather, in *Katz*, the Court established that 'the Fourth Amendment protects people, not places'.[273] *Katz* stands for the proposition that, where no trespass had occurred, a violation would nonetheless occur where the conduct in question violated a

---

[269] *Riley v California* 573 US 373 (2014) (*Riley*), cited by Roberts CJ for the Court in *Carpenter v United States* 585 US __ (2018) (*Carpenter*).

[270] *Carpenter* 585 US __ (2018) 5, citing *United States v Jones*, 565 US 400 (2012) (*Jones*) 405, 406, n 3.

[271] *Katz v United States* 389 US 347 (1967) (*Katz*).

[272] Ibid 353.

[273] Ibid 351.

person's 'reasonable expectation of privacy'. In the subsequent case of *Smith v Maryland*,[274] the Court established a two-part test for attracting Fourth Amendment protection, in which (a) a person 'seeks to preserve something as private'; and (b) the person's expectation of privacy is 'one that society is prepared to recognize as reasonable'.

6.27. Significantly for present purposes, the US Supreme Court has held that a person does *not* have a legitimate expectation of privacy in information voluntarily turned over to third parties,[275] even where the person in question had voluntarily made the information in question available to a third party on the assumption that it will only be used for a limited purpose.[276]

6.28. But the spread and evolution of technology has put concepts such as 'reasonable expectation of privacy' and 'information voluntarily made available' under increased strain. In recent years, the US Supreme Court has had to directly confront the question of what information a person in the digital context is said to be making voluntarily available when engaging in everyday activities.

6.29. In 2012, in *United States v Jones*[277] (*Jones*), the US Supreme Court was asked to decide whether, by affixing a GPS tracking device to a vehicle and tracking its movements for 28 days, the Government had violated the Fourth Amendment. As plurality observed,[278] the GPS device generated more than 2,000 pages of data on the vehicle's movements during that period.

6.30. Justice Sotomayor's and Justice Alito's separate concurring opinions focus on the question of reasonable expectations of privacy in the digital age. As each observed, a physical intrusion is no longer necessary for many forms of surveillance.[279]

6.31. Justice Sotomayor said, 'GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations'.[280] She noted that GPS

[274] *Smith v Maryland* 442 US 735 (1979) (*Smith*).

[275] Ibid 743–744.

[276] *United States v Miller* 425 US 435, 443 (1976).

[277] 565 US 400 (2012).

[278] *United States v Jones* 565 US 400 (2012) 2.

[279] Ibid 9–12 (Alito J), 2 (Sotomayor J). This was a point of distinction between the plurality's decision and the concurring Justices' separate opinions, as neither accepted the plurality's analysis that a physical trespass had in fact occurred in this case.

[280] Ibid 3.

tracking allows the Government to obtain, store and later 'mine' data as to a person's movements, with little external oversight.

6.32. She continued:

> *I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.* [281]

6.33. Justice Sotomayor's decision went on to question whether it is indeed still possible to hold that a person has no reasonable expectation of privacy in information voluntarily disclosed to third parties. She observed that:

> *[T]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. … I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.* [282]

6.34. In the 2018 decision of *Carpenter v United States*[283] (*Carpenter*), the US Supreme Court considered what information a person can be said to have voluntarily turned over to third parties in the use of a mobile (cell) phone. The case concerned the use of cell-site location information (CSLI), which permits identification of a mobile phone's approximate location by identifying the sites with which the mobile phone is communicating. Information from several sites permits triangulation, permitting the identification of where a phone is located with much greater accuracy than from one tower alone.

6.35. Through the CSLI records at issue in *Carpenter*, 'the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days – an average of 101 data points per day' and 'prosecutors used the records at trial to show that Carpenter's phone was near 4 of the robbery locations at the time those

[281] Ibid 3–4.

[282] Ibid 4–5.

[283] *Carpenter* 585 US __ (2018).

robberies occurred'.[284] Carpenter was convicted and his appeal eventually reached the Supreme Court.

6.36. Even before *Carpenter*, the Court had considered cell phones in its decision in *Riley v California*.[285] In that case, the Court invalidated warrantless searches of a mobile phone on the basis of the extensive amount of data a mobile phone contains. In *Carpenter*, the information in question was not obtained directly from the person's phone but, rather, from the 'third party' company to whom Mr Carpenter was alleged to have voluntarily made his cell phone location information available.

6.37. The *Carpenter* plurality held the collection of this data amounted to a Fourth Amendment search, rejecting the argument that Mr Carpenter had voluntarily turned it over to a third party. Picking up on the analysis in *Jones*, Roberts CJ, delivering the opinion of the Court, held as follows:

> *As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' These location records 'hold for many Americans the "privacies of life."' And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense … While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.*[286]

6.38. As the opinion continues, 'when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user'.[287] Chief Justice Roberts considered that 'the retrospective quality of the data' gave it even greater force, overcoming the problems that ordinarily 'plague' attempting to reconstruct a person's past movements.

6.39. The decision continues as follows:

> *This case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. … Cell phone location information*

[284] Ibid 1.

[285] 573 US 373 (2014).

[286] *Carpenter* 585 US __ (2018) 12–13 (citations omitted).

[287] Ibid 13.

> *is not truly 'shared' as one normally understands the term. In the first place, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements.*[288]

6.40. The plurality concluded:

> *In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.*[289]

6.41. Even though Australia does not have a Fourth Amendment, for my purposes, *Carpenter* and the statements of authority it cites:

a. show how much information may be revealed by metadata – that is, the statement that it was revealing not only his particular movements but also, through them, his 'familial, political, professional, religious, and sexual associations'[290]

b. establishes that cell-site location information is not to be regarded as voluntarily 'shared', as using a mobile phone is an essential aspect of modern society, and the mere operation of the phone will generate so much information about its user

c. warns that legal rules 'must take account of more sophisticated systems that are already in use or in development'[291]

[288] Ibid 16–17.

[289] Ibid 19.

[290] Ibid 12.

[291] Ibid 14.

d. underlines the fundamental point that consent for privacy invasion given by people to commercial providers does not answer the question 'can the government or its agencies access that same material'.

Reasonable expectations of privacy in the European context

6.42. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU) deal with privacy as follows:

a. Article 7 provides that '(e)veryone has the right to respect for his or her private and family life, home and communications'.

b. Article 8 provides that '(e)veryone has the right to the protection of personal data concerning him or her' and provides that all such data is to be processed on the basis of consent or some legitimate basis prescribed by law.

6.43. The EU has developed data protection policies. In 2019, the European Parliament and the Council of European Union promulgated the General Data Protection Regulation (GDPR).[292] The GDPR replaced the previously existing Data Protection Directive.[293] It supplements the rights to privacy under Articles 7 and 8 of the CFREU.[294]

6.44. The GDPR deals with processing of personal data within or concerning people within the EU and European Economic Area and the transfer of that data out of that area. In broad terms, the GDPR gives 'data subjects' greater control over the collection and use of their personal data. Chapter 3 of the GDPR sets out the privacy rights of 'data subjects'.[295] Those include:

a. rights to know when personal information is being collected from the 'data subject'

b. rights of access to that data

c. rights of rectification for data that is incorrect.

---

[292] General Data Protection Regulation (EU) 2016/679 (available at <https://eur-lex.europa.eu/eli/reg/2016/679/oj>).

[293] Data Protection Directive (EU) 95/46/EC.

[294] Article 8 of the *European Convention on Human Rights* establishes a right to privacy. That provision states that '(e)veryone has the right to respect for his private and family life, his home and his correspondence'. Further, it prohibits a public authority from interfering with the exercise of that right except in limited circumstances. Any such interference must be 'in accordance with the law' and 'necessary in a democratic society in the interests of' such things as national security, public safety, crime prevention or health.

[295] See also Recitals 65 and 66 to the GDPR.

6.45. The GDPR includes detailed requirements for consent to a person's use of data. While consent is only one 'legitimate basis' for processing a person's data, it is highly relevant to a person's legitimate expectations as to the use of his or her personal data. The GDPR states that '[c]onsent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[296]

6.46. The GDPR also provides conditions of valid consent[297] and principles of data processing.[298] Among other matters it requires specific, informed consent for each instance of data processing, and it limits the permissible use of data to that which is required to deliver the good or service in question. In doing so, it limits companies' ability to rely on a consumer's generalised consent from the mere use of a product or service (in the manner which the ACCC describes in the Australian context).

6.47. In addition, Article 17 of the GDPR contains what is commonly known as the 'right to erasure', or the 'right to be forgotten'.[299] Broadly, this comprises an obligation on the part of the entity controlling personal data to erase that data where certain circumstances exist, including, for instance, where the data is no longer necessary for the purpose for which it was required or where the 'data subject' has removed consent for its use.

6.48. The 'right of erasure' or 'right to be forgotten' does not have any direct Australian equivalent. In the 2014 ALRC Report, the ALRC considered but ultimately did not recommend the introduction of an APP that would have that effect.[300] While the ALRC noted its concern that no such APP presently exists, it concluded that the issue was better addressed as part of a broader review of the Privacy Act's operation.[301]

---

[296] Ibid Article 4(11).

[297] Ibid Article 7.

[298] Ibid Recital 39.

[299] A right that first arose in the so-called 'Google Spain' case: *Google Spain SL, Google Inc Agencia Española de Protección de Datos, Mario Costeja González* (2014).

[300] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Final Report* (Report No 123, 2014) [16.44]–[16.56] <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/>.

[301] Ibid [16.56].

What are reasonable expectations of privacy in Australia in the digital era?

6.49. It is difficult to say with any certainty what constitute Australians' legitimate expectations of privacy. I asked a number of witnesses at the public hearings for their understanding of what was meant by 'the legitimate expectations of the Australian community relating to privacy and cybersecurity' in TOLAS's Schedule 1:

a. The Director-General of Security said that 'Australians would have an expectation of privacy … and have expectations of things being secure. Sadly, I think examples almost every day in the press show that that's not the case'.[302]

b. Mr John Howell, from the Australian Human Rights Commission, said that 'the right to privacy may also be subject in some circumstances to legitimate limitations, and that will depend on whether that is necessary to achieve a pressing legitimate objective'.[303]

6.50. The Department of Home Affairs, in guidance it has publicly issued, stated that the phrase 'legitimate expectations' may be interpreted to include factors derived from 'in some cases, opinion polling or media coverage'.[304] TOLA's revised Explanatory Memorandum said that 'all Schedules of the Bill engage the protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR … the purpose of the Bill, and the associated limitations on the right to privacy, are to protect national security, public safety, address crime and terrorism'.[305]

6.51. It is clear from the international instruments, academic discussion and case law that the 'right to privacy' is never absolute when considering access by Government or its agencies to data content or metadata. This is an application of the fundamental principle in this review that just as we do not accept lawlessness in the physical world, we should not accept lawlessness in the virtual world. As a matter of policy, the need to protect national security, provide public safety and address crime will *sometimes* justify intrusions upon privacy. When this occurs, the principle of legality will require those intrusions to be expressed by clear words in the statute or by necessary implication. So much should be uncontroversial.

---

[302] Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 13.

[303] Ibid p 50.

[304] Ibid p 39.

[305] Revised Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth), 9.

6.52. Equally uncontroversial should be the opening remarks by the Encryption Working Group in their report *Moving the Encryption Policy Conversation Forward* that:

> *The working group rejects two straw men – absolutist positions not actually held by serious participants, but sometimes used as caricatures of opponents. These are:*
> *(1) that we should stop seeking approaches to enable access to encrypted information;*
> *(2) that law enforcement will be unable to protect the public unless it can obtain access to all encrypted data through lawful process.*[306]

6.53. The real complexities and difficult policy choices arise at the next stage of analysis. The Encryption Working Group went on to say:

> *We believe it is time to abandon these and other such straw men… More work is necessary, such as that initiated in this paper, to separate the debate into its component parts and examine risks and benefits in greater granularity… There will be no single approach for requests for lawful access that can be applied to every technology or means of communication… Having selected mobile phone encryption as a possible area for further analysis, the working group has identified core principles against which to judge proposals for mobile phone encryption access. The group agrees that proposals should, at a minimum, adhere to these principles [including]…*
>
> - *Law Enforcement Utility: The proposal can meaningfully and predictably address a legitimate and demonstrated law enforcement problem.*
> - *Equity: The proposal offers meaningful safeguards to ensure that it will not exacerbate existing disparities in law enforcement, including on the basis of race, ethnicity, class, religion, or gender.*
> - *Specificity: The capability to access a given phone is only useful for accessing that phone (for example, there is no master secret key to use)*

---

[306] Encryption Working Group, 'Key Takeaways from "Moving the Encryption Policy Conversation Forward"' (Carnegie Endowment for International Peace and Princeton University, September 2019) <https://carnegieendowment.org/programs/technology/cyber/encryption>. The report states:

> *The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.*

> *and that there is no practical way to repurpose the capability for mass surveillance, even if some aspects of it are compromised.*

6.54. As made clear earlier in this report, I also find the example of the mobile device adopted by the working group as a useful focus for discussion. In the public hearings and in my 2020 Lowy Institute address, I raised for consideration the analogy between a traditional personal paper diary and a personal mobile phone. If the police were to seize someone's paper diary, they can be reasonably confident about the writing it contains (and can ask for a photocopy). They will be aware that it will probably contain fingerprints and DNA. Nothing of the sort can be said about a mobile phone seized, especially if passwords to the phone and what is on it are provided to the authorities.

6.55. *First*, the typical mobile phone probably amalgamates the functions that were once performed by several devices: telephone, address book, calendar, internet browser, camera, video camera, calculator, thermometer, pedometer, heart monitor and dictaphone. Depending on how it is used, it can also contain grocery lists, body weight, sleep patterns and purchase records.

6.56. *Secondly*, a typical mobile phone is in fact a very powerful computer containing vast quantities of data. Accessing the content data of a phone is a little like the exercise of a search warrant on premises in the sense that, like the occupier of the premises, the phone owner/user will be specifically aware of some content and broadly aware of the existence of various categories of content.

6.57. *Thirdly*, the mobile phone will contain vast quantities of very revealing information about the phone owner/user not only because of the data content deliberately created by them, such as records of web searches, texts and emails, music and videos, but also data content and metadata created by the device or the applications on it, of which we may know nothing. Such data is an example of the monetisation of personal information. In my 2020 address to the Lowy Institute I said:

> *We suspect, but can never fully know, what the information says about its user. For example, we know the phone maps our physical movements, but I understand that because the way we walk, our gait, is unique, just like our heartbeat, and each is being recorded on the mobile or a mobile watch, it can be shown that it was indeed me using my phone or watch at a particular time and place.*

6.58. *Fourthly*, as the ACCC report on the Digital Platforms Inquiry establishes, it is naïve, if not entirely misconceived, to say that phone owners/users give properly informed consent to the terms and conditions they 'accept' when using a phone or its applications and electronic systems. In fact:

a. they have little if any capacity to negotiate the terms of their use of devices and apps or their access to data on them

b. it may not even be technically possible to ascertain all of the data and metadata created by the owner's or user's use

c. it is not realistic to avoid using the phone or other devices altogether, as these devices are effectively essential to fully participate in Australian life.

6.59. *Fifthly*, I consider that US and EU jurisprudence is right to be sceptical of any idea that, when they use commonplace technology to conduct their day-to-day affairs, individuals are consenting to its use for other purposes or voluntarily providing it to the world at large.

6.60. *Sixthly*, I consider that there is a greater need for the traditional safeguards in the virtual world than in the physical world. That is for reasons of trust and because, as Chapter 4 of this report shows, of the wide and unknown impact of technology. I agree with Professor Peter Leonard's evidence to the public hearing, as part of the evidence from the Law Council of Australia, that:

> *In the digital world, digital trust of citizens is affected by activities that may not relate to their specific digital activities. So we always need to consider, as we look at the digital world, the effect on broader digital trust of citizens, and potentially undermining that trust. Now, often a degree of undermining that trust will be justified in national security or law enforcement, but I do think that you can't take the digital world as an exact analogue of the physical world, because of that different nature of the digital system.*[307]

[307] Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 150. The supplementary submission from the Law Council of Australia states:

> *The Law Council recognises that in some circumstances, it is legitimate for law enforcement agencies to introduce weaknesses or exploit vulnerabilities. However, as noted by Law Council representatives at the public hearing, the concern relating to weaknesses and vulnerabilities in the digital context is that they are more difficult to confine to the purpose of their introduction. … the Law Council considers that the potential implications of systemic weaknesses or vulnerabilities that may be introduced in the course of compliance with a TAR, TAN or TCN are not as easy to identify, target and regulate as the compromise that is inserted into Australia's identity verification system through the creation of an identity document for an assumed identity.*

Conclusion

6.61. Bearing these matters in mind, I conclude that:

a. personal privacy is a fundamental value but not an absolute value that admits of no exceptions

b. it can be outweighed by legitimate public policy aims such as cybersecurity, the detection of serious crime, the prevention of public corruption or the protection of national security

c. the principle of legality requires such policies to be clearly stated or implied in any law allowing search, seizure or access to data content or metadata

d. it is right that the test for determining whether a TOLA Schedule 1 request or notice is 'reasonable and proportionate' requires consideration, among other factors, of 'the legitimate expectations of the Australian community relating to privacy and cybersecurity', but details of those expectations are hard to enunciate. At present, they are one of many factors the decision-maker – agency head for Technical Assistance Requests (TARS) and Technical Assistance Notices (TANs) or ministers for Technical Capability Notices (TCNs) – must weigh up in making a decision but need not explain by reasons published to the Designated Communications Provider in question

e. there is a greater need for the traditional safeguards in the virtual world than in the physical world

f. because of the matters discussed in this report, the absence of an independent decision-maker with access to technical advice so that they fully understand the privacy implications of the exercise of a Schedule 1 power is a matter of real concern, given the normal assumption that warrants affecting privacy must be issued by a knowledgeable person who is, and is seen to be, independent. Whether Schedule 1 of TOLA thus falls short, including of the legitimate expectations of the Australian community, is a matter I discuss later in the report.

7. CONTEXT: AUSTRALIA'S INTERNATIONAL OBLIGATIONS

7.1. Under s 8 of the INSLM Act, I am required to consider Australia's compliance with its international obligations. In the context of TOLA, these international obligations relate to cybercrime and human rights. In this chapter I assess these obligations to inform my view on whether the relevant laws contain 'appropriate safeguards for protecting the rights of individuals'.[308]

International obligation to counter cybercrime

7.2. The *Convention on Cybercrime* of the Council of Europe, known as the Budapest Convention, is, for Australia, the only internationally binding instrument on cybercrime. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties to the treaty.[309] Australia is a party to the Budapest Convention.[310]

7.3. For the purposes of TOLA, those aspects of the Budapest Convention requiring the adoption of legislative and other measures to establish domestic criminal procedural laws are the most relevant. These are dealt with in Section 2 of Chapter II of the Convention and, subject to article-specific limitations or the making of specified reservations, apply to any offence committed by means of a computer system or the evidence of which is in electronic form (Article 15(2)).[311]

7.4. The Explanatory Report to the Budapest Convention explains that it ensures that evidence in electronic form of any criminal offence can be obtained or collected by means of the powers and procedures set out in Section 2. It also ensures an

---

[308] INSLM Act, s 6(1)(b)(i)).

[309] *Convention on Cybercrime*, opened for signature 23 November 2001, CETS No 185 (entered into force 1 July 2004) (Budapest Convention).

[310] [2013] ATS 9. The Budapest Convention entered into force for Australia on 1 March 2013.

[311] Article 14(3)(b) allows a reservation for countries which, due to existing limitations in their domestic law at the time of the Convention's adoption, cannot intercept communications on computer systems operated for the benefit of a closed group of users, which do not use public communications networks and which are not connected with other computer systems. Australia did not make any such reservation.

equivalent or parallel capability for the obtaining or collection of computer data as exists under traditional powers and procedures for non-electronic data.[312]

7.5. The Explanatory Report also notes that all the provisions of Section 2 aim to permit the obtaining or collection of data for the purpose of specific criminal proceedings, noting that there was no consensus on the imposition of an obligation for service providers to routinely collect and retain certain traffic data for a fixed period of time.[313] It is also important to note that nothing in the Budapest Convention requires or invites a Party to establish powers or procedures other than those contained in the Convention. However, equally, it does not preclude a Party from doing so.[314] That is, subject to complying with its other international obligations (such as human rights obligations), it is open to Australia to adopt domestic criminal procedural laws to obtain evidence held on computers and in cyberspace beyond those provided for in the Budapest Convention.

TOLA and the Budapest Convention

Obligations under Article 15 of the Budapest Convention

7.6. Article 15 of the Budapest Convention deals generally with the conditions and safeguards required for the measures in Section 2 of the Convention. It effectively requires the Budapest Convention to be given effect consistently with human rights law.

7.7. The Explanatory Report states that how these powers and procedures are incorporated into domestic legal systems, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. However, those domestic laws and procedures are required to include conditions or safeguards, which may be provided for constitutionally, legislatively, judicially or otherwise, so as to balance the requirements of law enforcement with the protection of human rights and liberties.[315]

7.8. As to what common standards or minimum safeguards are required, the Explanatory Report states that these include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human

[312] See Explanatory Report *Convention on Cybercrime*, CETS No 185 (Explanatory Report), [141].

[313] Ibid [136].

[314] See Budapest Convention, Article 39(3); and Explanatory Report, [131].

[315] Explanatory Report, [145]–[149].

rights instruments. For Australia, the most relevant of these is the *International Covenant on Civil and Political Rights*[316] (ICCPR).

7.9. The Explanatory Report emphasises that another safeguard in the Budapest Convention is that the powers and procedures shall 'incorporate the principle of proportionality'. The report states that proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For non-European States, this means applying related principles of their law, such as limitations on overwide production orders and reasonableness requirements for searches and seizures. The Explanatory Report further states that the explicit limitation in Article 21 (discussed below) that the obligations regarding interception measures only apply in relation to a range of serious offences, determined by domestic law, is an example of the application of the proportionality principle.

7.10. The Explanatory Report also discusses other conditions and safeguards. It states that, without limiting the types of conditions and safeguards that could be applicable, the Convention requires specifically that such conditions and safeguards include, as appropriate in view of the nature of the power or procedure, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. In applying binding international obligations and established domestic principles, it will be up to national legislatures to determine which of the powers and procedures are sufficiently intrusive to require implementation of particular conditions and safeguards. The report states that Parties should clearly apply conditions and safeguards such as these with respect to interception, given its intrusiveness. Other safeguards that should be addressed under domestic law include the right against self-incrimination; and legal privileges and specificity of individuals or places which are the object of the application of the measure.

7.11. Paragraph 3 of Article 15 provides that to the extent that it is consistent with the public interest – in particular, the sound administration of justice – each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties. The report states that consideration of the 'public interest' is of primary importance – in particular, the interests of 'the sound administration of justice'. To the extent consistent with the public interest, Parties should consider other factors, such as the impact of the power or procedure on 'the rights, responsibilities and legitimate interests' of third parties, including service providers, incurred as a result of the enforcement measures; whether appropriate means can be taken to mitigate such impacts; and the sound administration of justice and other public interests (for example, public

[316] Opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976) (ICCPR).

safety and public health and other interests, including the interests of victims and the respect for private life). To the extent consistent with the public interest, consideration would ordinarily also be given to issues such as minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure under Chapter 1 of the Convention, or protection of proprietary interests.

7.12. In this context it is relevant to note that a key concern of many submitters to this review is the lack of judicial or independent oversight of the issuance of interception notices, which, as the Explanatory Report notes, is a measure particularly in need of strong conditions and safeguards due to its intrusiveness.

Obligations under Article 18 of the Budapest Convention

7.13. Article 18 of the Budapest Convention deals with production orders. It states that each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person to submit to those authorities specified computer data in that person's possession or control (stored in particular systems)
b. a service provider offering its services in the territory of the Party to submit to those authorities subscriber information relating to such services in that service provider's possession or control.

7.14. The Explanatory Report states that a 'production order' provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The report also states that this is beneficial to third-party custodians of data, who prefer appropriate legal bases for giving assistance (rather than assisting voluntarily), relieving them of any contractual or non-contractual liability.

7.15. While Schedule 1 of TOLA makes provisions for both voluntary and mandatory industry assistance to Australia's competent authorities, the assistance that can be requested or required under Schedule 1 is not the provision of data or subscriber information. Schedule 1 of TOLA is thus not clearly directed to giving effect to Article 18 of the Budapest Convention.

7.16. Schedule 2 of TOLA establishes powers which enable certain authorities to obtain covert computer access warrants when investigating certain offences. Similarly, however, Schedule 2 is not clearly directed at giving effect to Article 18 of the Budapest Convention.

7.17. No other aspect of TOLA gives effect to these provisions.

Obligations under Article 19 of the Budapest Convention

7.18. The Explanatory Report states that the aim of Article 19(1) is to establish a power relating to stored data equivalent to that which exists for tangible objects. It also states that, in the new technological environment, many of the characteristics of a traditional search remain the same (including the period of the search, the degree of belief required and the fact that the data must already exist and afford evidence of a specific offence). However, additional procedural provisions are necessary to deal with the intangible form of data and the various ways in which it can be accessed and stored (such as an ability to seize the physical medium on which intangible data is stored or to copy that data, or to access data that is not stored on the computer searched but is accessible by it).

7.19. The provisions in Schedule 2 of TOLA conferring an additional power for Commonwealth, State and Territory agencies investigating federal offences punishable by a maximum of 3 years' imprisonment or more to obtain covert computer access warrants may be seen as giving effect to Article 19(1).

7.20. In addition, the provisions in Schedule 2 permitting the temporary removal of a computer or thing from premises for the purpose of executing a warrant may be seen as giving effect to Article 19(3) (although temporary removal is not specifically mentioned in Article 19(3); the list is inclusive, and temporary removal may be seen as necessary to empower competent authorities to seize or similarly secure accessed computer data).

7.21. The amendments relating to allowing the use of any other computer to access target data would also seem to be directed to the same end as the measure described in Article 19(2).

7.22. Further, while no express reference to remote enforcement of search warrants is made in the Budapest Convention, the reference to search or *similar access* could be seen as broad enough to allow for the remote access warrants provided for in Schedule 3 of TOLA.

7.23. The offence of not complying with orders from a judicial officer requiring assistance in accessing electronic devices where a warrant is in force, in relation to which Schedule 3 and Schedule 4 of TOLA are increasing the penalties and which is extended in its application in Schedule 5, would appear to be directed to giving effect to Article 19(4).

7.24. Finally, the amendments in Schedule 4 of TOLA to the search warrant framework to provide the Australian Border Force (ABF) with a power to request a search warrant in respect of a person (rather than a place) for the purposes of seizing a computer or data storage would also appear to fall within the types of legislative and other measures required by Article 19(1).

Obligations under Article 20 and 21 of the Budapest Convention

7.25. Articles 20 and 21 of the Budapest Convention create an obligation for signatory States to empower their authorities in specific ways to manage cybersecurity threats.

7.26. Article 20 deals with real-time collection of traffic data and requires Parties to empower competent authorities to:

a. collect or record through the application of technical means on the territory of that Party

b. compel a service provider, within its existing technical capability

c. collect or record through the application of technical means on the territory of that Party

d. cooperate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.[317]

7.27. Additionally, Article 21 requires each Party to adopt any legislative and other measures that may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party

b. compel a service provider, within its existing technical capability

c. collect or record through the application of technical means on the territory of that Party

d. cooperate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.[318]

---

[317] Article 20(2) provides that where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

[318] Article 21(2) provides that, where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified

7.28. Articles 20 and 21 of the Budapest Convention are particularly relevant to my understanding of Schedules 1 and 2 of TOLA.

7.29. Provisions in Schedule 1 relating to industry assistance measures – specifically, Technical Assistance Requests (TARs) and Technical Assistance Notices (TANs) – could be said to give effect to Articles 20 and 21, to the extent that they create a power for authorities to request and/or compel a service provider (within its existing technical capability) to assist in collection of traffic and content data. Technical Capability Notices (TCNs) would seem to go beyond the obligations in Articles 20 and 21 in that they are directed to ensuring the service provider has particular technical capabilities (that is, it may require them to acquire or develop new equipment or reconfigure their systems).

7.30. In addition, the provisions in Schedule 2 enabling the Australian Security Intelligence Organisation (ASIO) to also intercept communications for the purposes of executing a computer access warrant are arguably consistent with giving effect to Articles 20 and 21.

International obligation in the area of human rights

7.31. The key human rights obligations for Australia which are relevant to TOLA are those found in the ICCPR. Australia is a party to the ICCPR, which entered into force for Australia on 13 November 1980 (except Article 41, which came into force for Australia on 28 January 1993). Australia is therefore under an obligation at international law to give effect to the ICCPR. I consider the 2 key obligations under the ICCPR below.

Obligations under Article 17 of the ICCPR

7.32. Article 17 of the ICCPR sets out the right to privacy:

> 1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> 2. *Everyone has the right to the protection of the law against such interference or attacks.*

7.33. In Resolution 68/167, adopted in 2013, the United Nations General Assembly (UNGA) emphasised that:

---

communications transmitted in its territory, through the application of technical means on that territory.

> *unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society.*[319]

7.34. The UNGA called on all States to respect and protect the right to privacy, including in the context of digital communication.[320] It called on all States to review their procedures, practices and legislation on the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.[321]

7.35. The UN High Commissioner for Human Rights has emphasised that encryption secures a 'zone of privacy' that enables individuals to develop and share opinions through corresponding online, and by other, digital media.[322]

Obligations under Article 19 of the ICCPR

7.36. Article 19 of the ICCPR, dealing with the right to freedom of expression, is also relevant to the present Review:

> 1. *Everyone shall have the right to hold opinions without interference.*
> 2. *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
> 3. *The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
>
> a. *For respect of the rights or reputations of others;*

---

[319] *The Right to Privacy in the Digital Age*, GA Res 68/167, UN GAOR, 68th sess, Agenda Item 69(b), UN Doc A/RES/68/167 (18 December 2013) 2.
[320] Ibid.
[321] Ibid.
[322] David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HR/29/32 (22 May 2015).

b. For the protection of national security or of public order, or of public health or morals.

7.37. In General Comment No 34, the Human Rights Committee notes that '[f]reedom of opinion and freedom of expression are indispensable conditions for the full development of the person. They are essential for any society'.[323]

7.38. However, freedom of speech is not an absolute right and can be limited, as indicated in Article 19(3). Any limitation must be lawful, necessary and proportionate to achieve a legitimate objective within the scope of Article 19(3).[324]

7.39. The UN High Commissioner for Human Rights has also stated that the 'zone of privacy' that encryption and anonymity provide individuals and groups when online allows these people to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks.[325]

Permissible limitations on human rights

7.40. Some human rights are non-derogable – that is, they cannot legitimately be subject to any limitation (for example, the freedom from torture and other cruel, inhuman or degrading treatment or punishment in Article 7 of the ICCPR). None of these rights are directly raised in this review.

7.41. However, other human rights (including the rights to privacy and freedom of expression) can be limited where certain criteria are met. Such derogations must not be arbitrary and must not jeopardise the essence of the right. The Human Rights Committee has stated that 'arbitrariness' must not be equated with 'against the law' but be interpreted more broadly to include such elements as inappropriateness and injustice.[326]

7.42. Human rights may be limited in situations where the limitation is reasonable, necessary and proportionate to achieving a legitimate aim.[327] Certain prescribed

---

[323] United Nations Human Rights Committee, *General Comment No 34, Article 19: Freedoms of Opinion and Expression*, 102nd sess, Un Doc CCPR/C/GC/34 (12 September 2011) 1.

[324] Ibid 7; Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 12.

[325] David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HR/29/32 (22 May 2015) 7.

[326] United Nations Human Rights Committee, Communication No 560/1993, 59th sess, UN Doc CCPR/C/59/D/560/1993 (30 April 1997) ('A v Australia') [7.6].

[327] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other*

purposes or legitimate aims relevant to particular rights may include national security, public order, public health, public morals and rights and freedoms of others.

Legitimate aims

7.43. The High Commissioner for Human Rights has stated that surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a measure that serves a 'legitimate aim'. However, the degree of interference must be assessed against the necessity of the measure to achieve that aim and the actual benefit it produces towards such a purpose.[328]

7.44. As the submission by the Australian Human Rights Commission (AHRC) sets out, the *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (Siracusa Principles) state that national security cannot be used as a 'pretext for imposing vague or arbitrary limitations and may only be invoked when there exist adequate safeguards and effective remedies against abuse'.[329] The Siracusa Principles also state that '[n]ational security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force'.[330] Additionally, '[n]ational security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order'.[331]

7.45. The aim of 'public order (*ordre public*)', which is referred to within a number of articles as a legitimate aim, by reference to which a non-derogable right may be limited, is also relevant in the context of TOLA. The expression 'public order' as used in the ICCPR can be defined as the sum of rules which ensure the functioning of society or the set of fundamental principles on which society is founded. It is a broader concept than national security, and is to be interpreted in the context of

---

Legislation (Assistance and Access) Act 2018 (TOLA), 16 October 2019, 13; see also example Mr Howell's evidence on behalf of the Human Rights Commission: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 35.

[328] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) 8 [34].

[329] UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, E/CN.4/1985/4 (28 September 1984) 8 [31].

[330] Ibid 8 [29]

[331] Ibid 8 [30]

the purpose of the particular human right which is limited on this ground.[332] Maintaining 'public order' is the rationale underlying much of the criminal law.

Necessity

7.46. The Siracusa Principles state that, when a limitation is required, in the terms of the ICCPR, to be 'necessary', this term implies that the limitation is based on one of the grounds justifying limitations:

a. recognised by the relevant article of the ICCPR, which

b. responds to a pressing public or social need, which

c. pursues a legitimate aim, and

d. is proportionate to that aim.[333]

A State should not use more restrictive means than are required to achieve the purpose of the limitation.

Proportionality

7.47. The Human Rights Committee has stated:

> *Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected. The principle of proportionality has to be respected not only in the law that frames the restrictions, but also by the administrative and judicial authorities in applying the law.*[334]

Consistency of TOLA with engaged human rights obligations

7.48. This section sets out key features of the amendments in TOLA that engage the human rights obligations and outlines concerns that have been raised with me and

---

[332] Ibid [23]; Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights, Cases, Materials and Commentary* (Oxford University Press, 3rd Edition, 2013) 617.

[333] UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, E/CN.4/1985/4 (28 September 1984) [10].

[334] United Nations Human Rights Committee, *General Comment No 27: Article 12 (Freedom of Movement)*, 67th sess, UN Doc CCPR/C/21/Rev.1/Add.9 (2 November 1999) 3 [13]–[14].

the Parliamentary Joint Committee on Intelligence and Security (PJCIS) about the consistency of these amendments with Australia's human rights obligations.

7.49. To the extent that these amendments also give effect to the Budapest Convention, these concerns will also be relevant to an assessment of the consistency of the amendments and their implementation with the obligation in Article 15 of the Budapest Convention to establish, implement and apply the domestic criminal procedural law powers required in Section 2 of that Convention subject to conditions and safeguards that provide for the adequate protection of human rights and liberties.

Schedule 1

7.50. In its Statement of Compatibility for TOLA (the Statement) the Australian Government properly acknowledged that TARs, TANs and TCNs engage and may limit a number of human rights, including the right to privacy, the right to freedom of expression and the right to an effective remedy. However, it states that they represent permissible limitations on those rights.[335]

7.51. As noted in the Statement, the measures engage the right to privacy because, as a consequence of those notices, 'communications providers may facilitate law enforcement, security and intelligence agencies' access to private communications and data where an underlying warrant or authorisation is present'.[336] There may be associated issues with this, such as the breadth of the powers, the duration of the notices/requests and the decision-making criteria.

7.52. As acknowledged in the Statement, the measures may engage the right to freedom of expression 'by indirectly making some people more reluctant to use communications services'. This is because:

> *It is plausible that a person may minimise their use of communications services if they believe government agencies can ask providers to facilitate access to communications carried through these service, for example by removing forms of electronic protection applied to their communications if they are capable of doing so.*[337]

7.53. Given that the right to privacy and to freedom of expression are engaged, it is necessary to consider whether these measures pursue a legitimate aim and are necessary and proportionate to that aim.

---

[335] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth), 9–14.
[336] Ibid 9 [8].
[337] Ibid 14 [40].

7.54. The PJCHR, quoting the Statement, states that 'the bill pursues the legitimate objective of protecting national security and public order by addressing crime and terrorism', specifically referring to 'terrorism, espionage, acts of foreign interference and serious and organised crime'.[338]

7.55. In its initial analysis, the PJCHR stated that further information was required to establish a pressing and substantial concern justifying the use of TARs, TANs and TCNs, for the purposes of international human rights law.[339] The PJCHR sought the advice of the Minister as to the compatibility of the measures with the right to privacy and freedom of expression.

7.56. The Explanatory Memorandum to the Bill states:

> *The increasing use of encryption has significantly degraded law enforcement and intelligence agencies' ability to access communications and collect intelligence, conduct investigations into organised crime, terrorism, smuggling, sexual exploitation of children and other crimes, and detect intrusions into Australian computer networks. … The Bill will enhance cooperation by introducing a new framework for industry assistance, including new powers to secure assistance from key companies in the communications supply chain both within and outside Australia (Schedule 1).*[340]

7.57. With regard to a legitimate objective, the PCJHR's report quoted part of the Minister's response:

> *Measures employed by serious criminals and terrorists include, but are not limited to, communication devices with military grade encryption, remote-wipe capabilities, duress passwords, and secure cloud-based services. Beyond traditional communications platforms, online-only services now provide unprecedented secure connection and storage that enable the easy sharing, promotion and discussion of illicit material, such as child pornography. During development of the Bill, the government identified that 95 per cent of ASIO's most dangerous counter-terrorism targets use encrypted communications. Additionally, encryption has directly impacted around 200 operations conducted by the AFP in the last 12 months, all of which related to the investigation of serious criminality and terrorism offences.*[341]

---

[338] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 55.

[339] Ibid 29.

[340] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth), 2.

[341] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 57–58.

7.58. The Minister's response also stated:

> *The increasing use of encryption is symptomatic of a more dramatic change in the communications environment. It is enabled by the growing digitisation of communications and presence of new providers who, unlike traditional domestic carriers and carriage service providers, remain largely unregulated in the Australian market. The new spread and scope of providers and the multiple different ways for communications to be constructed and transmitted require agencies to work with multiple other entities in the communications supply chain to achieve investigative results …*
>
> *Decryption is only part of a solution, and is not possible or desirable in some circumstances. It may provide a better outcome to allow agencies access to communications at a point where data is unencrypted (via schedule 2), have longer to examine a computer (schedule 3 and 4), or to receive technical assistance from a directly relevant designated communications provider (DCP) …*
>
> *[T]he 'problem' to be overcome is not the use of encryption itself, but the degradation of agencies' access to existing methods of obtaining communications. Viewed through this lens, the measures of all schedules of the Bill can be seen as directed towards the objective of assisting agencies to restore the balance of access to communications that Parliament has seen fit to provide.*[342]

7.59. The PJCHR stated that, in light of the Minister's responses, the measures in Schedule 1 appear to pursue a legitimate objective for the purposes of international human rights law.[343]

7.60. In its submission to this review, the Department of Home Affairs stated:

> *It is essential that when interferences with privacy occur – online or offline – they occur consistently with the rule of law set down prospectively to ensure the application of the rules is not arbitrary or capricious, and that procedural fairness and natural justice are afforded to those under investigation. The Assistance and Access Act – in so far as it facilitates lawful interference with privacy that is authorised by other investigative powers – is one aspect of the rule of law that makes it permissible to abrogate individual privacy for legitimate purposes.*

---

[342] Minister for Home Affairs, Response to the Parliamentary Joint Committee on Human Rights, 2 November 2018.

[343] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 59.

> *This position finds precedent in international human rights law which recognises the right to privacy may be limited for the legitimate purposes of enforcing the criminal law, assisting the enforcement of criminal laws in a foreign country, the interests of national security, foreign relations or economic wellbeing. The Assistance and Access Act's safeguards and thresholds ensure that the law may only impose limitations on the right to privacy where it does so for one of these legitimate purposes.*[344]

7.61. In its submission to the INSLM, the Australian Federal Police stated:

> *The tempo and complexity of the criminal threat environment driving the operational urgency of the reforms in 2018 has not abated. The TOLA Act strengthens the AFP's ability to overcome technological impediments to our lawful access to digital content.*
>
> *Communication technology and encryption underpins everyday modern communications and is advancing at an incredible rate and is contributing to the creation of ungovernable space, free from the rule of law.*[345]

7.62. Initially, the PJCHR had questions about the types of agencies that may obtain technical assistance and whether empowering certain agencies would be effective to achieve the objectives of the Bill. However, in its more recent report, the PJCHR stated that empowering agencies that investigate Australia's most serious criminal offences with the ability to procure technical assistance in investigating serious crime and terrorism appears rationally connected with (that is, effective to achieve) the Bill's objectives of protecting national security and public order.[346]

7.63. The PJCHR was also concerned as to whether all 'acts or things' that may be specified in a TAR, TAN or TCN are rationally connected to the stated objectives of the measures.[347] However, after the Minister provided additional information, in its more recent report the PJCHR stated that this appears to demonstrate rational connection between the listed acts or things and the objectives of the Bill.[348]

---

[344] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 10.

[345] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, 9.

[346] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 59.

[347] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 11 of 2018, Parliament of Australia, Canberra, October 2018) 30.

[348] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, 2018) 59–61.

7.64. The initial PJCHR report stated that, in terms of proportionality, measures that restrict the right to privacy and freedom of expression must be no more extensive than is strictly necessary to achieve their stated objective.[349] In its most recent report, the PJCHR stated that the Minister's response goes some way towards explaining why the measures are necessary, by reference to how technical barriers impede lawful access to information granted pursuant to a warrant or authorisation, and how existing obligations for industry to assist with overcoming those barriers are 'inadequate'. However, it then stated that, having explained why the measures are necessary, the Minister's response does not address whether the measures are no more extensive than is necessary to achieve the objectives of the Bill; it does not address whether the measures adopt the least rights-restrictive approach, in order to satisfy the requirements of proportionality for the purposes of justifying a restriction on rights under international human rights law.[350]

7.65. Further, where grounds for TARs include 'the interests of Australia's foreign relations or Australia's economic well-being', the PJCHR questioned whether these grounds fall within those on which the right to freedom of expression can be validly restricted and whether this measure is sufficiently circumscribed.[351] The AHRC also questioned whether the 'relevant objectives' are too broad.[352] In its evidence during the public hearing, Electronic Frontiers Australia stated that there was an insufficient consideration of public interest in relation to TANs, TARs and TCNs.[353]

---

[349] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 11 of 2018, Parliament of Australia, Canberra, 2018) 31

[350] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 61; see also Mr Murray's evidence on behalf of Electronic Frontiers Australia, 70; and Ms Krahulcova's evidence on behalf of Access Now, 97, in Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript.

[351] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 62.

[352] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 24; see also Mr Howell's evidence on behalf of the Human Rights Commission: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 36.

[353] See Mr Murray's evidence on behalf of Electronic Frontiers Australia: Independent National Security Legislation Monitor, Review of the

7.66. The PJCHR also expressed concern about safeguards, including whether there were sufficient safeguards for TARs, the effectiveness of any consultation period, and whether there is the possibility of oversight and the availability of review. The report particularly stated that, in terms of ensuring the impact on individual rights is proportionate for the purposes of international human rights law, the availability of judicial review for providers does not appear to be an adequate safeguard.[354] Likewise, the Minister's response did not address the questions raised regarding whether the mandatory 28-day consultation period prior to issue of a TCN is an adequate safeguard. The AHRC also expressed as a key concern the lack of a requirement for judicial authorisation for assistance notices.[355]

7.67. Concerns have also been expressed regarding the breadth of 'acts or things' compelled and the operation of s 317ZH ('Limits on TARs, TANs and TCNs'), as well as the operation of s 317ZG (relating to the definition of systemic weaknesses or vulnerabilities).[356]

7.68. The PJCHR concluded that, while TARs, TANs and TCNs pursue a legitimate objective and are likely to be rationally connected to that objective, the current regime is unlikely to constitute a proportionate limitation on the rights to privacy and freedom of expression and is therefore likely to be incompatible with those rights.[357]

Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 (TOLA), Public Hearing Transcript, 70.

[354] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 65.

[355] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019.

[356] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 65–69. See also Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 19; Dr Chris Culnane and Associate Professor Vanessa Teague, Submission No 28 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 9 October 2019, 2–3. See also Mr Murray's evidence on behalf of Electronic Frontiers Australia, 70; Professor Leonard's evidence on behalf of the Law Council, 143; and Mr Ragland's evidence on behalf of BSA The Software Alliance, 170, in Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript.

[357] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 69.

7.69. The legitimacy of the objective is supported by the fact that, relevantly, these amendments could be said to be giving effect to Articles 20 and 21 of the Budapest Convention. The Explanatory Report to the Budapest Convention emphasises the importance of stringent safeguards given the intrusiveness of the interception of content data. However, it notes that the Convention itself does require many specific safeguards in relation to the powers and procedures related to real-time interception of content data. Nonetheless, the Explanatory Report lists as relevant safeguards judicial or other independent supervision; specificity as to the communications or persons to be intercepted; necessity; subsidiarity and proportionality (for example, legal predicates justifying the taking of the measure; other less intrusive measures not effective); limitation on the duration of interception; and right of redress. Therefore, the relevant question remains whether sufficient and effective safeguards are in place in respect of the powers to issue TARs, TANs and TCNs.

7.70. Furthermore, in its submission, the Office of the Victorian Information Commissioner raised concerns about an administrative decision-maker's ability to fully understand the wider security risks in issuing a TAR, TAN or TCN, when considering the legitimate expectations of the Australian community relating to privacy and cybersecurity as part of assessing the reasonableness and proportionality of a TAR, TAN or TCN.[358] In evidence given at the public hearing, Access Now stated that the technical impact of what a TCN seeks to do is not weighed in the decision-making and that this would not fall under reasonable expectations of privacy in cybersecurity on the part of Australians.[359]

7.71. In its initial report, the PJCHR also considered the measures in relation to the right to an effective remedy and expressed concern about how anyone could pursue judicial review of a decision to issue a TAN or TCN if they are not aware that a notice has been issued. Further, if an act or thing done by a provider in compliance with a TAR involves a breach of human rights, this could raise concerns about the availability of an effective remedy. In its most recent report, the PJCHR stated that the Minister's response did not address the right to an effective remedy for persons whose rights are impacted by a provider's compliance with a TAR but against whom no criminal proceedings are brought. It is also noted that, while the remedy available

[358] Office of the Victorian Information Commissioner, Submission No 7 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 13 September 2019, 3.

[359] See Ms Krahulcova's evidence on behalf of Access Now: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 99.

may prevent use of evidence unlawfully or improperly obtained, it may not provide a remedy for the original violation of the right to privacy, as a provider receives immunity from civil liability for an act or thing done pursuant to a TAR.[360] Additionally, the Minister's response did not address the concern about how a natural person could pursue judicial review where they may not know a notice has been issued.[361] The PJCHR therefore stated that it is unable to conclude that the measure is compatible with the right to an effective remedy.[362]

7.72. Agency submitters have contended that these powers are proportionate to any threat of terrorism or threat to national security. The Australian Signals Directorate (ASD), for example, wrote that these arrangements provide appropriate mechanisms to ensure that any requests made by ASD are a proportionate response to the cybersecurity threat and that the measures provide another avenue for industry and ASD to voluntarily cooperate on cybersecurity.[363] After setting out the safeguards present in relation to Schedule 1, ASIO stated that legislation that supports ASIO's ability to meaningfully engage with Australia's communications providers will remain essential to ASIO fulfilling its function of investigating matters of relevance to security.[364]

7.73. Other submitters maintained that the Department of Home Affairs has not sufficiently addressed the compromises to security and privacy that may occur.[365]

Schedule 2

Computer access warrants

7.74. In its initial report, the PJCHR sought the advice of the Minister as to the compatibility of the measures with the right to privacy, including whether there is reasoning or evidence that establishes that each of the measures addresses a

[360] Ibid 94–95.

[361] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 69–71.

[362] Ibid 70.

[363] Australian Signals Directorate, Submission No 2 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 September 2019, 3–4.

[364] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, 7.

[365] See, for example, Senatas, Submission No 6 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 13 September 2019, 1.

pressing or substantial concern, or whether the proposed changes are otherwise aimed at achieving a legitimate objective. The Minister responded:

> *Traditionally, the* Surveillance Devices Act 2004 *(Cth) (SD Act) has permitted a range of devices such as mobile phones to be accessed via warrant. However, this warranted access has so far only enabled 'view only' access. Essentially, once the surveillance device is installed on the mobile phone, law enforcement currently cannot access files or file structure, only view what the person of interest is currently doing. With the incredible uptake of technology, this is becoming increasingly restrictive to law enforcement efforts. For example, a person who accesses child sexual abuse material may have large collections on their device and is sharing with individuals overseas. This information may not be easily detected purely through read only viewing of the device. The added complexity of encryption means that accessing data on the phone both within the file structure of the device and before encryption takes place can be key to obtaining vital evidence to investigate and prosecute serious crime.*
>
> *…*
>
> *These changes modernise the evidence and intelligence collection capabilities of Australia's key agencies and will facilitate the lawful collection of data in a more accessible state.*[366]

7.75. In light of this information, the PJCHR was satisfied that the measures seek to address a pressing and substantial concern such that the measures pursue the legitimate objective of protecting national security and public order (and that they are rationally connected).[367] This conclusion is supported by the fact that these measures appear in part to give effect to Article 19 of the Budapest Convention. However, the question remains whether sufficient conditions and safeguards are in place to ensure these measures are consistent with Article 15 of the Budapest Convention and the ICCPR.

7.76. In relation to interference with data, the PJCHR acknowledged that the provisions of the Bill that provide for judicial issuing of (some) warrants provide an important safeguard against abuse. However, it also stated that judicial authorisation alone is not necessarily sufficient to ensure compliance with the right to privacy, and it suggested some further safeguards. The PJCHR therefore had remaining concerns that the proposed computer access warrant scheme may not be a proportionate limitation on the right to privacy.[368]

---

[366] Minister for Home Affairs' response to the PJCHR, November 2018.

[367] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 77.

[368] Ibid 78 and 81.

7.77. In relation to emergency authorisations, the PJCHR stated that there are a number of safeguards in place. However, it also noted that there are concerns regarding the treatment of information where a decision-maker does not subsequently approve the authorisation, and also with using information that has been improperly obtained to pursue an investigation. It remained concerned that these provisions were incompatible with the right to privacy.

7.78. The PJCHR therefore concluded that there is a risk that the proposed computer access warrant scheme in the *Surveillance Devices Act 2004* (Cth) (SD Act) may be incompatible with the right to privacy, due to the extent of the impact on privacy. However, noting the requirements for a decision-maker issuing the warrant to consider the extent to which the privacy of persons is likely to be affected and the existence of any alternative means of obtaining evidence, the PJCHR concluded that much will depend on how the computer access warrant scheme operates in practice. The PJCHR recommended that the scheme be monitored to ensure that any limitation on the right to privacy be only as extensive as is strictly necessary to achieve the legitimate objectives of the Bill.[369]

7.79. In relation to the right to a fair trial and fair hearing, the PJCHR considered that s 47A[370] may be compatible with the right to a fair trial and fair hearing. However, the PJCHR recommended that the operation of this provision be monitored to ensure that a defendant affected by the measure has sufficient information available to be able to prepare a defence.[371]

7.80. The PJCHR also expressed concern about the compatibility of the use of force power with multiple rights. It noted that the use of force provisions in proposed s 27E(6) of the SD Act[372] engage and may limit the right to privacy and the right to life. They

---

[369] Ibid 81.

[370] Which states in part:

> *(1) In a proceeding, a person may object to the disclosure of information on the ground that the information, if disclosed, could reasonably be expected to reveal details of computer access technologies or methods.*
> *(2) If the person conducting or presiding over the proceeding is satisfied that the ground of objection is made out, the person may order that the person who has the information not be required to disclose it in the proceeding.*
> *(3) In determining whether or not to make an order under subsection (2), the person conducting or presiding over the proceeding must take into account whether disclosure of the information:*
> *(a) is necessary for the fair trial of the defendant; or*
> *(b) is in the public interest.*

[371] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 84.

[372] Which provides:

may also engage the prohibition on torture, cruel, inhuman and degrading treatment or punishment. The PJCHR stated that the requirement that a decision-maker (a judge or AAT member) may only authorise force that is 'necessary and reasonable' pursuant to a computer access warrant may be a sufficient safeguard. This may ensure compatibility with the prohibition on torture, cruel, inhuman and degrading treatment or punishment, the right to life and the right to privacy. However, much will depend on how the use of force power operates in practice. The PJCHR recommended that the operation of the use of force power be monitored to ensure that it occurs in a manner compatible with human rights.[373]

7.81. The PJCHR discussed the engagement of a number of human rights relating to control orders. This includes the right to equality and non-discrimination, the right to liberty, the right to freedom of movement, the right to a fair trial and fair hearing, the right to privacy, the right to freedom of expression, the right to freedom of association, the right to protection of the family, the right to work, the right to social security and an adequate standard of living, and the rights of children.[374] The right to an effective remedy may also be engaged here, in relation to the provisions that preclude criminal liability for persons who exercised powers relating to the control order computer access warrant if the control order is declared void, as well as the provision which allows for the use of information obtained under the warrant even if the order is declared void.[375] In its most recent report, the PJCHR stated that it is unable to conclude that control order computer access warrants are compatible with human rights and noted that the Minister's response did not fully address the Committee's inquiries in relation to these complex issues.[376]

---

(6) A computer access warrant must:
(a) authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant; and
(b) if the warrant authorises entering premises – state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

[373] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 87.

[374] I have earlier considered control orders: Independent National Security Legislation Monitor, *Review of Divisions 104 and 105 of the Criminal Code (including the interoperability of Divisions 104 and 105A): Control Orders and Preventative Detention Orders* (Report No 3, 2017).

[375] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 11 of 2018, Parliament of Australia, Canberra, October 2018) 50–51.

[376] Control orders have been considered in previous INSLM reports: see Dr James Renwick CSC SC, Independent National Security Legislation Monitor, *Review of Divisions 104 and 105 of the Criminal Code (including the interoperability of Divisions 104 and 105A): Control Orders and Preventative Detention Orders* (Report No 3, 2017).

7.82. Some submitters maintained that this framework remains proportionate. For example, ASIO stated that the existing legal framework for the issuing of ASIO warrants provides robust assurance, accountability and oversight mechanisms. It also stated that it considers that the new powers in Schedule 2 of TOLA provide an update to ASIO's computer access warrant regime necessary to keep pace with technology.[377]

Concealment of access powers

7.83. The PJCHR commented that concealment of access powers in the proposed amendments to the SD Act and the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) engage and limit the right to privacy. In its most recent report it concluded that the concealment of access powers are likely to be incompatible with the right to privacy, noting that there will be no opportunity for the target or the third party to know whether access occurs in accordance with the terms of the warrant and also the fact that an authority could remain in force for a substantial period of time.[378]

Powers to compel persons to assist officers to access data and devices

7.84. These measures engage and limit the right to privacy in that that they enable certain officers and agencies to access private communications and other information on a person's device. The stated objective for the measures is the protection of national security and public order.[379]

7.85. The Minister's response to the initial analysis of the PJCHR stated that current assistance order powers are significantly outdated, as they can only be issued pursuant to a premises search warrant, while noting the broader importance of assistance orders in criminal investigations. In terms of proportionality, the Minister emphasised the judicial authorisation process. However, the PJCHR stated that the Minister's response did not address its concerns about whether the measures are

---

[377] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, –10.

[378] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 92; see also, for example, Mr Howell's evidence on behalf of the Human Rights Commission: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 36.

[379] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth), 26 [126]; Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 11 of 2018, Parliament of Australia, Canberra, October 2018) 55.

sufficiently circumscribed (including the fact that a broad range of persons may be compelled to assist). It therefore stated that it remains unclear whether it is proportionate for the broader categories of persons (which is a particular concern regarding the penalties for noncompliance). This again appears to overlap with the question of whether these measures would be consistent with Article 19(4) of the Budapest Convention, read with Article 15.

7.86. The PJCHR stated that it is unable to conclude that the assistance order provisions in Schedules 2, 3, 4 and 5 are compatible with the right to privacy.[380]

7.87. The AHRC has also expressed concern about whether a person subject to an assistance order is effectively being detained during the period in which they are required to provide the assistance, which might engage the prohibition on arbitrary detention.[381]

Interception of communications under ASIO computer access warrants

7.88. The interception of communications under ASIO computer access warrants engages the right to privacy because interception (including interception to enable remote access to a computer) is 'inherently privacy intrusive'.[382] Noting the lower threshold for the issuing of warrants under the ASIO Act when compared with the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), the potentially significant impact on the right to privacy, and the fact the regime is overseen by the Attorney-General and not by judicial authorisation, the PJCHR stated that it remained unclear whether this was the least rights restrictive approach. It stated that there is a significant risk that the proposed amendments to ASIO computer access warrants to allow ASIO to intercept a communication passing over a telecommunications system may be incompatible with the right to privacy. It recommended that the scheme be monitored to ensure that any limitation on the right to privacy be only as extensive as is strictly necessary to achieve the legitimate objectives of the measure.[383] Given that this measure could be seen as giving effect

---

[380] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 94–96.

[381] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 28.

[382] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth), 15 [50]; Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 11 of 2018, Parliament of Australia, Canberra, October 2018) 58.

[383] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 100–101.

to some extent to Articles 20 and 21 of the Budapest Convention, it is relevant to consider the types of conditions that have been considered desirable in that context.

Assistance to foreign countries in relation to data held in computers

7.89. In its report, the PJCHR noted that it had previously raised concerns regarding the human rights implications of Australia's mutual legal assistance scheme in relation to the right to liberty; the right to life; the prohibition against torture and cruel, inhuman and degrading treatment; the right to a fair hearing; the right to equality and non-discrimination; and the right to an effective remedy.[384]

7.90. The PJCHR reiterated its previous concern as to the human rights compatibility of allowing assistance to be given to a foreign country, even if the death penalty may apply, if there are 'special circumstances' and that there is no explicit obligation to consider whether a person may be subject to cruel, inhuman or degrading treatment or punishment. In the absence of these safeguards, the PJCHR considered that there is a risk that the proposed amendments to the *Mutual Assistance in Criminal Matters Act 1987* (Cth) (MACM Act) in Schedule 2 of the Bill may be incompatible with human rights, noting, however, that much will depend on how the applicable safeguards operate in practice.

7.91. As discussed above, these provisions related to the MACM Act can be said to give effect to Article 25 (and possibly Article 31 in relation to stored computer data) of the Budapest Convention.

7.92. The PJCHR also reiterated its previous view that the MACM Act would benefit from a full review of the human rights compatibility of the legislation, as it raises human rights concerns in relation to the right to liberty; the right to life; the prohibition against torture and cruel, inhuman and degrading treatment; the right to a fair hearing; the right to equality and non-discrimination; and the right to an effective remedy.[385] This view is relevant to the view I expressed above that a good faith interpretation of the relevant Budapest Convention provisions would assume that these mutual assistance obligations would be fulfilled in a manner that is consistent with Australia's human rights obligations.

---

[384] Ibid 63.

[385] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 13 of 2018, Parliament of Australia, Canberra, December 2018) 108–109.

Schedules 3 and 4

Power for law enforcement and Australian Border Force to access computers remotely

7.93. The PJCHR raised questions about whether the proposed power of law enforcement agencies and the ABF to access computers remotely was compatible with the right to privacy. In its most recent report, it stated that there is a risk that remote access of computers pursuant to a warrant under the *Crimes Act 1914* (Cth) and the *Customs Act 1901* (Cth) may be incompatible with the right to privacy. However, noting the safeguards that apply before law enforcement and the ABF may access computers remotely, the PJCHR stated that much will depend on how the scheme operates in practice. It recommended that the scheme be monitored to ensure that any limitation on the right to privacy is only as extensive as is strictly necessary to achieve the legitimate objectives of the Bill.

Power for Australian Border Force to search persons who may have computers or devices under the Customs Act

7.94. The PJCHR raised questions as to the compatibility of this power with the right to privacy, including the proportionality of the limitation on this right, and whether the proposed safeguards will be effective to limit the impact on the right to privacy of third parties who are lawful users of the computer or device subject to the warrant.[386]

7.95. The PJCHR stated that safeguards on the issue of a warrant authorising an ordinary search or a frisk search of a person by the ABF may be capable, in practice, of ensuring that the limitation on the right to privacy of persons subject to an ordinary or frisk search is proportionate. However, again, it stated that much will depend on how the scheme operates in practice. It recommended that the scheme be monitored to ensure that any limitation on the right to privacy is only as extensive as is strictly necessary to achieve the legitimate objectives of the Bill.

7.96. The PJCHR raised questions about whether the amendments to the Crimes Act and Customs Act which allow electronic devices moved under warrant to be kept for analysis for 30 days were compatible with the right to privacy. It stated that the proposed amendments to the Crimes Act and Customs Act which extend the time allowed for electronic devices moved under warrant to be kept for analysis for up to 30 days may be compatible with the right to privacy. However, it is noted that the Minister's response did not explain why extending the time period to 30 days represented the least rights-restrictive approach, so there is a risk that the measures may not constitute a proportionate limitation on the right to privacy in an individual

[386] Ibid 113.

case. It is suggested the scheme be monitored to ensure that any limitation on the right to privacy goes only as far as is strictly necessary to achieve the legitimate objectives of the measure.

Schedule 5

7.97. This measure has the potential to raise issues in relation to the right to an effective remedy. However, the most recent PJCHR report stated that, based on the Minister's response and noting the types of activities that are excluded from the application of civil immunity, on balance it appears that the measure may be compatible with the right to an effective remedy.[387]

7.98. The ASIO said in its submission that it sees these amendments as both proportionate and necessary.[388]

Proportionality

7.99. A repeated theme in the provisions referred to in this chapter is the need for TOLA's provisions to be proportionate in both their terms and their operation to the legitimate ends being pursued. This includes the effective safeguarding, in the face of encryption and other technological changes, of national security and public order, as well as the prevention of crime. Proportionality is also a factor I must consider under s 6 as well as s 8 of the INSLM Act. I return to it later in this report.

Giving evidence at the public hearing. Left to right: Mr Peter Vickery, Deputy Director-General Enterprise Service Delivery; and Mr Mike Burgess, Director-General of Security, Australian Security Intelligence Organisation

[387] Ibid 120.

[388] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, 12.

8. CONTEXT: THE CLOUD ACT, IPCO AND AAT

8.1. Where evidence (including data) is held overseas beyond the reach of Australian laws, Australian agencies have relied upon mutual legal assistance requests to obtain that material. These requests are governed by mutual legal assistance treaties and the *Mutual Assistance in Criminal Matters Act 1987* (Cth). That Act set outs a process for obtaining material which can take months or even years.

8.2. In recently introducing the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) (IPO Bill), the Minister's second reading speech stated:

> *The exponential rise of global connectivity and reliance on cloud computing means that intelligence and evidence that was once stored within Australia and available under a domestic warrant or authorisation is now distributed over different services, providers, locations and jurisdictions, and is often only obtainable through international cooperation. Criminals, including terrorists, typically access communications services that are supplied or operated by entities outside Australia. The overwhelming majority of data from these services is held by companies located overseas, including the United States. This places these service providers in a unique position to assist Australian law enforcement and national security efforts.*[389]

8.3. The US *Clarifying Lawful Overseas Use of Data Act 2018* (CLOUD Act) provides that:

> *An electronic communication service (ECS) or remote computing service (RCS) provider … in response to an order from a foreign government with which the United States has an executive agreement on data access … may:*
>
> - *intercept or disclose the contents of an electronic communication, and*
> - *disclose the contents of a stored electronic communication or non-content records or information pertaining to a subscriber or customer.*
>
> *It establishes a framework to allow the United States to enter into executive agreements with foreign governments to govern data access. To be valid, an executive agreement must meet certain requirements, including that the foreign*

[389] Commonwealth, *Parliamentary Debates*, House of Representatives, 5 March 2020, 2647 (Mr Alan Tudge, Minister for Population, Cities and Urban Infrastructure).

> *government affords robust procedural privacy protections and adopts minimization procedures. [It] … does not preclude a foreign authority from obtaining assistance in a criminal investigation or prosecution.*[390]

8.4. There is to date a single such agreement – namely, between the US and the UK. The Joint US/UK press release announcing the agreement stated:

> *The United States and the United Kingdom entered into the world's first ever CLOUD Act Agreement that will allow American and British law enforcement agencies, with appropriate authorization, to demand electronic data regarding serious crime, including terrorism, child sexual abuse, and cybercrime, directly from tech companies based in the other country, without legal barriers.*
>
> *The current legal assistance process can take up to two years, but the Agreement will reduce this time period considerably, while protecting privacy and enhancing civil liberties. …*
>
> *[US] Attorney General William Barr said: 'This agreement will enhance the ability of the United States and the United Kingdom to fight serious crime – including terrorism, transnational organized crime, and child exploitation – by allowing more efficient and effective access to data needed for quick-moving investigations. Only by addressing the problem of timely access to electronic evidence of crime committed in one country that is stored in another, can we hope to keep pace with twenty-first century threats. This agreement will make the citizens of both countries safer, while at the same time assuring robust protections for privacy and civil liberties.'*
>
> *[UK] Home Secretary Priti Patel said: 'Terrorists and paedophiles continue to exploit the internet to spread their messages of hate, plan attacks on our citizens and target the most vulnerable. As Home Secretary I am determined to do everything in my power to stop them. This historic agreement will dramatically speed up investigations, allowing our law enforcement agencies to protect the public. This is just one example of the enduring security partnership we have with the United States and I look forward to continuing to work with them and global partners to tackle these heinous crimes.'*
>
> *Both governments agreed to terms which broadly lift restrictions for a broad class of investigations, not targeting residents of the other country, and assure providers that disclosures through the Agreement are compatible with data protection laws. Each also committed to obtain permission from the other*

[390] See 115 *Congressional Record* HR4943 (2 June 2018) <https://www.congress.gov/bill/115th-congress/house-bill/4943>.

> *before using data gained through the agreement in prosecutions relating to a Party's essential interest – specifically, death penalty prosecutions by the United States and UK cases implicating freedom of speech.*
>
> *The novel US–UK Bilateral Data Access Agreement will dramatically speed up investigations by removing legal barriers to timely and effective collection of electronic evidence. Under its terms, law enforcement, when armed with appropriate court authorization, may go directly to tech companies based in the other country to access electronic data, rather than going through governments, which can take years. The current Mutual Legal Assistance (MLA) request process, which sees requests for electronic data from law enforcement and other agencies submitted and approved by central governments, can often take many months. Once in place, the Agreement will see the timeline obtaining evidence significantly reduced.*
>
> *…*
>
> *The United States will have reciprocal access, under a US court order, to data from UK communication service providers. All requests for access to data will be subject to independent judicial authorization or oversight.*[391]

8.5. It is expected that the agreement will enter into force in July 2020. The implementing legislation in the UK is the *Crime (Overseas Production Orders) Act 2019* (UK).

8.6. On 7 October 2019 the US and Australia issued a joint press release announcing the negotiation of a CLOUD Act agreement. It stated:

> *The United States and Australia and have entered into formal negotiations for a bilateral agreement under the U.S. Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), as the first step towards significantly boosting law enforcement cooperation between the two allies, with strong protections for rule of law, privacy and civil liberties.*
>
> *United States Attorney General William Barr and Australian Minister for Home Affairs, Peter Dutton, announced the negotiations during a meeting on Oct. 7, 2019.*

[391] US Department of Justice, 'US And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online' (Press Release 19-1065, 3 October 2019) <https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists>.

Attorney General Barr said that the United States is pleased that Australia has begun formal negotiations with the United States under the CLOUD Act. 'The CLOUD Act was created to permit our close foreign partners who have robust protections for privacy and civil liberties, such as Australia, to enter into executive agreements with the United States,' said U.S. Attorney General Barr. 'This agreement, if finalized and approved, will allow service providers in Australia and the United States to respond to lawful orders from the other country without fear of running afoul of restrictions on disclosure, and thus provide more access for both countries to providers holding electronic evidence that is crucial in today's investigations and prosecutions.'

The Attorney General also noted that the conclusion of an executive agreement with Australia will strengthen public safety for both countries. 'The United States looks forward to working with the Australian Government on this agreement, which will enhance each country's ability to fight crime by allowing faster access to data needed for quick-moving investigations. By increasing the effectiveness of investigations and prosecutions of serious crime, including terrorism, in both countries, citizens of both countries will be safer.'

Minister Dutton said Australia was very pleased to have taken this step.

'Last year, Australia congratulated the United States for its leadership in passing this legislation, which recognized that timely access to electronic information held by U.S.-based service providers is critical to efforts to combat serious crime,' said Mr. Dutton. 'Current processes for obtaining electronic information held by service providers in other countries risk loss of evidence and unacceptable delays to criminal justice outcomes. When police are investigating a terrorist plot or serious crime such as child exploitation, they need to be able to move forward without delay, but within the law – and the CLOUD Act strikes exactly that balance. This is the way of the future between likeminded countries. We have some way to go before the agreement is finalized, but once in place it will mean service providers based in the United States can respond directly to electronic data requests issued by our enforcement agencies under Australian law for data critical for the prevention, detection, investigation and prosecution of serious crime.'

The United States enacted the CLOUD Act in 2018 to speed access by foreign partners to electronic information held by U.S.-based global providers that is critical to such foreign partners' investigations of serious crime. The Act creates a new paradigm: an efficient, privacy and civil liberties-protective approach to ensure effective access to electronic data through executive agreements between the United States and trusted foreign partners.

> *While this electronic data can currently be sought through the mutual legal assistance (MLA) process, the CLOUD Act provides an alternative expedited framework for obtaining the data. The number of MLA requests for electronic information held by service providers in the United States has increased dramatically in recent years, straining resources and slowing response times. The CLOUD Act addresses delays in the MLA process by providing a new route for trusted partner countries to obtain electronic data.*
>
> *Underpinned by Australian legislation yet to be introduced, a bilateral CLOUD Act agreement would enable Australian law enforcement to serve domestic orders for communications data needed to combat serious crime directly on U.S.-based companies, and vice versa.*[392]

8.7. The IPO Bill is a critical step in Australia successfully obtaining a bilateral CLOUD Act agreement. As the Department of Home Affairs outlined in their preliminary submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), the CLOUD Act has 2 'pillars', namely:

a. It authorises the United States to enter into executive agreements with other countries, and while meeting certain requirements relating to the rule of law and privacy protections, enables the removal of any 'blocking statutes' between jurisdictions which are domestic laws which prevent access to or disclosure of electronic data.

b. It clarifies in statute an existing US legal position that a CSP under United States jurisdiction is compelled to produce data that it controls or possesses in the operation of its services in response to relevant United States legal process.[393]

8.8. The IPO Bill would enable Australia to give effect to the bilateral agreement by creating a new international production order framework that allows Australian law enforcement and intelligence/security agencies to issue or obtain extraterritorial orders for electronic data on foreign Designated Communications Providers (DCPs) (where there is an agreement in place). In introducing this Bill, the Government has stressed that this new framework will be complementary to existing data access and

---

[392] US Department of Justice, 'Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by US Attorney General William Barr and Minister for Home Affairs Peter Dutton' (Press Release 19-1075, 7 October 2019) <https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us>.

[393] Department of Home Affairs, Submission No 10 to the Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, 4.

international crime cooperation mechanisms.[394] The IPO Bill also introduces provisions to remove the 'blocking statutes' for Australian providers to respond to foreign orders to requests.

8.9. The IPO process, set out in a proposed new schedule to the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), covers 3 types of orders:

a. law enforcement criminal investigations

b. control order monitoring

c. national security.

All of these are then also divided into 3 subcategories:

a. interception

b. access to stored communications

c. access to telecommunications data.

8.10. The oversight mechanisms for this new regime broadly draw on existing arrangements while enlarging certain bodies. The Inspector-General of Intelligence and Security (IGIS) retains broad powers to interrogate intelligence agencies' systems, processes and actions. The IPO Bill also introduces a compulsory notification scheme: every 3 months, the Australian Security Intelligence Organisation (ASIO) must provide details of its orders to the IGIS for review. The 3-month period may be amended before the Bill again goes to Parliament for consideration. The Commonwealth Ombudsman gains new specified oversight powers over law enforcement agencies' use of the IPO framework and of the Commonwealth Attorney-General's Department (AGD) (in the AGD Secretary's role as the Australian Designated Authority (ADA)).

8.11. The ADA, through delegation to senior executive and executive level officials in AGD, will:

a. review orders for compliance with the relevant international agreement and, if not compliant, cancel such orders and advise the obtaining agency

b. act as intermediary between agencies and DCPs by serving orders and other notices on DCPs, relaying DCPs' objections to orders, and receiving the requested electronic data from a DCP and then providing it to the relevant agency

[394] Ibid 5.

c. have a broad discretion to cancel an order at any time, including to protect the public interest and when subject to any agreed dispute resolution processes

d. be obliged to keep a register of orders issued, to which the Ombudsman will have full physical and electronic access.

8.12. In this way, the implication of the IPO regime in practice largely mirrors existing processes for the International Crime Cooperation Central Authority (ICCCA) in running Australia's mutual legal assistance and foreign extradition schemes, which are already located in AGD.

The IPO Bill and the AAT

8.13. The Bill provides that, in a criminal law enforcement IPO application, for example, the issuer, an eligible judge or nominated AAT member, must consider:

> *(b) in the case of an application for an international production order that is in respect of one or more individual message/call application services:*
>
> > *(i) how much the privacy of any person or persons would be likely to be interfered with by intercepting, under an international production order, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services; and*
> >
> > *(ii) the gravity of the conduct constituting the serious category 2 offence or serious category 2 offences being investigated; and*
> >
> > *(iii) how much the information … would be likely to assist in connection with the investigation by the interception agency of the serious category 2 offence or serious category 2 offences; and*
> >
> > *(iv) to what extent methods of investigating the serious category 2 offence or serious category 2 offences that do not involve so intercepting messages, voice calls or video calls have been used by, or are available to, the interception agency; and*
> >
> > *(v) how much the use of such methods would be likely to assist in connection with the investigation by the interception agency of the serious category 2 offence or serious category 2 offences; and*
> >
> > *(vi) how much the use of such methods would be likely to prejudice the investigation by the interception agency of the serious category 2 offence or serious category 2 offences, whether because of delay or for any other reason; and*

…

(ix) such other matters (if any) as the eligible Judge or nominated AAT member considers relevant.[395]

ASIO IPO applications

8.14. The Director-General of Security, a Deputy Director-General or an ASIO employee may approve an application for an International Production Order (IPO). The application then goes to the Attorney-General for consent, after which it is sent to a nominated member of the Security Division (SD) of the Administrative Appeals Tribunal (AAT) to approve *persona designata*. This is a very significant change to the existing ASIO warrant approval process, although I do note the proposed changes in the subsequently introduced Australian Security Intelligence Organisation Amendment Bill 2020 (Cth), which has also been referred to the PJCIS.

8.15. ASIO has since clarified to the PJCIS in a public hearing[396] that not all ASIO employees would have such approval authority but that, consistent with similar regimes in Commonwealth agencies, that authority would sit with an Executive Level (EL) 1 or EL2 employee[397] or above. For IPOs not relating to interception and stored communications (therefore, an IPO for telecommunications data, including subscriber data), the Attorney-General's consent is not required and the application goes from an ASIO approver directly to the SD member.

8.16. The IGIS, in her submission to the PJCIS on the IPO Bill, stated that 'there is currently no statutory requirement for nominated members of the AAT to consider privacy, proportionality and human rights in deciding whether to issue … IPOs that may be sought in relation to national security'.[398] That follows from clause 98 of the IPO Bill, which states:

---

[395] IPO Bill, s 43, inserting new Schedule 1, s 30(5) in the *Telecommunications (Interception and Access) Act 1979* (Cth).

[396] Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 14 May 2020 (Peter Vickery, Deputy Director-General Enterprise Service Delivery, Australian Security Intelligence Organisation, via teleconference).

[397] Assistant Director and Director, respectively (broadly analogous to private sector middle management).

[398] Inspector-General of Intelligence and Security, Submission No 27 to the Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, 4.

Issue of international production order – national security

(2) [the IPO can be issued] If the nominated AAT Security Division member is satisfied, on the basis of the information given to the nominated AAT Security Division member under this Division in connection with the application, that:

(a) there are reasonable grounds for suspecting that the relevant person is engaged in, or is likely to engage in, activities prejudicial to security [that is, matters within ASIO's jurisdiction]; and

(b) there are reasonable grounds for suspecting that the designated communications provider holds any of the following stored communications: [these are listed]

(3) In deciding whether to issue an international production order under subclause (2), the nominated AAT Security Division member must have regard to the following matters:

(a) to what extent methods of carrying out the Organisation's function of obtaining intelligence relating to security (so far as carrying out that function relates to the relevant person) that are less intrusive than obtaining, under such an order, a copy of the stored communications have been used by, or are available to, the Organisation;

(b) how much the use of such methods would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security (so far as carrying out that function relates to the relevant person);

(c) how much the use of such methods would be likely to prejudice the Organisation in carrying out its function of obtaining intelligence relating to security (so far as carrying out that function relates to the relevant person);

(d) such other matters (if any) as the nominated AAT Security Division member considers relevant.

8.17. The IGIS made the fundamental point that the requirement in the IPO regime 'for two-step approval (consent by the Attorney-General and authorisation by an AAT

member) means that a more rigorous process would apply to the issue of international orders than to domestic warrants for similar types of information'.[399]

8.18. Throughout this review I have made clear that the notion that there should be a less stringent (because the decision-maker is not independent) authorisation of domestic access to data compared with international access (with proposed AAT approval) is unsatisfactory. So the proposed amendments to the IPO Bill in the IGIS' submission to the PJCIS may be tailored to apply to TOLA.

8.19. The IGIS' submission also suggests a need for greater transparency of agencies' use of IPOs, including some form of public statistical reporting.[400] I make various recommendations for increased reporting of use of TOLA powers.

The Administrative Appeals Tribunal

8.20. The AAT was established in 1976. AAT members are appointed by the Governor-General.[401] The President of the AAT must be a judge of the Federal Court of Australia.[402] Any other person serving as a member of the AAT must be a judge, a legal practitioner of at least 5 years' standing or a person with special knowledge or skills relevant to the duties of the role.[403]

8.21. The AAT's jurisdiction is determined by statute. It includes merits review of administrative decisions made under more than 400 Commonwealth Acts and legislative instruments. Typically, in merits review, the AAT 'stands in the shoes' of the original decision-maker but decides for itself the correct and preferable decision.

8.22. AAT members are also, with their agreement, chosen, *persona designata*, to issue various Commonwealth warrants and authorities. For instance, an application for a surveillance device warrant is ordinarily made to 'an eligible Judge or to a nominated AAT member'.[404] The same is true of applications for computer access warrants[405] and for warrants to intercept telecommunications over a telecommunications service.[406] In each of these cases, the term 'nominated AAT member' means an AAT

[399] Ibid.

[400] Ibid.

[401] *Administrative Appeals Tribunal Act 1975* (Cth), s 6(1).

[402] Ibid s 7(1).

[403] Ibid s 7(2), (3).

[404] *Surveillance Devices Act 2004* (Cth) (SD Act), s 14(4).

[405] Ibid s 27A(7).

[406] *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), s 39(1).

member (including a senior member or Deputy President) who the Minister has nominated in writing and who has accepted that nomination.[407]

8.23. The AAT has a registry in every state or territory capital city (apart from Darwin, as Northern Territory applications are handled through the Adelaide registry).

8.24. The SD is one of the 9 divisions of the AAT. As at 30 June 2019, it was constituted by 10 full-time Senior Members, 3 part-time Senior Members, and 16 full-time Members.[408] The SD reviews adverse or qualified security assessments issued by ASIO[409] and the cancellation of passports on security grounds.

8.25. It has special powers and procedures. For example, it has wide non-publication powers and powers to hear matters in private. It also has the capacity to ensure that classified information is not revealed to the non-Government party but equally to hear from the non-Government applicant in the absence of the Government party.[410]

8.26. According to AAT statistics, the SD finalised 10 matters in the year 1 July 2017 to 30 June 2018, 13 matters in the year 1 July 2018 to 30 June 2019, and 3 matters in the 6-month period of 1 July 2019 to 31 December 2019. As at 31 December 2019, 7 matters were still pending in the SD.[411]

---

[407] SD Act, ss 6, 13; TIA Act, ss 5, 6DA.

[408] Administrative Appeals Tribunal, *Annual Report 2018–2019* (Australian Government, Canberra, 2019) Appendix 1, 'Members of the AAT'.

[409] *Australian Security Intelligence Organisation Act 1979* (Cth), ss 54, 65; see also definition of 'Tribunal' in s 35 of that Act.

[410] See *Administrative Appeals Tribunal Act 1975* (Cth), ss 39B, 39C.

[411] Note that this information is drawn from 'Statistics', *Administrative Appeals Tribunal* (Web Page) under 'Caseload Reports', 'Whole of Tribunal', for each year in question <https://www.aat.gov.au/about-the-aat/corporate-information/statistics>.

9. FINDINGS: GENERAL PRINCIPLES

9.1. The PJCIS referral to me was to review 'the operation, effectiveness and implications of amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and whether that Act:

a. contains appropriate safeguards for protecting the rights of individuals; and

b. remains proportionate to any threat of terrorism or threat to national security, or both; and

c. remains necessary.'[412]

9.2. My function to review TOLA under s 6(1D) of the INSLM Act also requires that I review the operation, effectiveness and implications of amendments made by TOLA, having regard to, and applying, the tests in the INSLM Act: necessity, proportionality, rights protection (s 6), Australia's obligations under international agreements, including obligations relating to human rights, counter-terrorism obligations; and international security (s 8), but not individual complaints or agencies' priorities and use of resources (s 6(2)).

9.3. Given the terms of each review are identical, my findings and recommendations are therefore the same for both reviews.

9.4. In this chapter I consider the 'the operation, effectiveness and implications' of TOLA. In the next chapter I consider the remaining matters of necessity, proportionality and rights protection. As seen in Appendix E, the main focus of submissions to my review was criticism of TOLA's Schedule 1. That also is my main focus.

Schedule 1

9.5. A detailed description of the powers and capabilities of the relevant agencies that existed before the enactment of TOLA can be found in Chapter 4. As I there explained in detail, essentially TOLA made the following changes by Schedule 1:

a. There are 3 types of industry assistance: Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs).

b. Neither TARs nor TANs require external approval, but they can be agreed or issued by the agency head or delegate.

c. TCNs are issued by the Attorney-General.

[412] Or any related law – see INSLM Act, ss 6(1)(a)(iii), (1A), (1D).

d. The Australian Security Intelligence Organisation (ASIO), the Australian Criminal Intelligence Commission (ACIC) and the police have access to all 3 types of industry assistance powers.

e. The Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD) both obtain the capacity to agree TARs with Designated Communications Providers (DCPs) but not to obtain TANs or TCNs.

f. Integrity agencies are not mentioned in Schedule 1, so they do not have access to those powers and capacities.

9.6. The Department of Home Affairs has advised that as at early April 2020 there had been no TANs or TCNs issued.

9.7. According to the *Telecommunications (Interception and Access) Act 1979 Annual Report 2018–19*, the Australian Federal Police (AFP) issued 5 TARs and NSW Police issued 2 TARs between 9 December 2019 and 30 June 2019.[413]

9.8. Information on any TARs issued by ASIO in the reporting period is not publicly available.[414] However, I can say that I have examined all relevant action by ASIO as part of my review. I provide some details in the necessarily classified confidential annexure.

Use of other TOLA powers

9.9. According to the *Surveillance Devices Act 2004 Annual Report 2018–19*, between 9 December 2018 and 30 June 2019 the ACIC was issued 1 computer access warrant (CAW) and the AFP was issued 7 CAWs, with 1 application refused by a nominated Administrative Appeals Tribunal (AAT) member.[415] The warrant was refused because an AAT member raised concerns that a physical computer had to be identified. The AFP was also issued 2 extensions of CAWs, granted due to ongoing investigations. No agencies made remote applications for CAWs during this period. Information on the number of CAWs issued to ASIO in the reporting period is not publicly available, but I have had access to all relevant ASIO records.

9.10. As to Schedule 3, the AFP does not keep centralised records on the numbers of executed warrants and thus was unable to provide the figures. I regard that as

---

[413] Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2018–19* (Australian Government, Canberra, 2019) 76.

[414] Although it is required to be mentioned in a classified annexure in its annual report, which by law must, for example, be provided to the Leader of the Opposition.

[415] Department of Home Affairs, *Surveillance Devices Act 2004 Annual Report 2018–19* (Australian Government, Canberra, 2019) 19.

unsatisfactory and make recommendations later in this report that these records now be kept and published at least annually.

9.11. As to Schedule 4, I am advised that Australian Border Force (ABF) has obtained 16 assistance orders and executed 8 during the period for which I sought information. Not all assistance orders have been executed, as in some cases the subject person may have voluntarily complied with a request for information before the assistance order was executed. The nature of the information or assistance the ABF typically seeks to obtain through the orders is to unlock computers and mobile electronic storage devices to enable a digital forensic examination or, in some circumstances, to facilitate a manual examination.

9.12. There is no public information on ASIO's exercise of powers under Schedule 5. I later make recommendations that this information form part of ASIO's annual report.

9.13. Despite the small number of TARs agreed and the absence of TANs and TCNs (as far as is known publicly), ASIO and police forces regard the Schedule 1 powers as extremely important. I do expect the numbers to increase in time, and for TANs and TCNs to be issued.

9.14. As to the operation of Schedule 1 from the agencies' perspectives:

a. The AFP said it has 'provided significant operational benefit to address a number of emerging and urgent operational issues and facilitated productive engagement on potential technical options. This has been, and continues to be, of significant value to the AFP's investigative effectiveness'.[416]

b. ASIO said that it is 'an essential enabler of its ability to stay abreast of the technical development that might otherwise render its powers ineffective. The mechanisms the Act introduced have offered significant utility to date, and ASIO continues to make operational use of these capabilities … evidence suggests that the complexities that ASIO will face into the foreseeable future will continue to necessitate access to the mechanisms provided under the Act and the operational efficiencies that they afford'.[417]

[416] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, [55].

[417] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, [83], [85].

c. ASD, the Queensland Police Service, Tasmania Police and the Northern Territory Police Force also value the benefits of the powers enabled under TOLA. However, at this stage they have not used the powers.

9.15. In my opening statement at the public hearing I said this, and I now confirm:

> *nothing I have seen to date suggests there has been any form of 'mass surveillance' as a result of TOLA; in fact, what I have seen to date suggests that TOLA has allowed for pre-existing intrusive powers to now be used in a more targeted or limited fashion against persons of interest to make content or data otherwise obtained by warrant or authority to be made intelligible or accessible, or to do another listed act or thing.*[418]

9.16. My assessment is that TOLA powers and capacities are being used for the purposes Parliament intended and not otherwise.[419]

Conclusions

9.17. I consider that the following propositions are established.

9.18. *First*, as the internet became indispensable to the legitimate operations of, and interactions between, governments, corporations and other organisations, and individuals, it was used by criminals and other bad actors for their illicit purposes.

9.19. *Secondly*, the internet was not designed with security in mind. As Martin Thomson submitted to this review:

> *the internet was built without a semblance of security in the first place and so the early internet relied on trust and cooperation. Today, it's not really enough to trust that others share our goals. There are just far too many people and far too diverse interests. Instead, what we have done is we have developed systems that safeguard our online activities and trust in those systems is crucial to the function of the internet as a whole.*[420]

---

[418] Dr James Renwick CSC SC, Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing, Opening Statement, [28] <https://www.inslm.gov.au/sites/default/files/2020-02/INSLM%27s%20Opening%20Statement%20-%20TOLA%20Public%20Hearing.pdf>.

[419] Cp: INSLM Act, s 6(1)(d).

[420] Martin Thompson, Distinguished Engineer, evidence on behalf of Mozilla Corporation: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 102.

9.20. This is an inherent weakness. To remedy it, widespread data content encryption and, to an increasing extent, metadata encryption has been used.

9.21. *Thirdly*, pre-TOLA coercive statutory powers for access to intelligible data content and metadata were heavily relied on by intelligence, police and integrity agencies. The evidence I have received establishes that there has been widespread adoption of internet-based encryption by criminals and other bad actors. This has greatly impeded the important work of the Australian intelligence community, police, and integrity agencies, because encrypted data content and, to some extent, metadata are generally no longer readable by them or accessible to them in an intelligible form. As encryption steadily deprived them of this access, the effectiveness of those powers significantly diminished. In this way, for them, the internet is 'going dark' or has 'gone dark'.[421] The key justification put forward for TOLA is that it will reverse this trend.[422] No country which operates as Australia does under the rule of law can countenance the creation of ungovernable space, free from the rule of law. I therefore accept that some legislative response such as TOLA was necessary. Whether TOLA was necessary in its terms is bound up in the related questions of proportionality and rights protection.

9.22. *Fourthly*, encryption seeks to maintain general confidence in the security of the internet. It seeks to provide effective security and protection for internet communications and transactions and Government, commercial and private data, and also to maintain legitimate personal rights to privacy, and its near relative, anonymity.

9.23. *Fifthly* (to bring together what I have written earlier):

a. Under Australia's international law and other human rights obligations, personal privacy is a fundamental, but not an absolute, value. It can be outweighed by legitimate public policy aims such as cybersecurity, the detection of crime, the prevention of public corruption or the protection of national security.

---

[421] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019 – see the description at page 6.

[422] The stated purpose of TOLA is to amend a range of Commonwealth legislation to allow law enforcement and national agencies to 'better work in the increasingly complex digital environment' and 'introduce measures to better deal with the challenges posed by ubiquitous encryption': Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access Bill) 2018 (Cth), 2 [1].

b. In contrast to protections conferred in the US by the Fourth Amendment to the Constitution, or in the EU by the General Data Protection Regulation (GDPR), personal privacy across Australia is not (yet) protected by a specific tort or a constitutional guarantee. Rather, it is protected by statutes such as the *Privacy Act 1988* (Cth) and its State and Territory analogues and by a common law rule inherited from English law that holders of public office can only seize or access private property as authorised by law.

c. A policy corollary of that rule is the historically entrenched practice that laws which authorise investigatory agencies and police to seize or access private property do so by warrant, issued by persons independent of the agency or person which seeks to exercise the warrant.

d. This rule applies to accessing and copying data content and metadata on personal devices such as computers and mobile phones, just as much as it does to searches of people or premises.

e. The rule has rightly been said to recognise the 'link between protection of personal property and protection of freedom of thought and political expression'.[423]

f. As the rule is a fundamental right, it is protected by the principle of legality, so that a statute which seeks to overcome it will only be effective in doing so by clear statement of intent or by necessary implication.

g. In contrast, for national security and historical reasons ASIO warrants are usually issued by the Attorney-General (although that has and is changing).

9.24. *Sixthly*, international human rights law and the INSLM Act both require consideration of proportionality and the related question of human rights protections. What is required is a proportionate response to the problem of 'going dark'. Among other matters, this requires a range of ethical and policy concerns to be weighed up and, where possible, reconciled in a manner suited to our democratic system of government, noting that modern Australian society is sceptical of opaque exercises of intrusive power undertaken by ministers or senior officials, hence the need for trust with verification.

9.25. *Seventhly*, TOLA Schedules 2, 3 and 4 follow the historically entrenched practice of warrant powers issued by persons independent of the agency or person which seeks to exercise the warrant. TARs and some Schedule 5 arrangements are not coercive in effect, so this practice does not apply. But the issue of TANs and TCNs in Schedule 1

[423] *Smethurst v Commissioner of Police* [2020] HCA 14 [155] (Gageler J, citing Lord Camden in *Entick v Carrington* (1765) 19 St Tr 1029).

does not follow that practice. It therefore falls to those making this change to justify it – an issue I consider next.

9.26. *Finally*, noting the ongoing importance of privacy, encryption and access to data by law enforcement and intelligence agencies, **I conclude that the definition of 'counter-terrorism and national security legislation' in s 4 of the INSLM Act should be amended to include TOLA so that future INSLMs may review it of their own motion as necessary.**

Giving evidence at the public hearing. Left to right: Dr Natasha Molt, Director of Policy, and Ms Pauline Wright, President, Law Council of Australia

10. FINDINGS: TARS, TANS AND TCNS

10.1. This chapter sets out my findings and recommendations on Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs). In summary:

a. Almost every non-Government submitter had strong concerns regarding, and objections to, the following aspects of TANs and TCNs:

– the absence of independent authorisation for notices

– the absence of independent technical assessment of proposed notices in relation to such matters as whether they met the statutory definitions of being 'reasonable and proportionate' or 'technically feasible', or would result in a 'systemic weakness or systemic vulnerability'

– whether those definitions, as well as the definition of 'Designated Communications Providers' (DCPs), should be amended.

b. The integrity agencies have the same necessity for access to Schedule 1 of TOLA as police.

c. I conclude that Schedule 1 should only remain in force to the extent it operates in such a manner to make it both proportionate to threats and properly protective of individual rights, which it can do it if my key recommendations are followed concerning independent and technically informed approval of TANs and TCNs and changes to key definitions.

Absence of independent authorisation of TANs and TCNs

10.2. It was almost unanimously agreed in non-Government submissions that TANs and TCNs should be independently authorised (by either an independent tribunal member or a judicial officer) and be subject to meaningful judicial review once issued.[424] Indeed, during the public hearing, a number of stakeholders indicated that their main concern with Schedule 1 was that no independent person was involved

[424] See the following written submissions: Atlassian, No 17 (3); Google, No 19 (4–5; Access Now, No 32 (6–7); BSA, No 25 (4–5); Communications Alliance, No 15 5, 7), Internet Australia, No 29 (4, 16); Australian Human Rights Commission, No 30 (16–18); Human Rights Law Centre & Digital Rights Watch, No 11 (4); Law Council of Australia, No 45 (7, 10, 24–25); Office of the Australian Information Commissioner, No 20 ([9], [24]).

in the decision to issue an industry assistance notice. A number of submissions also conveyed strong support for the UK's double-lock model of judicial authorisation.[425]

10.3. The Australian Human Rights Commission (AHRC) submitted that the human rights concerns associated with TOLA would be better addressed if an eligible judge had to approve the giving or variation of a TAN or TCN.[426] During the public hearings, Mr John Howell of the AHRC described the independence of the issuing party as 'a vital safeguard' for human rights. He put forward 2 criteria that would broadly satisfy the AHRC's concerns: first, that the person be independent, and be seen to be independent; and, secondly, that the person be appropriately qualified.[427]

10.4. Law enforcement agencies, intelligence agencies and the Department of Home Affairs responded that there are already a number of conditions that apply to the issuing of compulsory industry notices that operate as effective and sufficient oversight; therefore, no change to the authorising provisions was necessary. In particular, they submitted that:

a. A distinction needs to be drawn between the compulsory industry notices that provide technical 'access' on the one hand, and warrants or other like instruments, which provide 'content', on the other. TANs and TCNs:

   – do not provide the authority to obtain content without an underlying warrant, a matter made explicit by s 317ZH[428]

---

[425] See Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 54; and Law Council of Australia, Submission No 45 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 6 November 2019, [182]–[183].

[426] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 74.

[427] See Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 35, 40, 42, and listing lack of judicial authorisation as the first of 5 key concerns.

[428] Which provides:

> *(1) A technical assistance request that relates to an agency, or a technical assistance notice that relates to an agency, or a technical capability notice that relates to an agency, has no effect to the extent (if any) to which it would request or require a designated communications provider to do an act or thing for which the agency, or an officer of the agency, would be required to have or obtain a warrant or authorisation under any of the following laws*

- are merely a mechanism to ensure that whatever data is obtained under a lawful warrant is accessible and comprehensible. Accordingly, the independent or external authorisation customarily required for warrants sought by agencies is unnecessary. Thus, 'a key safeguard in Schedule 1 powers is that they cannot authorise access to data'.[429]

b. The conditions of issue of the compulsory industry notices are rigorous – for instance, through:

- decision-making criteria, including that the notice be 'reasonable and proportionate', 'practicable' and 'technically feasible'
- notification obligations
- statutory limitations on the scope of the power, effected through the prohibition on requiring DCPs to build or maintain any 'systemic weakness' or 'systemic vulnerability'.[430]

10.5. It is also contended that there are already mechanisms contained within the amendments effected by Schedule 1 of TOLA to Part 15 of the *Telecommunications Act 1997* (Cth). For example, in the case of TCNs:

a. there is provision for consultation with DCPs

b. there is a right on the part of DCPs to seek an assessment of the proposed TCN by an independent assessor and retired judge prior to approval and the Attorney-General must have regard to the outcome of that independent assessment

c. there is a double-lock in the sense that the Attorney-General and the Minister for Communications must both agree on the issue of the TCN.

(a) the Telecommunications (Interception and Access) Act 1979*;*

(b) the Surveillance Devices Act 2004*;*

(c) the Crimes Act 1914*;*

(d) the Australian Security Intelligence Organisation Act 1979*.*

(f) a law of the Commonwealth (other than this Part) that is not covered by paragraph (a), (b), (c) or (d); (g) a law of a State or Territory.

[429] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 16 [99].

[430] Ibid 2 [12].

10.6. The intelligence and law enforcement agencies also contend that their exercise of power to request the issue of various warrants and instruments is already subject to external, effective and regular periodic review by, respectively, the Inspector-General of Intelligence and Security (IGIS), the Commonwealth Ombudsman and similar agencies (depending on the agency).

Findings on TANs

10.7. I do not accept the Government submissions in this regard. The onus is on the Government agencies to explain why the normal practice of independent authorisation should not apply for Schedule 1 of TOLA. I do not accept that onus has been discharged. Instead, for the following reasons, I *do accept* the non-Government submissions that there should be independent authorisation for TANs (and also TCNs as I explain next).

10.8. *First*, I apply the fundamental principle guiding me in this review, namely:

> *Just as in the physical world we do not accept lawless ghettos where the law does not apply, so also it should be in the virtual world: in this context it means intrusive surveillance powers – conferred by law and with clear thresholds and safeguards – which already apply in the physical world should in principle apply in the analogous virtual world unless there are good reasons otherwise.*

10.9. Having accepted the necessity of the powers, the next issue is the safeguards. The starting point, therefore, is to apply the physical world principles that:

a. The ability to use coercive powers without external and independent review and authorisation is exceptional and requires justification.

b. For the reasons set out in Chapter 5, there is a fundamental common law rule that holders of public office can only seize or access private property as authorised by law. There is also a policy corollary of that rule: the historically entrenched practice that laws which authorise investigatory agencies and police to seize or access private property do so by warrant. Those warrants are issued by persons independent of the agency or person which seeks to exercise the warrant.

c. It is equally appropriate that there be some form of external authorisation or approval for the exercise of powers that have no direct impact on private property rights, but are nonetheless coercive or intrusive in their effect – for instance, by mandating that a person engage in certain conduct or provide certain information.

d. Any scheme involving the use of coercive statutory powers must ensure that it has the necessary checks and balances to ensure not only that correct and lawful decisions are made but also that they are seen to be made. The scheme must instil and inspire trust in the community that such decisions will be made.

e. With the exception of most Australian Security Intelligence Organisation (ASIO) powers, coercive warrants require external approval or authorisation, usually by a magistrate, an eligible judge acting as *persona designata* or a member of the Administrative Appeals Tribunal (AAT). For example, in its recent submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) (IPO Bill), the Attorney-General's Department rightly states that:

> *[16] The conferral of persona designata powers recognises that federal judges, magistrates and AAT members are well-placed to conduct dispassionate assessments of evidence, and to balance the rights and liberties of individuals with the interests of law enforcement agencies. The Bill ensures that the system for issuing IPOs will be applied with fairness and accountability owing to the skill, experience and independence of the individuals appointed.*
>
> *[17] A judge, magistrate or AAT member exercises a function in their personal capacity as a way to ensure accountability in the course of a sensitive investigation or law enforcement procedure. Requiring an executive action to be approved by a decision-maker who is independent of government and outside of the investigation process can provide an important safeguard and promote public confidence that law enforcement agencies are operating with appropriate oversight.*[431]

10.10. I agree. The approval processes that apply to warrants provide a useful frame of reference for industry assistance notices. For instance, warrants require external authorisation because they interfere with fundamental property rights and privacy expectations. Industry assistance notices do likewise, so they require external authorisation. However, there are limits to the analogy between warrants and industry assistance notices. This is because an industry assistance notice differs from a warrant in key respects, including the following:

a. A person in respect of whose person or premises a warrant issues is often, though not always, a target of the investigation. Though a warrant ordinarily

[431] Attorney-General's Department, Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, [5] – [6]

issues where police reasonably suspect that evidential material is located in a house, in a car or on a computer, the person to whom that house, car or computer (as the case may be) belongs, or by whom it is habitually used, is often a criminal suspect. By contrast, in respect of an industry assistance notice, the person most immediately affected by the notice is the DCP, who is not suspected of any offence.

b. An application for a warrant is made ex parte so that the person of interest does not learn about the warrant before it is executed. As the DCP is not the subject of any criminal investigation and will ordinarily have a good deal of notice that the TAN or TCN is pending (on the basis of prior negotiations with the agency or because a TAR has already issued), the rationale for making an application ex parte does not apply.

c. A warrant does not ordinarily compel a person affected by the warrant – or any other person – to do anything (although they cannot obstruct the execution of the warrant). The occupier of premises where a warrant is being executed is not ordinarily required to help with the search or point to where evidence is located (subject to anything that a *Crimes Act 1914* (Cth) s 3LA assistance order might require). By contrast, a TAN and a TCN impose direct, and perhaps significant, obligations on a DCP to assist law enforcement.

10.11. I consider that there is a *greater* need for the traditional safeguards in the virtual world than in the physical world. That is both for reasons of trust and, as explained in Chapter 5, because of the wide and unknown impact of technology, including how data from disparate sources is fused. As to trust, I have earlier quoted from, and agree with, Professor Peter Leonard's evidence to the public hearing.

10.12. *Secondly*, I do not accept the argument that 'a key safeguard in Schedule 1 powers is that they cannot authorise access to data', access being granted by separate warrant issued by a tribunal member or judge. This argument elevates form over substance. In substance:

a. A key policy reason for Schedule 1 of TOLA was to reverse the effect of going dark by making intelligible or otherwise useful the content of data already, or to be, accessed, by warrant.

b. The proportionality of TANs must therefore be measured by reference to their use with those pre-existing powers.

c. The coercive impact on the recipient of the TAN is entirely distinct from any coercive effect of any underlying warrant or authorisation. Thus, unlike the underlying warrants, the compulsory industry notices have a direct and coercive effect upon the DCP, which is not the subject of the warrant or under reasonable suspicion of committing any relevant offence or in all likelihood the

subject of security agency or law enforcement interest more broadly. The DCP will have no standing to challenge the underlying warrant even though the fruits of the warrant will only produce something meaningful for the TAN issuer's agency when combined with the TAN.

10.13. *Thirdly*, the requirement that the notice be 'reasonable and proportionate' *increases* the need for independent authorisation. By s 317RA it is provided that:

> *In considering whether the requirements imposed by a technical assistance notice or a varied technical assistance notice are reasonable and proportionate, the Director-General of Security or the chief officer of an interception agency, as the case requires, must have regard to the following matters:*
>
> *(a) the interests of national security;*
>
> *(b) the interests of law enforcement;*
>
> *(c) the legitimate interests of the designated communications provider to whom the notice relates;*
>
> *(d) the objectives of the notice;*
>
> *(e) the availability of other means to achieve the objectives of the notice;*
>
> *(ea) whether the requirements, when compared to other forms of industry assistance known to the Director-General of Security or the chief officer, as the case requires, are the least intrusive form of industry assistance so far as the following persons are concerned:*
>
> *(i) persons whose activities are not of interest to ASIO;*
>
> *(ii) persons whose activities are not of interest to interception agencies;*
>
> *(eb) whether the requirements are necessary;*
>
> *(f) the legitimate expectations of the Australian community relating to privacy and cybersecurity;*
>
> *(g) such other matters (if any) as the Director-General of Security or the chief officer, as the case requires, considers relevant.*

10.14. In itself, s 317RA (and the equivalent provisions in Schedule 1 for TARs and TCNs) is in terms which appropriately allow for all issues relevant to proportionality and human rights be taken into account. The factor that is missing to ensure proportionality and human rights protection in both perception and practice is a technically informed decision-maker who is independent of the agency which will utilise the TAN once issued.

10.15. The current terms under which a TAN is issued are an unsatisfactory alternative as:

a. The relative weight to be given to these factors in s 317RA is unstated. DCPs will rightly be concerned that an agency head or minister will give greater or even decisive weight to factors favouring the agency, in comparison to the approach an eligible judge or tribunal member would take.

b. The decision-maker's weighing up of these factors will be very hard if not impossible for the DCP to successfully challenge in court:

– the decision-maker's reasons and relevant weighting of factors will probably be unknown: there is here neither a statutory right to reasons (and there is no common law right to reasons for an administrative decision: *Public Service Board v Osmond*[432]) and the likely, even inevitable, claim of public interest immunity in answer to a subpoena or notice to produce may make it impossible to allege or prove any judicially reviewable error at all

– there is no merits review in a tribunal or court

– although there is a constitutionally entrenched right to seek relief under s 75(v) of the Australian Constitution, which has a Federal Court and Federal Circuit Court analogue in s 39B of the *Judiciary Act 1903* (Cth), the requirement in s 317RA is that the decision-maker be satisfied – that is, presumably, 'reasonably satisfied' – so it is not for the court to determine for itself whether it considers the requirements imposed by the TAN (or TCN) are reasonable and proportionate. Rather, the DCP must attack the satisfaction of the decision-maker, which is forensically difficult.[433]

---

[432] (1986) 159 CLR 656.

[433] In *Gedeon v Commissioner of the New South Wales Crime Commission* [2008] HCA 43 the plurality said:

> *[43] The expression 'jurisdictional fact' was used somewhat loosely in the course of submissions. Generally the expression is used to identify a criterion the satisfaction of which enlivens the exercise of the statutory power or discretion in question. If the criterion be not satisfied then the decision purportedly made in exercise of the power or discretion will have been made without the necessary statutory authority required of the decision maker.*

c. It may be slightly easier for a DCP to establish by declaration that the notice would create 'systemic weakness' or 'systemic vulnerability' or that complying with the notice is not 'practicable' or 'technically feasible' because they can best prove such matters from their own resources and knowledge. However, a DCP can legitimately argue that it should not have to bear the onus of proving those matters, and the DCP would no doubt be concerned about revealing, in court, commercial-in-confidence matters relating to its own technology, just as much as the issuing agency would be concerned about revealing its operational secrets. (I deal with this issue below.)

10.16. *Fourthly*, while the IGIS serves an important function in keeping security agencies accountable, as do the Ombudsman and similar agencies for police, none has any ability to control the issue of the notices at the time of the exercise of power. It would give little comfort to a recipient of a notice, who had to comply with it, for the IGIS or Ombudsman to determine after the fact that a notice was wrongly issued.

10.17. *Fifthly,* there is an absence of independent technical assessment of the relevant technological factors – indeed, there is no requirement that any issuer under TOLA as its stands be technically qualified or advised, save for the possibility of an assessors' report for a TCN.

10.18. For these reasons the case for independent approval – external of the requesting agency – is compelling in the case of TANs. My recommendations in this chapter for the issue of TANs by the AAT with access to technical expertise, if adopted, will, to repeat the language of the Attorney-General's Department submission for the IPO Bill, ensure that TANs will be considered:

> *…with fairness and accountability owing to the skill, experience and independence of the individuals appointed…Requiring an executive action to be approved by a decision-maker who is independent of government and outside of the investigation process can provide an important safeguard and promote public confidence that law enforcement agencies are operating with appropriate oversight.*[434]

---

[44] The concept appears from the following passage in the reasons of Latham CJ in R v Connell; Ex parte The Hetton Bellbird Collieries Ltd [31]:
'The subject matter with which the Industrial Authority deals is, inter alia, rates of remuneration. There is power to deal with this subject matter in respect of rates of remuneration which existed on the specified date only if the authority is satisfied that the rates in question are anomalous. Unless this condition is fulfilled, the authority cannot act - it is a condition of jurisdiction.'

[434] Attorney-General's Department, Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, [16]–[17].

10.19. I now consider whether the approval of TCNs by the Attorney-General should be under a different scheme. Although the statutory scheme for TCNs is slightly different, I come to the same conclusion.

Findings on TCNs

10.20. In recognition of the potentially greater burden that a TCN may impose upon a DCP as it compels the creation by the DCP of a new capability, TOLA provides, among other requirements, as follows.[435]

10.21. *First*, the Attorney-General rather than the agency head issues the notice.

10.22. *Secondly*, there is a governmental 'double-lock' in the sense that the Attorney-General must give the Minister for Communications notice of and an opportunity to comment upon the proposed TCN, and the other minister must approve the giving of the notice (s 317TAAA(1)(b)) having had regard to:

> *(a) the objectives of the notice;*
>
> *(b) the legitimate interests of the designated communications provider to whom the notice relates;*
>
> *(c) the impact of the notice on the efficiency and international competitiveness of the Australian telecommunications industry;*
>
> *(d) the representation (if any) that was made under subsection (4) [by the Attorney-General];*
>
> *(e) such other matters (if any) as the Minister considers relevant.*

10.23. *Thirdly*, the Attorney-General must invite the DCP to make a submission to the Attorney-General on the proposed notice (or 'consult' the DCP on a notice which is the same or substantially the same as a previous one).

10.24. *Fourthly*, the Attorney-General may choose to ask, and must at the request of the DCP ask, a retired judge and an expert to produce a report as assessors. The assessors must:

> *(a) consider:*
>
> > *(i) whether the proposed technical capability notice would contravene section 317ZG [systemic weakness or vulnerability]; and*
> >
> > *(ii) whether the requirements imposed by the proposed technical capability notice are reasonable and proportionate; and*

[435] See generally TOLA, Schedule 1, Division 4.

(iii) whether compliance with the proposed technical capability notice is practicable; and

(iv) whether compliance with the proposed technical capability notice is technically feasible; and

(v) whether the proposed technical capability notice is the least intrusive measure that would be effective in achieving the legitimate objective of the proposed technical capability notice; and

(b) give the greatest weight to the matter mentioned in subparagraph (a)(i).

10.25. *Fifthly*, the assessors' report must be provided to the DCP and Attorney-General but must also be provided to the IGIS or Ombudsman as appropriate depending on what the notice requires. The Attorney-General *must have regard to the report but is not bound by it.* The Attorney-General must consider whether requirements to be imposed on a TCN are reasonable and proportionate using essentially the same factors as apply to TANs.

10.26. The Government submissions argue that the assessors' report is an important safeguard, that the Attorney-General is independent and that there is a 'double-lock' given the need for approval by another minister. It is also said that, for ASIO, warrants have traditionally and continue to be issued by the Attorney-General rather than an eligible judge or tribunal member. I now consider these matters.

The assessors' report

10.27. I agree that the functions of the assessors for TCNs is an improvement on the arrangements for TANs. It is certainly desirable that a retired judge consider these factors with the assistance of a technical expert. But the resulting report is not binding on the Attorney-General, although he or she must have regard to it. Also, in contrast with their equivalents under the UK's Investigatory Powers Commissioner's Office (IPCO), the assessors will not have the opportunity to build up experience in these difficult matters.

The double-lock argument

10.28. During the public hearings, the Department of Home Affairs emphasised that, even though they form part of the same Cabinet, the Attorney-General and the Minister for Communications are independent repositories of statutory power who are required to be independently satisfied of the relevant factors.[436] No doubt that is

[436] See the evidence of Mr Hansford on behalf of the Department of Home Affairs: Independent National Legislation Security Monitor, Review of the

generally true, although it is likely that they would each be bound by a Cabinet decision to issue a particular, or a particular type of, TCN.[437]

10.29. Perhaps more fundamentally, in my view one Cabinet minister's approval of another's decision to issue a TCN does not, in substance or perception, amount to an independent or external review of the decision to issue the notice. The overwhelming message I have received from non-Government submitters during the course of my review is that any 'independent' person must be independent not only of the issuing agency but also of the Government more broadly, so as to provide sufficient assurance of independence to DCPs and to the community generally in this controversial and developing area. I agree.

10.30. Accordingly, for all agencies other than ASIO, I consider that the issuer needs to be independent of Government. Thus, it cannot be the Attorney-General.

10.31. I recommend below that State and Territory integrity agencies should be given access to Schedule 1 powers. In relation to TCNs, it is usually inappropriate for any minister (rather than an independent judge or tribunal member) to be privy to the details of an integrity agency's ongoing investigations. That will be especially so once there is a Commonwealth Integrity Commission. Accordingly, if my recommendation is accepted, those notices too should be issued by an external issuing authority independent of Government, including the Attorney-General.

10.32. Given the historical role of the Attorney-General approving ASIO warrants, I next ask whether ASIO should be in a different position.

Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 (TOLA), Public Hearing Transcript, 195.

[437] In *Ansett Transport Industries (Operations) Pty Ltd v The Commonwealth* [1977] HCA 71; (1997) 139 CLR 54, Aickin J said (115–116):

> *Although the discretion [in that case] is that of the Secretary of the Department of Transport, it is not one to be exercised entirely according to his personal views. Government policy, and particularly that applicable to matters within the scope of his Department must in every case be a matter for his serious consideration. Moreover the Minister or the cabinet may properly indicate to him what government policy is in relation to imports of aircraft generally or to the importation of particular aircraft. There is nothing improper in the Minister requesting him to act in a particular manner or seeking to influence or persuade him to act in a particular manner, nor is there any failure of duty by the head of a department of government in acting in accordance with such a request.* In many matters of policy it might indeed be the duty of the Secretary to act in accordance with the policy of the government of the day. [emphasis added]

The historical role of the Attorney-General in relation to ASIO

10.33. The UK and Australia have a long history of having search warrants for intelligence and security purposes issued solely by ministers (Secretaries of State).

10.34. For ASIO, it has been true until recently that all ASIO coercive powers (save for some temporary, emergency powers) are approved by the Attorney-General. However, there is already a significant exception in the case of Questioning Warrants (QWs) and Questioning Detention Warrants (QDWs),[438] and there is a current Government Bill before the PJCIS – namely, the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth), to which reference has and will be made. If this Bill is enacted, it would make another significant exception.

10.35. As to the UK, in *A Question of Trust* it is said:

> *14.48 The recommendation that Secretary of State authorisation be replaced by judicial authorisation is one of the more radical recommendations in this Report, since if adopted it would replace a practice of several centuries' standing. But there is a precedent for it and … I found it one of the easiest to arrive at.*
>
> *14.49 My starting point was not any legal consideration, but rather the remarkable fact (at least to an outsider) that* the Home Secretary routinely signs thousands of warrants per year, *most of them concerned with serious and organised crime and the remainder with national security (principally terrorism). The Home Secretary leads a huge department of state with responsibility for immigration and passports, drugs, policing, crime policy and counter-terrorism. Yet she has herself described warrantry as occupying more of her time than anything else (some of it on an urgent basis in the middle of the night). In 2014, the Home Secretary personally authorised 2,345 interception and property warrants and renewals …. Warrantry is no doubt approached by most Home Secretaries in a thoroughly conscientious manner, and the Home Office WGD does an admirable job in supporting her. But it is open to question whether this function is the best use of the Secretary of State's valuable time.*
>
> *14.50 The second reason for recommending change is to* improve public confidence *in the system. I do not suggest that recent Secretaries of State have*

[438] On 13 May 2020 a Government Bill was introduced into Parliament and immediately referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS). It partly implements the review of QWs or QDWs by the second INSLM, the Hon Roger Gyles AO QC. The Australian Security Intelligence Organisation Amendment Bill 2020 amends the compulsory Questioning Warrant and Questioning Detention Warrant framework in the ASIO Act by enabling ASIO's continued use of Questioning Warrants, by removing its ability to use Questioning Warrants and Questioning Detention Warrants but replacing the existing detention framework with a more limited apprehension framework.

> *been complicit in the abuse of the warrantry system, so as to target people for political or otherwise improper reasons. The professionalism of the WGD would make this difficult, at least in a blatant fashion. But neither the British public nor the global public can be counted on to take the probity of the Secretary of State on trust …*
>
> *14.51 The third reason for recommending change relates to what the ISC has described as 'the single most important challenge that the Agencies face', which is no less a challenge for law enforcement: the difficulties in obtaining* assistance from service providers based in the US*. US companies which are used to a domestic system of judicial authorisation and not instinctively inclined to obey a UK warrant can find it difficult to understand why they should honour a warrant signed by the Secretary of State, as was impressed upon me in Silicon Valley (11.19 above) and as others have also observed.*
>
> *14.52 The fourth reason for recommending change is that there is an* established and well-functioning system for judicial approval *by Commissioners of comparably intrusive measures, when applied for by the police: property interference, intrusive surveillance and long-term undercover police operations (which are adjudicated upon by the Commissioners even when they are sought on national security grounds). I have spoken to four Surveillance Commissioners and been introduced to the tasks that they have to perform. Their experience (from a lifetime's court work) of police attitudes and methods renders them well qualified to judge whether an application is truly necessary and – if not – to send it back for reconsideration. The police also have the highest professional respect for the Commissioners, which is reinforced when the Commissioners go to speak to them about what they expect. Even if they had the necessary time to consider the detail, few Home Secretaries would have the same experience or expertise*.[439]

10.36. As already noted, the *Investigatory Powers Act 2016* (UK) (IP Act) did not entirely remove the function of secretaries of State (that is, ministers); rather, it established a double-lock through the use of IPCO. But, essentially, David Anderson QC found the factors in the preceding quote persuasive, as I do. Applying these factors to the Australian position, they all favour independent, non-ministerial approval of TCNs for ASIO as well as for other agencies. Thus:

a. *'The Home Secretary routinely signs thousands of warrants per year … Warrantry is no doubt approached by most Home Secretaries in a thoroughly conscientious manner, and the Home Office does an admirable job in supporting her. But it is open to question whether this function is the best use of the*

[439] David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (UK Government, London, 2015) 271 (emphasis in original; citations removed).

Secretary of State's valuable time.': As I have previously stated of the ASIO warrants issued or approved by the Attorney-General, this is 'not a small number'. In the classified annexure to this report I set out the approximate number issued by the Attorney-General last year. The point is that for decades now the warrant-issuing function has been a significant impost of time on an ever-busier Attorney-General, and it is indeed 'open to question' in Australia, as in the UK, whether this is the best use of that Minister's time in view of his or her significant other ministerial and parliamentary commitments.

b. *To 'improve public confidence' and the related issue of trust with verification*: This has been a consistent theme of this report as well. Modern democracies are increasingly sceptical of the opaque or secret exercise of powers by ministers and public officials. The universal feedback from my UK and US consultations in this review – from officials, oversight bodies and civil society alike – has been that one undoubted benefit brought by the creation and operation of IPCO in the UK has been a tangible increase in public trust in the powers being exercised. That trust cannot be taken for granted, as a former head of MI5 recently wrote:

> *In the years after 9/11 the government sometimes struggled to maintain public, parliamentary and judicial support for the use of intrusive techniques. Some measures failed to get through parliament and others were struck down in the courts. There was acceptance that surveillance was needed but this was not always matched by support for particular measures, and this gap was used by our enemies to sow mistrust. We should not make that mistake again.*[440]

c. While ministerial responsibility to Parliament is an important aspect of Australian democracy, as it is in Westminster, it is a necessary but not in and of itself a guarantee of trust. In practice, certain aspects of intelligence agencies' work must remain classified and not available to the general public. Important parliamentary mechanisms, including the PJCIS, therefore exist to scrutinise such classified activities on behalf of the people because this cannot realistically occur in debates in either House of Parliament.

d. *'Assistance from service providers based in the US'*: Tellingly, the Government has accepted the importance of this factor given its introduction of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 so as to have in place a system which will work with the US *Clarifying Lawful Overseas Use of Data Act 2018* (CLOUD Act) agreement currently being

[440] Rt Hon Baron Evans of Weardale KCB DL, 'Use of Surveillance Techniques to Beat Coronavirus Requires Public Trust', *The Times*, 12 April 2020.

negotiated with the US. Under that Bill certain ASIO requests for information under the CLOUD Act must be issued by the AAT, not by any minister. No reason has been put forward in this inquiry to justify a different approval mechanism for TANs by the Director-General, or TCNs by the Attorney-General, when external requests under the IPO Bill would require AAT approval *independent* of ASIO and the Attorney-General.

e. *There is 'an established and well-functioning system for judicial approval … of comparably intrusive measures. Their experience (from a lifetime's court work) of police attitudes and methods renders them well qualified to judge whether an application is truly necessary and – if not – to send it back for reconsideration. The police also have the highest professional respect for the Commissioners … Even if they had the necessary time to consider the detail, few Home Secretaries would have the same experience or expertise'*: There are in Australia, also, 2 such systems in operation – one is the *persona designata* system involving members of the judiciary and of the AAT; the other is the Security Division of the AAT itself, and the remaining remarks are equally applicable in Australia.

10.37. As with TANs, the vital and respected work of the IGIS and the Commonwealth Ombudsman complement, but are no substitute for, independent issuers. That is all the more compelling for the powers to which Schedule 1 of TOLA relates, given their covert nature, the technical complexity of the matters with which they deal, and the broad public concern over their potential exercise, including how the warranted data stream is to be fused with other unknown data streams and capabilities.

Findings on TARs

10.38. In contrast, in relation to TARs, **I conclude there should be no changes to the capacity of the relevant agencies and a DCP to freely agree a TAR with each other, other than that a prescribed form be used**. Many of the submissions I received on independent authorisation of industry assistance notices focused on TANs and TCNs. That focus makes sense, given that these are coercive notices issued by an agency or the Attorney-General on a DCP, without the DCP's consent. Indeed, while the legislation does not precisely require it, many agency or Government submissions (including, for instance, ASIO, the Australian Federal Police (AFP) and the Department of Home Affairs) referred to TANs and TCNs as an 'escalation' mechanism where the agency and DCP in question have failed to negotiate a TAR.[441]

[441] See Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 17 (ASIO), 181 (AFP), and 195 (Department of Home Affairs).

10.39. Most fundamentally, a TAR is not a coercive instrument. A DCP that receives a TAR can freely choose not to comply with the request it contains, in whole or in part, without any legal consequence.

10.40. Ms Lucie Krahulcova of Access Now submitted at the public hearing that the immunity from civil prosecution that a TAR confers on a complying DCP has the consequence of extinguishing any civil right of action that a customer of the DCP might have had against it – for instance, for breach of the contract that governs the relationship between the DCP and its customer. But that immunisation from suit is not significantly different to the effect of anyone being required to produce under search warrant a document or thing that impacts the rights of a third party, which that third party may know nothing about. The TARs that have been issued to date have been classified, and the unauthorised disclosure provisions under TOLA cover all relevant details of a TAR, TAN or TCN. Even if TARs were to come for approval before an independent issuing authority, the DCP's customer will not be able to challenge the TAR or enforce contractual rights against the DCP, not least because they will not know of it.

10.41. Further, the IGIS and the Ombudsman have jurisdiction to consider the terms of TARs which have been agreed, and what they have produced and, no doubt will do so.

10.42. I note that ASIO is not the only intelligence agency with industry assistance powers under Part 15 of the Telecommunications Act as effected by Schedule 1 of TOLA. The Australian Signals Directorate (ASD) and Australian Secret Intelligence Service (ASIS) also have the power to agree TARs. However, they do not have the power to issue TANs or to apply for TCNs. As I do not recommend any amendment to the process by which TARs are issued, nothing that I propose will directly affect the manner in which ASD or ASIS obtain TARs. In this respect, the position in respect of ASD and ASIS is no different from that of ASIO or any interception agency in relation to the issue of TARs.

Integrity agencies should be included in Part 15 of the Telecommunications Act

10.43. Early on in this review I publicly indicated that integrity/anti-corruption agencies should have the same access to Schedule 1 TOLA powers as police do. I note that, at present, there is no federal anti-corruption commission in existence, but if one were to come into existence (as has been publicly foreshadowed) then it too should enjoy those powers.

10.44. The rationale for the extension of these powers to such agencies is clear. They are already empowered under other legislative schemes to exercise various investigative powers, including, for instance, the power to make requests under

s 313 of the Telecommunications Act and the power to obtain warrants to lawfully intercept communications under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act). Indeed, the real question appears to be: why should integrity agencies be excluded from the exercise of these powers? There has been no real opposition to them being included.

10.45. I note in that regard that a Bill extending industry assistance powers to such agencies has previously been before Parliament. The Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 (Cth) sought to extend TOLA's definition of an interception agency to include State and federal agencies including, amongst others, the Independent Commission Against Corruption of New South Wales, Independent Broad-based Anti-corruption Commission of Victoria, and the Australian Commission for Law Enforcement Integrity. That Bill lapsed at the end of the last Parliament.

10.46. In their submissions and during the public hearings, the integrity commissions identified concrete disadvantage that flows from their exclusion from the power to issue industry assistance notices.

10.47. Mr Shane Butler, for the NSW Law Enforcement Conduct Commission, provided a case study in which:

a. Facebook had declined to assist in identifying IP addresses associated with racist and defamatory posts about a member of Parliament. Those IP addresses would have facilitated the identification of the alleged perpetrators (understood to be NSW Police officers).

b. No prosecution could proceed in the absence of that evidence.

c. Section 313 was not available in the circumstances, given Facebook is not an Australian carrier or carriage service provider.[442]

10.48. Ms Bernadette Dubois, representing the NSW Independent Commission Against Corruption, noted 2 further disadvantages with her agency's exclusion from Part 15 powers:

a. It meant that those agencies were not included in meetings between interception agencies addressing new developments in technology, which means that the agencies are not privy to that information.

b. While noting that integrity agencies have the power to make requests of carriers and carriage service providers under s 313 of the Telecommunications Act, the integrity agencies' exclusion from the exercise of Part 15 powers might signal to carriers and carriage service providers that are also DCPs that the

[442] Ibid 27–28.

integrity agencies are not entitled to the same degree of assistance as interception agencies that have been granted powers by Schedule 1.[443]

10.49. It is clear from the submissions I have received that these agencies face the same challenges in fulfilling their mandate as a consequence of the growth in encryption of communications as do police, and many of the agencies have a statutory role to investigate alleged police corruption. Further, Mr Butler noted during the public hearings that the persons of interest to his agency's investigations are 'very surveillance aware'.[444] Those persons are therefore more likely than ordinary members of the community to seek out and to use encrypted or otherwise protected means of communication.

10.50. For these reasons, it is necessary and **I conclude that State and Territory anti-corruption commissions should be given power to agree to or apply for all 3 types of industry assistance notice – that is, TARs, TANs and TCNs. This power should also be given to the foreshadowed Commonwealth Integrity Commission, when and if it is established.**

10.51. I consider it especially important that these commissions, which perform an important function in holding Government agencies and personnel to account, are empowered to exercise these investigative tools of their own accord without the need to call on any other agency or branch of Government, especially where they have the capacity to investigate them.

10.52. In relation to TCNs, it is usually inappropriate for any minister (rather than an independent judge or tribunal member) to be privy to the detail of an integrity agency's ongoing investigations. That will be especially so once there is a Commonwealth Integrity Commission. In relation to TANs, integrity commissions currently need to obtain TIA Act warrants in respect of telecommunications interception, just as police do, from eligible judges or AAT members. This accords with my recommendations.

10.53. I also consider that it is inappropriate for State and Territory police to have their powers approved the AFP. Therefore, **I conclude that the AFP should no longer have any role in the consideration of industry assistance notices requested by or issued on behalf of State and Territory police**.

10.54. I now turn to the final major complaint about Schedule 1.

[443] Ibid 23, 33.
[444] Ibid 26.

Key definitions

Systemic weakness and systemic vulnerability

10.55. As will be clear from the stakeholder discussion on this point, during my review I have received many submissions that are critical of both the definition and operation of key terms, primarily the definitions of 'systemic weakness' and 'systemic vulnerability'. Those definitions are contained in s 317B:

a. ***systemic vulnerability*** *means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified; and*

b. ***systemic weakness*** *means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*

10.56. Those terms are also given content – in terms of what they do and do not include – by the operative provision in which they feature – namely, s 317ZG, which provides:

> *317ZG Designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability etc.*
>
> *(1) A technical assistance request, technical assistance notice or technical capability notice must not have the effect of:*
>
> > *(a) requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection; or*
> >
> > *(b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.*
>
> *(2) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection includes a reference to implement or build a new decryption capability in relation to a form of electronic protection.*

(3) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection includes a reference to one or more actions that would render systemic methods of authentication or encryption less effective.

(4) Subsections (2) and (3) are enacted for the avoidance of doubt.

(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.

(4B) In a case where a vulnerability is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic vulnerability into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.

(4C) For the purposes of subsections (4A) and (4B), an act or thing will, or is likely to, jeopardise the security of information if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party.

(5) A technical assistance request, technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).

Removal of references to 'systemic vulnerability'

10.57. There seems to be little if any difference conceptually or in normal language or technical usage between a 'systemic weakness' and 'systemic vulnerability'. A 'weakness' and a 'vulnerability' are synonymous, at least in the present context. If a 'weakness' is something that is at risk of exploitation then it seems equally accurate to describe it as a 'vulnerability'. Further, none of the materials I have seen, including in response to s 24 notices I issued to police and intelligence agencies, indicated that either of the concepts had any meaning or operation that distinguished one from the other. To the extent that the terms are already used interchangeably in industry and public discourse, there should be no further need to use both in the legislation, especially where they are defined separately. Separate definitions for the same thing invites confusion.

10.58. Therefore, **I conclude that all references to 'systemic vulnerability' in Schedule 1 should be removed, as it is redundant**.

Provide statutory examples in the definitions of 'class of technology' and 'target technology' in relation to 'systemic weakness'

10.59. A point raised in numerous submissions[445] is the absence of any useful definitional examples of key terms associated with the concepts of 'systemic weakness' and 'systemic vulnerability'. To the extent that technical definitions are retained in the Act, the meaning should be clarified, including through the use of examples in the legislation itself (not just in the Explanatory Memorandum).[446]

10.60. One such example is 'whole class of technology' as used in the definition of each of these terms in s 317B, although it is not defined itself. Various submitters argued that, in the absence of a definition of 'whole class of technology' in Part 15 of the Telecommunications Act, it is simply not possible to say with any confidence what amounts to a 'class of technology', let alone a '*whole* class of technology'. The term is used in the legislation in contrast to the term 'target technology', which is defined in s 317B in the case of customer equipment, say a mobile device, as:

> *For the purposes of this Part, a particular item of customer equipment used, or likely to be used, (whether directly or indirectly) by a particular person is a* target technology *that is connected with that person.*

10.61. At the public hearing, Mr Murray of Electronic Frontiers submitted that the term 'target technology' requires clearer guidance because it is unclear, for instance, how it would apply to the Facebook Messenger application.[447] Would Facebook Messenger amount to a 'technology' if deployed on a single device? Would Facebook Messenger be classed as a 'whole class of technology' to the extent it operated as an application on all devices around the world, or the totality of a network, or something located on a server either inside or outside Australia?

---

[445] See, for example, the following submissions to the review: Atlassian, No 17 (4); Google, No 19 (1–3); Communications Alliance, No 15 (5); Australian Human Rights Commission, No 30 ([85]); and the Law Council of Australia, No 45 (8).

[446] *Re Bolton; Ex Parte Douglas Beane* [1987] HCA 12; 162 CLR 514 is a leading example of the error of placing too much faith in secondary material when it comes to judicial interpretation of laws.

[447] Evidence of Mr Murray, on behalf of Electronic Frontiers: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 71.

10.62. Submitters proposed various solutions. Some proposed that the definitions be repealed in their entirety. Others, including the Law Council of Australia,[448] highlighted concerns with the existing definitions but expressly disclaimed any desire to be involved in the process of redrafting them. Some industry representatives indicated their willingness to consult with Government to achieve more useful definitions or provided alternative definitions of their own.[449]

10.63. **I conclude that the definition of 'target technology' in s 317B should be clarified through the use of non-exhaustive statutory examples to clarify it refers to the specific instance used by the intended target.** For example, whether it includes:

a. the mobile phone service as provided only to one or more specified mobile phone numbers

b. a particular physical device such as the mobile phone that belongs to a target?

10.64. 'Class of technology' can then be defined through examples of services used by a group of users broader than the intended target – for example, all Telstra mobile phone subscribers or all subscribers in a particular location.

Amending s 317ZG to focus on material risk

10.65. Turning next to what the limitations in these definitions seek to achieve, there is general agreement across Government, industry and civil society that the legislation should not permit actions which create an unacceptable risk of compromising the security of users of a DCP's services who are not the subject of the agency's investigations. That begs the question: what is an acceptable level of risk? Some have argued that *any* risk at all is unacceptable, but that approach would make the expression unworkable.

10.66. I am persuaded from the submissions that the most effective approach to clarify the intended prohibition on systemic weakness is to focus on 'prohibited effects' so as to avoid unacceptable risks to the security of users who are not the intended target of an agency's investigations or operations. Then independent persons issuing TANs

[448] Evidence of Mr Howell, on behalf of the Australian Human Rights Commission: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 45–46.

[449] See, for example, the evidence of Mr Stanton on behalf of the Communications Alliance: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 116; and the evidence of Mr Zhang on behalf of Atlassian: ibid 84.

and TCNs would be given access to expert technical advice in a forum which allows DCPs to effectively litigate such issues.

10.67. As far as amending s 317ZG is concerned, the uncertainty comes from the terms of s 317ZG(4A) and 4(B). If there is only a systemic weakness, not a vulnerability, then sub-s (4B) can be repealed. Sub-section (4B) presently states that a systemic weakness 'includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person'. Sub-section (4C) provides that an 'act or thing will, or is likely to, jeopardise the security of any information held by any other person' where it 'creates a material risk that otherwise secure information can be accessed by an unauthorised third party'.

10.68. **I conclude that s 317ZG(4A) should state prohibited effects as follows:**

> ***(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in sub-s (1)(a) to implement or build a systemic weakness into a form of electronic protection means a reference to any act or thing that creates a material risk that otherwise secure information will be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.***

I further conclude that the following definitions should be introduced:

a. **'Otherwise secure information' means 'information of any person who is not the subject, or is not communicating with the subject, of an investigation'.**

b. **'Unauthorised third party' means 'anyone other than a party to the communication, the agency requesting the relevant technical assistance request, technical assistance notice or technical capability notice and/or integrity agencies'.**

10.69. The assessment of the material risk as redefined would be for the independent issuer of the TAN or TCN to determine.

Technical expertise

10.70. A regular complaint in non-Government submissions concerned the absence of independent technical assessment of, or advice concerning, proposed TANs in relation to such matters as whether the TAN met the statutory definitions:

a. of being reasonable and proportionate, and technically feasible, or

b. would result in a systemic weakness or systemic vulnerability.

10.71. There is presently a legal obligation for the issuing authority to obtain a technical assessment or advice only if a DCP requests an assessment in the case of a proposed TCN. If that occurs, the assessors must consider these matters mentioned in the previous paragraph as well as 'whether the proposed technical capability notice is the least intrusive measure that would be effective in achieving the legitimate objective of the proposed technical capability notice'.

10.72. It is, I hope, clear from the section on 'systemic weakness' and 'systemic vulnerability' above, as well as Chapters 4 and 5 of this report, that there are real technical complexities involved, which means that the issuer of a TAN or TCN will certainly need expert advice to properly appreciate what is being proposed and bring that appreciation to bear in making a decision. Undoubtedly, both security and law enforcement agencies engage technical experts of the highest calibre to advise and counsel agency heads, but these personnel are, quite properly, acting in the interests of their respective agencies. Therefore, in addition to concluding, as I have, that TANs and TCNs be issued by persons who are, and are seen to be, independent, those persons must have access to technical expertise.

10.73. For all of these reasons, **I conclude that Part 15 of the Telecommunications Act should be amended such that the head of an interception agency no longer has the power to independently issue a TAN and the Attorney-General no longer has the power to issue a TCN on the application of the head of an interception agency. I conclude that the legislation should be amended to provide instead that, in each case, the industry assistance notice is to be issued by an independent issuing authority with access to technical expertise**.

10.74. Before explaining the details of that recommendation, I now turn to the UK's experience with a similar arrangement.

UK Investigatory Powers Commissioner's Office

10.75. Following publication of *A Question of Trust*, the UK IP Act was enacted in November 2016. It consolidated a number of existing investigatory powers relating to the interception of communications, the retention and acquisition of communications data, equipment interference, and the acquisition of bulk data – namely, how public authorities and specific persons can:

a. obtain warrants (bulk and targeted) to intercept communications, interfere with telecommunications equipment, and obtain bulk personal datasets[450]

[450] As MI5 explains:

What are bulk personal datasets?

Bulk personal datasets (BPDs) are sets of personal information about a large number of individuals, the majority of whom will not be of any interest to MI5. The datasets

b. receive authorisation to obtain communications data

c. issue notices requiring telecommunications operators to:

   – retain communications data

   – engage in conduct necessary in the interests of national security

   – secure or develop their technical capability to assist intelligence agencies.

10.76. The IP Act established a number of entities and roles involved in these processes, including:

a. a senior serving or former judge, called the Investigatory Powers Commissioner (IPC) – initially Lord Justice Fulford, a senior serving judge, now the Rt Hon Sir Brian Leveson, a senior former judge – who reviews the exercise of powers under the IP Act and other relevant legislation and applies a double-lock on a decision by, for example, a Secretary of State to issue a sensitive or intrusive warrant

b. the double-lock can also be exercised by Judicial Commissioners, who are distinguished, senior, retired judges

c. the Technology Advisory Panel, which provides ongoing advice to the IPC about technological developments relating to the use of powers under the IP Act

d. the Technical Advisory Board, which must be consulted during the review of decisions relating to certain notices.[451]

---

are held on electronic systems for the purposes of analysis, although analysts will only actually look at the data relating to the minority who are of intelligence interest. Examples of these datasets include the electoral roll, telephone directories or travel-related data.

What are bulk personal datasets used for?

BPDs are essential in helping MI5 identify subjects of interest or individuals who surface during the course of an investigation, to establish links between individuals and groups, to better understand a subject of interest's behaviour and connections, and to quickly exclude the innocent. In short, BPDs enable MI5 to join the dots in an investigation and to focus its attention on individuals or organisations that threaten national security. The analysis of BPD is a critical part of our response to the increasingly complicated and challenging task of defending the UK's interests and protecting its citizens in a digital age.'

Security Service MI5, 'Bulk Data' (Web Page) <https://www.mi5.gov.uk/bulk-data>.

[451] The Technical Advisory Board (TAB) advises the Home Secretary on whether the obligations imposed on communications service providers (CSPs) under the terms of Regulation of Investigatory Powers Act (RIPA) are reasonable. The TAB has 2 functions: In accordance with section 12(9), the TAB must be consulted before the Home Secretary makes an order under s 12(1) of the 2000 Act, imposing obligations on CSPs. In accordance

10.77. When a secretary of State (that is, a minister) approves those warrants, their decision is subject to a 'double-lock' mechanism, so that a judicial commissioner, considering such matters as necessity, proportionality and lawfulness, must approve the decision to issue a warrant before the warrant operates: no approval, no warrant.

10.78. A judicial commissioner refusing to approve a warrant must set out written reasons for the refusal. An applicant may ask the IPC personally to reconsider an application that a judicial commissioner has refused. If the IPC also refuses to approve the warrant, there is no right of appeal and the warrant cannot be issued.

10.79. There are provisions in the IP Act for urgent applications, as well as safeguards for protecting legal privilege and confidential journalistic material, including sources. IPCO has inspectors who, along with the IPC, the judicial commissioners and the Technology Advisory Panel, conduct the functions which the Ombudsman and the IGIS conduct in Australia. Based on detailed briefings from IPCO and the agencies it supervises, and discussions in the UK and the US, I consider that the IPCO model has worked well in the UK and I consider certain aspects of its operation are both relevant and useful to adopt in the Australian context under TOLA.

with s 12(5), a notice issued to a CSP under s 12(2), the effect of which is to trigger the imposition of the obligations provided for in the s 12(1) order, may be referred by the CSP to the TAB within 28 days of the notice's issue. In accordance with s 12(6), the TAB shall consider the requirements set out in the notice and their financial consequences for the CSP. If appropriate, the Chairman may seek expert advice from outside the TAB. The TAB will then report its views to the CSP and to the Home Secretary and to the CSP making the referral. After considering any report from the TAB relating to a notice, the Home Secretary may either withdraw the notice or give a further notice under s 12(2) of the 2000 Act confirming its effect, with or without modifications.

11. FINDINGS: AN AUSTRALIAN IPCO AND A FURTHER ROLE FOR THE AAT

11.1. In the previous chapter I concluded that Technical Assistance Requests (TANS) and Technical Capability Notices (TCNs) (but not Technical Assistance Notices (TARs)) should be issued independently of government and agencies, by persons or bodies with access to technical advice. I noted the UK's Investigatory Powers Commissioner's Office (IPCO) model, which works well in relation to similar powers. In this chapter I conclude:

a. that approval of, and hearings concerning, TANs and TCNs be by the Administrative Appeals Tribunal (AAT) sitting in a new Investigatory Powers Division, with powers and procedures based upon the existing Security Division

b. the creation of a new statutory office – the Australian Investigatory Powers Commissioner (IPC), who would also be appointed as a part-time Deputy President within the AAT, assisted by eminent technical advisers and able to share information with oversight bodies such as the Inspector-General of Intelligence and Security (IGIS), the Ombudsman and State and Territory counterparts.

11.2. In this chapter I do not attempt to provide every detail of such a new office. That can be done if it is adopted by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and Government, and it could then be done by a newly appointed IPC. Rather, I here set out the key principles and their rationale.

The function of issuing TANs and TCNs

11.3. As I concluded in the preceding chapter, the industry assistance notice is to be issued by an independent issuing authority with access to technical expertise.

11.4. The issuing body will therefore need to:

a. independently consider whether the TAN or TCN should be issued and, in so doing, consider such matters in Schedule 1 as whether:

b. on the evidence before it, the notice, if issued, would be:

– 'reasonable and proportionate' weighing up the defined relevant considerations and such other matters as are considered appropriate

– 'practicable'

- 'technically feasible'
- likely to breach the prohibitions on creating or maintaining a 'systemic weakness' (as this term now encompasses 'systemic vulnerability').

11.5. For TCNs, the issuing authority should also consider the impact of the notice on the efficiency and international competitiveness of the Australian telecommunications industry as the Minister for Communications now does. The Attorney-General should retain an important gatekeeping role, as with the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) (IPO Bill) and the current terms of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) relating to Questioning Warrants, and indeed some parts of TOLA Schedule 5 – namely, his or her approval should be required before a federal agency makes an application for a TCN to the AAT. However, the Attorney-General's approval should not be required for any State or Territory body, or for the Commonwealth Integrity Commission if and when established.

11.6. One option for the Australian context which I have considered during my review is the creation of a new independent tribunal that resembles the UK IPCO, for the sole purpose of exercising functions in relation to TOLA powers. Although I have little doubt that TANs and TCNs will start to be issued, the lack of TANs and TCNs issued to date does not justify creation of a new institution for the sole purpose of exercising TOLA-related functions. Instead, by appointing a senior retired judge as an Australian IPC, the new role can be established and the appointee can be joined by part-time retired judges as the workload requires. The appointees would sit in a newly-established Investigatory Powers Division of the AAT. The division would be constituted for this purpose by the IPC as a Deputy President, another part-time Deputy President and a technical expert who would be a part-time Senior Member of the AAT. Although by s 6(2) of the INSLM Act it is not my role 'to review the priorities of, and use of resources by, agencies', I here observe that the history of my own office is an example of how a small, efficient and low-cost office can be established by a shortly stated statute.

11.7. I next explain why I have concluded that the function should be vested in the AAT, but not a court, and that the power should not be exercised *persona designata*.

Courts, tribunals and persona designata

11.8. I am not saying that such intrusive powers could not be vested in a court, as they are powers which, while usually seen as executive rather than judicial in nature, are of a type which would take their constitutional character from the institution in

which they were vested. This is an example of the 'chameleon doctrine'.[452] As Gaudron J put it in *Re Dingjan; Ex parte Wagner*:[453]

> *[S]ome powers are essentially judicial so that they can be conferred by the Commonwealth only on courts named or designated in Ch III of the Constitution,[454] while others take their character from the tribunal in which they are reposed and the way in which they are to be exercised and, thus, may be conferred on courts or other tribunals as the Parliament chooses.*[455]

11.9. But a fundamental difficulty with vesting the issuing function in a court, which must generally sit in public and apply the rules of evidence, and which must by application of the principles of procedural fairness ensure each party sees and can test the evidence of the other party, is dealing with the inevitable and justifiable wishes of:

a. Designated Communications Providers (DCPs) to keep from their competitors and from the requesting agency such highly sensitive commercial-in-confidence information as source codes[456]

b. agencies to keep secret their operational objectives and whether in that regard the notice is 'necessary', as well as such matters as 'the interests of national security', 'the interests of law enforcement' and, if my recommendation is

---

[452] In *Pasini v United Mexican States* [2002] HCA 3; (2002) 209 CLR 246, 253–254 [12] Gleeson CJ, Gaudron, McHugh and Gummow JJ said: 'The line of authorities establishing that there are some powers which appropriately may be treated as administrative when conferred on an administrative body and as judicial when conferred on a federal court or court exercising federal jurisdiction recently was affirmed in *H A Bachrach Pty Ltd v Queensland* and *Sue v Hill*.'

[453] [1995] HCA 16; (1995) 183 CLR 323 at 360.

[454] *Waterside Workers' Federation* [1918] HCA 56; (1918) 25 CLR 434, 467; *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254, 270, 296, 314, 338.

[455] *Precision Data Holdings Ltd v Wills* (1991) 173 CLR 167, 189. See also *R v Davison* [1954] HCA 46; (1954) 90 CLR 353, 370; *R v Hegarty; Ex parte City of Salisbury* [1981] HCA 51; (1981) 147 CLR 617, 628; *Re Ranger Uranium Mines* (1987) 163 CLR 656, 665–666; *Harris v Caladine* [1991] HCA 9; (1991) 172 CLR 84, 93, 147–148.

[456] See, for example, regarding industry, the following submissions to the review: BSA The Software Alliance, No 25(8, point 5); Mozilla, No 49 (5). Also see the evidence of Internet Australia: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 53; Department of Home Affairs, ibid 197, 199. Regarding agencies, see the following submissions to the review: Australian Federal Police, No 27 ([53]–[55]); and Department of Home Affairs, No 26 ([187]–[190]). See also the evidence of Ms Vonthethoff: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 198–199.

> followed 'the interests of integrity agencies', and also 'whether the requirements … are the least intrusive form of industry assistance [in relation to] persons whose activities are not of interest to ASIO or interception agencies'.

11.10. Although it may be possible to have a court hearing in camera, and to alter the rules of evidence, an inquisitorial process whereby the court does not share information of one party creates constitutional problems, running the risk of invalidating the process altogether. This issue was at least touched on by the High Court in the control order test case of *Thomas v Mowbray*[457] in relation to the capacity of the Australian Federal Police to deny information to the potential controlee at least at the interlocutory stage.[458] In contrast, the Security Division of the AAT operates under valid provisions which are, or could be made, flexible enough to allow those competing desires to be met.

11.11. The next question is whether the functions should be exercised by AAT members *persona designata*.

11.12. In *Wainohu v State of NSW*,[459] French CJ said, 'The term "*persona designata*" means "[a] person pointed out or described as an individual, as opposed to a person ascertained as a member of a class, or as filling a particular character".'[460]

11.13. A number of cases have established that judges of federal courts may exercise administrative functions such as issuing search warrants provided that, as it was put in *Hilton v Wells*[461] and confirmed in *Grollo v Palmer*:[462]

> *No non-judicial function that is not incidental to a judicial function can be conferred without the judge's consent [and] … no function can be conferred that is incompatible either with the judge's performance of his or her judicial functions or with the proper discharge by the judiciary of its responsibilities as an institution exercising judicial power*.[463]

11.14. Although it may therefore be permissible for judges (and certainly tribunal members who are not serving judges) to exercise this administrative function of issuing TANs

---

[457] [2007] HCA 33.

[458] See, for example, ibid, Gummow and Crennan JJ at 122–125.

[459] [2011] HCA 24.

[460] Ibid [34], footnotes omitted.

[461] [1985] HCA 16; (1985) 157 CLR 57.

[462] [1995] HCA 26; (1995) 184 CLR 348.

[463] (1995) 184 CLR 348, 364–365. Cited by French CJ in *Wainohu v State of NSW* [2011] HCA 24 [38].

and TCNs *persona designata*, whereby notices are issued *ex parte* without any type of hearing, **I conclude that such powers should not be exercised persona designata**.

11.15. *First*, and most fundamentally, although the issue of TANS and TCNs is an administrative function, it is critical to my recommendations not only that there be an independent, technically informed issuer but also that a DCP can choose to contest the issue of TAN/TCN. In such cases the issuer must have the capacity to hear and determine a dispute rather than proceed ex parte.

11.16. *Secondly*, there is some evidence that the *persona designata* warrant-issuing function does not lend itself to taking the time to understand the complex policy and technical factors which will be required for at least the initial issue of TANs and TCNs. Thus at a Senate additional estimates hearing on 3 March 2020 the Registrar of the AAT provided information on a recent survey of the length of time AAT members take to consider applications for warrants under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) and the *Surveillance Devices Act 2004* (Cth) (SD Act). She said:

a. the average time for an AAT member to consider a TIA Act warrant application may be as short as 18 minutes

b. the average appointment time for an AAT member to consider a SD Act warrant application may be as short as 24 minutes, with one instance of a TIA or SD Act warrant appointment apparently lasting one minute.[464]

11.17. While the relevant members may have reviewed related documents ahead of the appointment (outside of the times above), I consider this time on its face will be insufficient for the TAN and TCN roles. This seemingly short consideration of surveillance and access warrants may perhaps be attributed to the members having to act as *persona designata* and therefore not being able to draw on AAT resources in issuing the warrant as such tasks are seen as at least peripheral to, and perhaps a distraction from, members' tribunal duties.

11.18. *Thirdly*, a key part of the success of the UK IPCO is that the IPC and the judicial commissioners become very familiar with the work and the technology used by the agencies seeking the issue of intrusive warrants and bring that knowledge to bear in considering subsequent applications, ensuring both insight and efficiency. The operation of the *persona designata* function can mean that the eligible judge or tribunal member never exercises the same function twice and cannot build up experience and knowledge.

[464] Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Senate Additional Estimates* (3 March 2020) 113–114.

11.19. **I therefore conclude that the powers of approval of TANs and TCNs, presently vested in agency heads (for TANs) and the Attorney-General (for TCNs), should instead be vested in the AAT and assigned to a new Investigatory Powers Division using the Security Division model of powers, further details of which follow.**

An Australian Investigatory Powers Commissioner

11.20. **I conclude that there should be a new statutory office called the Investigatory Powers Commissioner, (IPC). The Commissioner would be appointed as the head of the new Investigatory Powers Division and perform the approval function of that division as concluded above. In recognition of the importance of the position and its need to be, and be seen to be, filled by someone who is independent of Government, eminent in the law and its application, and enjoying bipartisan support, I conclude that the IPC should be a retired judge of the Federal Court or the Supreme Court of a State or Territory. The IPC would be appointed by the Governor-General, on the advice of the Attorney-General, following mandatory consultation on the appointment with the Leader of the Opposition. I would expect there would also be consultation with industry, but I would not mandate it.**

11.21. The IPC would be appointed as a part-time Deputy President of the AAT and designated as the Head of the new Investigatory Powers Division of the AAT. In addition to functions in that role, the IPC would have the following functions:

a. concurring in the appointment, as the volume of work requires, by the Governor-General of a suitable number of similarly qualified Assistant Commissioners who would also be assigned to the new Investigatory Powers Division and be appointed as part-time AAT Deputy Presidents. They could be drawn from existing Deputy Presidents if qualified and should be eminent legal experts

b. concurring in the appointment by the Governor-General of a suitable number of eminent, independent technical experts, who would also be assigned to the new Investigatory Powers Division as part time Senior Members. In order to encourage industry support, there should be mandatory consultation with industry groups as to who should be appointed to these roles

c. concurring in the appointment by the AAT President of a registrar of the new division who would not only ensure proper protection of sensitive and classified material but also, by bringing them to the Commissioner's attention, ensure 'deconfliction' of inconsistent or oppressive requests to DCPs

d. able to share information with other bodies, although it would not take over or be part of any such bodies. IPCO in the UK also performs the functions of the

IGIS and, to an extent, the Ombudsman, and State and Territory oversight bodies. It is important that each can share information with the others and that the Australian IPC and staff can accept invitations from, for example, the IGIS and Ombudsman to attend investigations and audits into the exercise of TANs and TCNs, and I so recommend

e. approving the prescribed form of TAN and TCN applications, issuing guidelines[465] and, with the concurrence of the AAT President, issuing practice notes for the Investigatory Powers Division

f. providing to the Attorney-General and the PJCIS with an annual report on the operation of Schedule 1 and such other functions as may later be conferred upon the Commissioner and the division, with the capacity to create a classified annexure to those reports as necessary. The unclassified reports would be required to be tabled in Parliament within 15 sitting days of receipt.

Technical advisers

11.22. One of the strengths of IPCO in the UK is that the IPC and the judicial commissioners, assisted by Technical Advisory Panel members, build up deep experience in the use to which the latest technology is put by the particular requesting agencies. This allows them to consider new requests expeditiously and to understand the potentially difficult and complex questions involved.

11.23. The UK Technical Advisory Panel's role is stated in the *Technology Advisory Panel Working Protocol* as follows:

> *The TAP has a dual function under the Act: both to advise about the impact of changing technology, and also to advise about the availability and developments of techniques to use investigatory powers while minimising interference with privacy. In the definition of the panel's remit, 'technology' will be taken to be interpreted broadly, to include all relevant areas of science and mathematics. However, the technological remit of the Panel should not be unduly diluted through consideration of matters of law, partisan politics or moral philosophy.*
>
> *Given that a key role overarching all the Commissioner's work is to ensure that powers are used in such a way as to minimise interference with privacy, advice may be sought from the TAP on any scientific or technological aspect of methods being used in the exercise of investigatory powers, either in a specific*

[465] For example, the Commissioner could be given the power to approve guidelines in relation to notices sought regarding, or which would directly affect parliamentarians, lawyers, and journalists.

> *case or in a more general context. In addition, advice may be sought about other relevant technical matters within the capabilities of the TAP, for example in support of the development and effectiveness of other core functions of the Commissioner's Office (IPCO), such as inspections and thematic reviews, and in support of any decision by a Judicial Commissioner exercising their powers to approve a warrant or other authorisation under the Act. The TAP is not a decision-making body. Its advice cannot constrain any decision of the Commissioner or of any part of the Government.*[466]

11.24. **I conclude that there should be appointed part-time to the AAT in the new IPD a group of eminent, technically qualified persons drawn from Government, industry and academia and covering the range of scientific and technical disciplines required.**

11.25. This proposal draws on the United Kingdom's IPCO model – in particular, the Technical Advisory Board as well as the Technical Advisory Panel that forms part of that model. It differs from the UK's Technical Advisory Board in that it envisages the appointment of these people to the position of a decision-maker (that is, through each person's appointment as a part-time Senior Member of the AAT) and not merely the person's performance of an advisory role.

11.26. It also reflects, to some degree, the existing legislation's concept of a technically qualified 'assessor'[467] who reports on technological developments. But this proposal differs from the concept of a technically qualified assessor under the existing legislation. I envisage that, through this proposal, a standing pool of technical advisers will be created, not merely the ad-hoc selection of a technically-qualified assessor from time to time.

11.27. I consider the creation of a standing pool of technical experts, appointed also as members of the AAT, carries significant advantages. First, it would bring together a group of people with appropriate skills, qualifications and experience to properly grapple with the complex technological issues to which TANs and TCNs might be expected to give rise. That alone would be a significant improvement on the status quo, as at present there is no requirement that any person issuing an industry assistance notice have any technical expertise.

---

[466] Technology Advisory Panel, *Technology Advisory Panel Working Protocol*, March 2019, 1 <https://www.ipco.org.uk/docs/TAP%20working%20protocol%20(25%20March%202019)%20FINAL.pdf>.

[467] *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), s 317WA generally, but particularly sub-s (4)(a).

11.28. Secondly, it is reasonable to expect that exposure to the issues to which industry assistance notices give rise will ensure that this group of people develops not only their technical knowledge over time but also their knowledge and understanding of Australia's security landscape. In my view, the development of a pool of people who understand both cutting-edge technology and the nuances of Australia's security challenges would bring significant advantages.

11.29. I have no doubt that, despite the skills shortage that presently exists in the technology sector, there exist within Australia sufficiently qualified technical experts who could form part of that group of technical experts. Indeed, during the public hearings, Ms Michelle Price of AustCyber – an independent body that receives federal funding for the purpose of increasing the Australian cyber sector – expressed her certainty that appropriately qualified experts can be found in Australia for that purpose.[468]

An Investigatory Powers Division of the AAT

11.30. The proposed Investigatory Powers Division would operate as follows:

a. It would comprise the Commissioner and Assistant Commissioners sitting as part-time Deputy Presidents, and part-time eminent technical persons sitting as part-time Senior Members. The *Administrative Appeals Tribunal Act 1975* (Cth) already deals suitably with how disagreements in multi-member panels are dealt with.

b. It would adapt suitable provisions applicable to the Security Division to ensure that a contested hearing can be held while preserving the quality of confidence residing in classified and commercial-in-confidence material.[469]

---

[468] See Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 131.

[469] For example, s 17F Assignment to Security Division; s 19E Constitution of Security Division; s 27AA Applications to Tribunal under Australian Security Intelligence Organisation Act; s 29B Notice of application – review of security assessment; s 30A Intervention by Attorney-General; s 35AA Orders for non-publication and non-disclosure – certain Security Division proceedings; s 36 Disclosure not required: Attorney-General's public interest certificate; s 38A Director-General of Security to lodge certain material with Tribunal; s 39A Procedure in Security Division review of security assessment; s 39B Certain documents and information not to be disclosed in Security Division review of security assessment; s 43 Tribunal's decision on review; s 43AAA Findings of Tribunal in Security

c. It would decide for itself, rather than on review, whether a TAN or TCN should be issued and, in that regard, whether the proposed notice was:

   – 'reasonable and proportionate' weighing up the defined relevant considerations and such other matters as are considered appropriate

   – 'practicable'

   – 'technically feasible'

   – likely to breach the prohibitions on creating or maintaining a 'systemic weakness'.

d. The agency seeking the issue of either notice would lodge an application with the Investigatory Powers Division – as with the IPO Bill, there is the option of the Australian Security Intelligence Organisation (ASIO) being required to first obtain the Attorney-General's consent to the application being made by the authorised ASIO employee to the nominated member.[470]

e. The Investigatory Powers Division, like the AAT, could inform itself as it thinks fit; consider material, whether or not it complies with the strict rules of evidence; and hear/receive evidence and submissions.

f. In some cases the TAN or TCN would be unopposed by the DCP, in which case the Division would still have to be satisfied the notice should be issued.

g. If the DCP opposes issue of the particular notice, the Division has the flexibility to fashion the type of hearing to the issues in dispute including directing the use of alternative dispute resolution to narrow the issues for determination.

h. The Investigatory Powers Division would comprise a mixture of the Deputy President / Commissioner (and Assistant Commissioners) and Senior Members with technical knowledge. Some hearings – for example, regarding whether a draft notice is likely to breach the prohibitions on creating or maintaining a 'systemic weakness' – will be complex and hard-fought litigation involving detailed findings on technical matters; and others may be less complex.

i. The Division would provide reasons, often with a classified annexure.

Division review of security assessment; s 44 Appeals to Federal Court of Australia from decisions of the Tribunal.

[470] Attorney-General's Department, Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, 8.

11.31. I again note that I am here setting out key principles and their rationale. There may well be other provisions which commend themselves to the PJCIS and to Government.

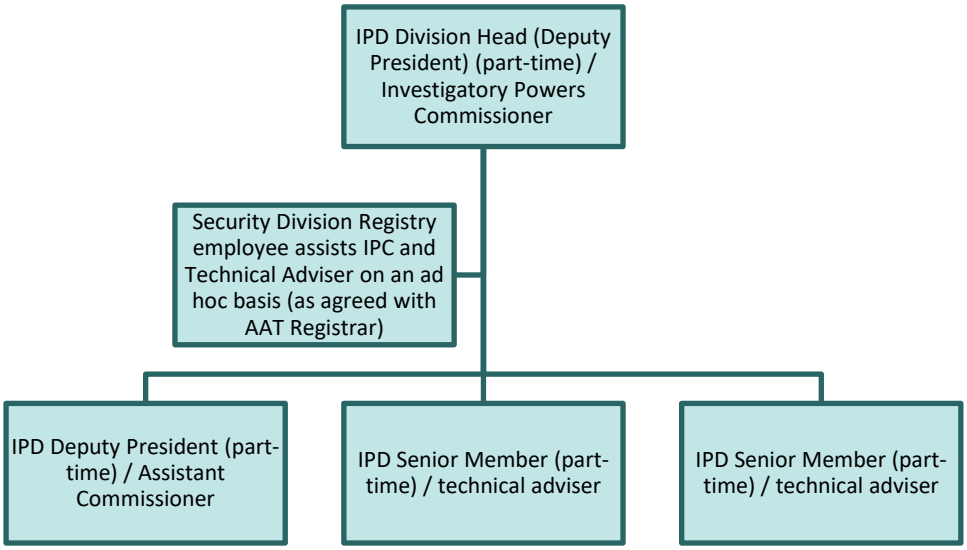

Figure 1: Phase 1 of the operation of the Investigatory Powers Division

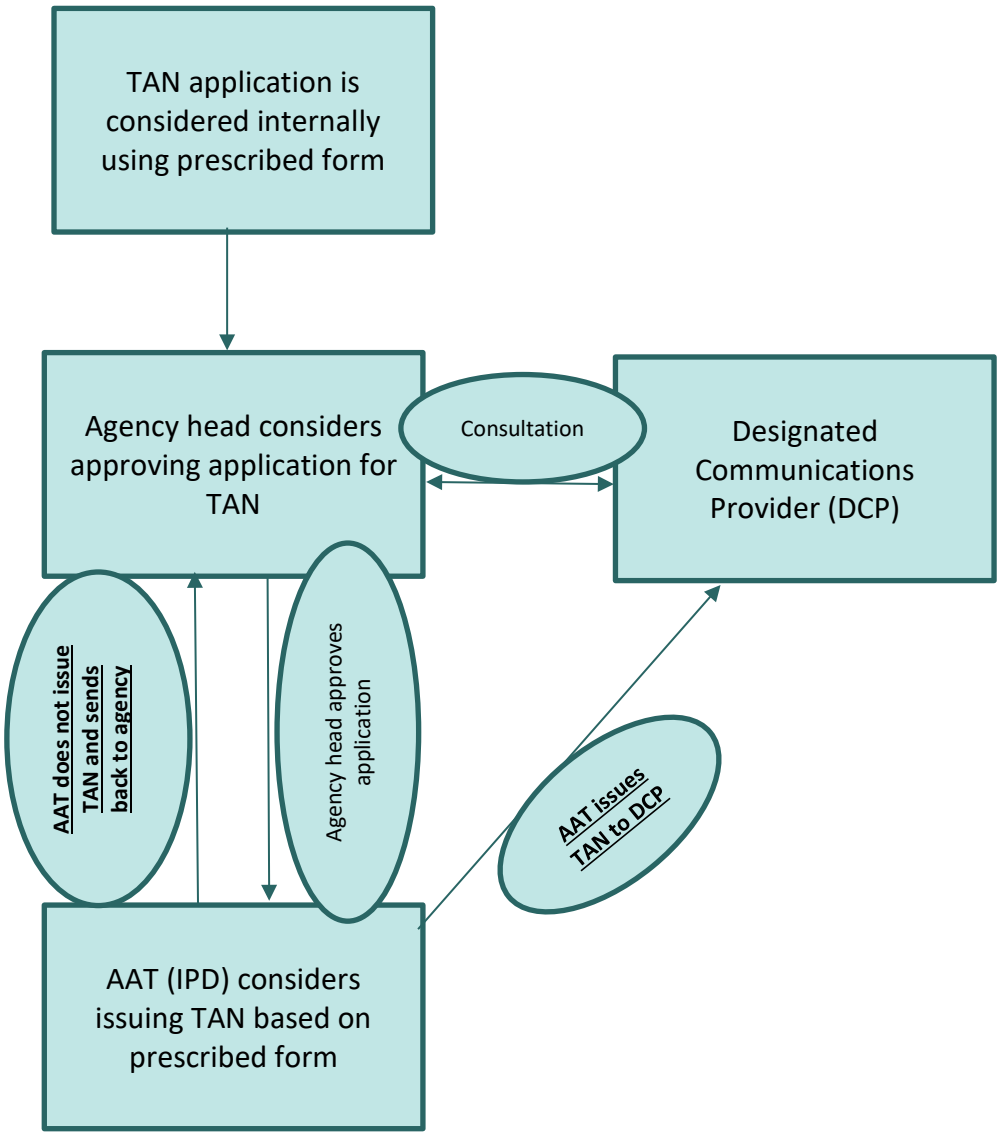

Figure 2: New process for Technical Assistance Notices (TANs)

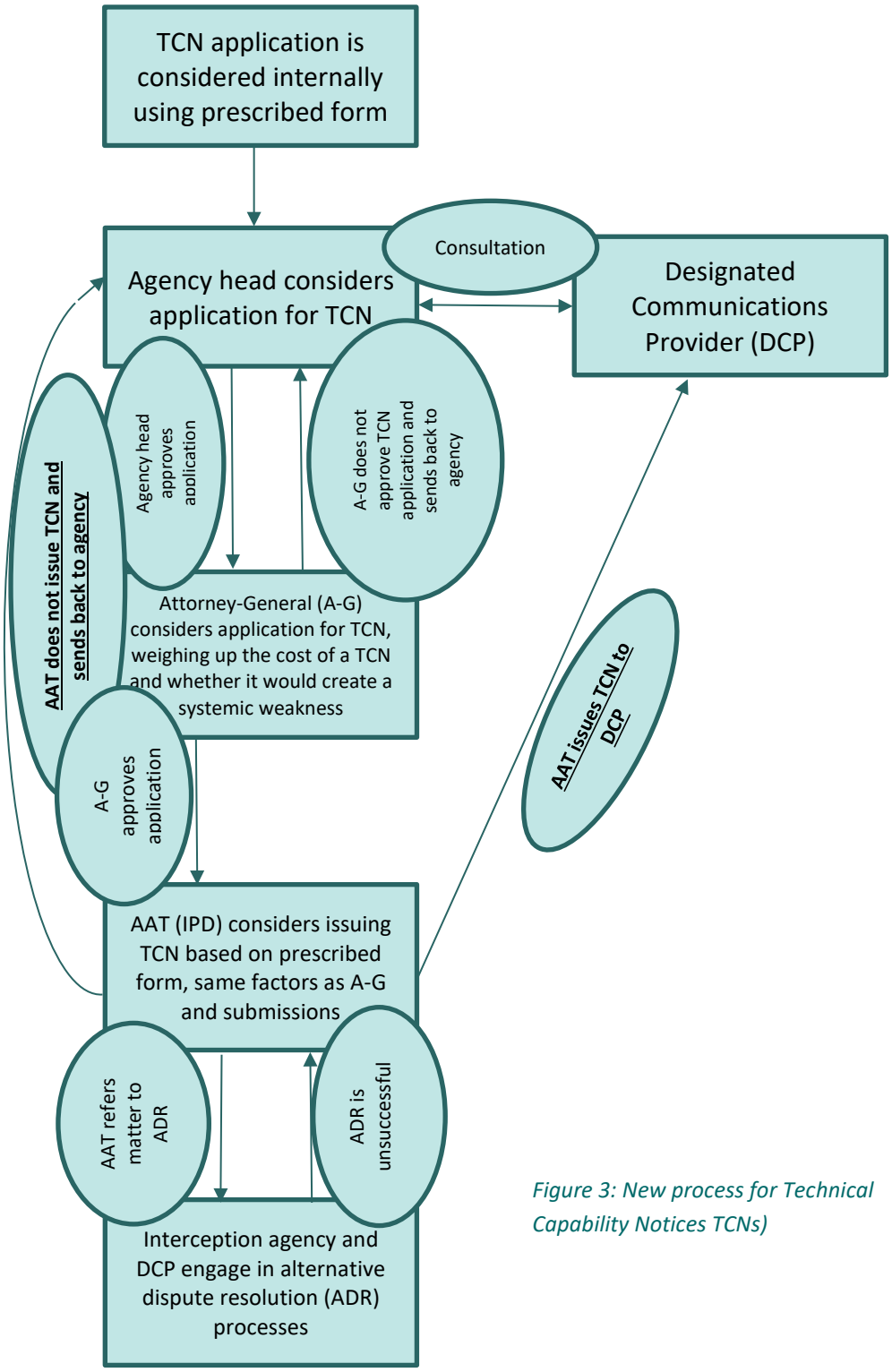

Figure 3: New process for Technical Capability Notices TCNs)

12. FINDINGS: SCHEDULES 2, 3, 4 & 5

Conclusions

All notices should issue under cover of a prescribed form

12.1. As part of my royal commission-like powers, I have had access to, and have received copies of, the Technical Assistance Requests (TARs) that various agencies have issued since Part 15 of the *Telecommunications Act 1997* (Cth) came into force. They vary between agencies, including in the information they contain that is directed toward recipients.

12.2. Industry assistance notices are significant instruments which provide for civil and some criminal immunity according to their terms and, in the case of notices, contain compulsory requirements. A Designated Communications Provider (DCP) on whom a TAR, Technical Assistance Notice (TAN) or Technical Capability Notice (TCN) is served should have no doubt as to its authenticity, what it requires, and what it does not – and cannot – require. A DCP and its staff that deal with various interception agencies and security agencies are entitled to expect that a document bearing such significant consequences will look broadly the same on each occasion, regardless of the agency at whose behest it issues.

12.3. I propose that the prescribed form would include key information as to, for instance, the 'listed acts or things' in respect of which the notice issues, the 'eligible activities' of the DCP to which it relates, and the rights and obligations of the DCP in relation to the notice. In this way, it will perhaps perform a similar function to the 'notice to occupier' that Australian Federal Police (AFP) members are required to serve on the occupier of premises during the execution of a *Crimes Act 1914* (Cth) s 3E search warrant. The inclusion of those details in a prescribed form would also assist agencies in compiling and reporting general information as to their use, which I address in more detail in recommendations later in this chapter.

12.4. During the public hearings, I was not made aware of any opposition to the creation of a prescribed form. The AFP indicated that it would have no objection to a form coming into effect.[471] Similarly, the Department of Home Affairs expressed no objection to the development of a prescribed form. The department noted that it

[471] See Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 182. See also evidence on behalf of ASIO by Mr Burgess, ibid 16.

had previously provided guidance documents to agencies intended to assist them in developing standardised forms for that same purpose.[472]

12.5. Accordingly, **I conclude that there be developed prescribed forms for TARs, TANs and TCNs, to be approved by the Investigatory Powers Commissioner (IPC) and used when the Administrative Appeals Tribunal (AAT) is issuing TANs and TCNs; and that each prescribed form set out the recipient's rights and obligations, and any other important information specific to the TAR, TAN or TCN in question.**

'Acts or things' listed in s 317E

12.6. Many of the industry submissions to my inquiry noted the breadth of the list of 'acts or things' in s 317E of the legislation that could be included in a TAR, TAN or TCN. This is true. For example, '(f) assisting with the testing, modification, development or maintenance of a technology or capability' could cover a very broad range of actions. Also, my review of some of the examples of TARs issued to date show that the requested actions could come under more than one heading in this list. I give more details of this in the classified annexure.

12.7. However, I am not persuaded that there is any benefit in making this defined list narrower or more specific. This would make the act very specific to technology as it currently exists and is perceived today, complicating the practical use of the legislation without necessarily providing any additional meaningful safeguards.

12.8. A better approach, as discussed elsewhere, is to focus on the effects and outcomes of the acts or things requested. This would address the legitimate concerns raised by industry and civil society – for example, the risks of systemic weakness; and the other decision-making criteria listed in the legislation.

12.9. This approach is also consistent with modern approaches to cybersecurity, which focus on principles and outcomes rather than specific technical controls that may or may not be relevant given the context and that may rapidly go out of date.

Width of the definition of 'Designated Communications Providers'

12.10. A number of non-Government submissions requested a more confined list of defined DCPs. I do not agree. First, the less extensive definition in s 313 of the Telecommunications Act does not match the wide variety of organisations that could do listed acts or things, whereas the DCP definition does. There is no merit in having gaps in the definition which might be used by the unscrupulous.

12.11. The more justified complaint in the submissions concerns which DCP to choose as a recipient of a request or notice if there is more than one who could do the listed

[472] Ibid 207.

acts or things under a Schedule 1 notice. That is a question of proportionality and it is answered by the recommendation concerning the AAT. The DCP can argue that, for example, issuing the notice on a DCP at a different point in the supply chain would be less intrusive on privacy of others, less likely to adversely impact international competitiveness, or less likely to result in a systemic weakness.

12.12. Some submitters have also expressed concern about the potential for a TAR, TAN or TCN to be agreed with or issued to an individual employee of a DCP. This would affect that employee's ability to seek legal or technical advice (discussed later). At the public hearing the Department of Home Affairs provided assurance that TOLA was not drafted with the intention that TARs, TANs and TCNs would be agreed with or issued to an individual employee (and the law would not be used in that way). However, it is necessary to put this issue beyond doubt.

12.13. Therefore, **I conclude that a 'Designated Communications Provider' should not be taken to include a natural person (where that natural person is an employee of a DCP) but only apply to natural persons insofar as required to capture sole traders**.

'Form of electronic protection' in s 317ZG

12.14. Other submissions concerned the concept of 'form of electronic protection' as used in s 317ZG of TOLA. The term 'electronic protection' is defined in s 317B in a manner that includes 'authentication' and 'encryption'. Various submissions indicated that that inclusive definition is too vague to provide any useful assistance.[473] I agree that, if this definition is to have utility in clarifying the operation of the legislation, it should also include non-exhaustive examples of what is excluded. **I conclude that the definition of 'electronic protection' in s 317B should also include non-exhaustive examples of what is excluded from its meaning.**

12.15. Examples could be given to clarify whether it was intended that weakening forms of physical protection is acceptable, as this can be limited to operation on a specific instance of the technology. In this case, an example not covered by the 'electronic protection' term may be assisting to bypass tamper detection mechanisms when opening up a mobile phone to access data stored on its electronic components inside.

[473] See Communications Alliance, Submission No 15 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 September 2019, 8, table item 1.

Recording and reporting on use of assistance orders

12.16. The reforms effected by TOLA introduced 2 new powers by which law enforcement officers or security officers can compel a person to provide assistance.[474] In addition, TOLA made certain amendments to the AFP's and the Australian Border Force's (ABF's) existing powers[475] to obtain assistance orders.[476]

12.17. At present, none of the agencies empowered to seek an assistance order has any obligation to report to an inspection agency on its use of that assistance order.

12.18. Various submissions identified the highly coercive effect of an assistance order, including on the privilege against self-incrimination.[477] On the other hand, agencies have emphasised the operational utility of an assistance order. For instance, assistance orders are routinely deployed to obtain a password so that an investigator can unlock a smartphone, laptop or other electronic device that might otherwise be unexaminable even though it was lawfully obtained under warrant.[478]

12.19. Without statistics on the frequency with which assistance orders are sought, obtained and executed, it is difficult for me to assess the competing arguments for and against their use, let alone to make any recommendations as to what, if any, amendments to those powers might be appropriate.

12.20. I note that the AFP provided information in response to the s 24 INSLM Act notice I issued on the Commissioner of the AFP indicating that the AFP often obtains s 3LA orders 'pre-emptively' (that is, at the time of obtaining a s 3E premises warrant) and that, in many circumstances, the orders are not served because they are not

---

[474] *Surveillance Devices Act 2004* (Cth), s 64A; *Australian Security Intelligence Organisation Act 1979* (Cth), s 34AAA.

[475] In the case of the AFP, *Crimes Act 1914* (Cth), s 3LA, as amended by Schedule 3 of TOLA; in the case of the ABF, *Customs Act 1901* (Cth), s 201A, as amended by Schedule 4 of TOLA.

[476] For clarity, I note that the 'assistance orders' to which I am referring here are not the 'industry assistance orders' contained in Part 15 of the *Telecommunications Act 1997* (Cth), as introduced by Schedule 1 of TOLA. Rather, they are powers to compel an individual to provide information and assistance to a law enforcement agency in particular circumstances.

[477] See, for example, the following submissions to the review: Australian Human Rights Commission, No 30, esp 77–80 of Annexure 1; also Riana Pfefferkorn, No 4 (2–3); Electronic Frontiers, No 47 (32–33); and the International Civil Liberties and Technology Coalition, No 5 (7).

[478]See Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 36.

required (for instance, because the person provides the information sought voluntarily and without the need to serve the notice).

12.21. For this reason, **I conclude that the reporting obligation for the AFP should be confined to an obligation to report on the number of assistance orders *executed* each year and should not extend to the number of *applications made* to a magistrate or other issuing officer or the number of those applications granted each year.**

12.22. Accordingly, **I conclude that the various assistance order provisions should be amended to mandate that the agency in question report to its inspection agency (that is, the Commonwealth Ombudsman, or the IGIS) as to the number of assistance orders that it executes each year and, other than for the Australian Security Intelligence Organisation (ASIO), publish those figures in the public annual reports of the relevant agencies and the oversight bodies. I conclude that statistics on the use of TOLA powers, including a broad description of the acts or things implemented, should be made public annually by the IPC (tabled in Parliament within 15 sitting days of receipt), provided that publication would not reveal operationally sensitive or classified information**.

12.23. **I conclude that ASIO's exercise of powers under Schedule 5 should be detailed in its annual report (in a classified appendix as necessary) and that this information be provided to the PJCIS, the Leader of the Opposition, the IGIS, the INSLM, the Attorney-General and the Minister for Home Affairs.**

Information sharing and disclosure

12.24. One of the major issues I encountered with public engagement in this review was the prohibition on public disclosure or discussion of the TAR/TAN/TCN information, outlined in Division 6 of TOLA. While my coercive powers enabled confidential discussion of this information, I consider that the prohibitions on disclosure are overly restrictive and undermine public confidence in the use of the provisions. They even limit what I can state in this public report. Additionally, the prohibitions on disclosure extend to Commonwealth officials acting in an official capacity. This could mean that agencies are prohibited from sharing information relevant to cyber or national security with partners simply because that information falls under the broad description of TAR/TAN/TCN information.

12.25. **I conclude that Commonwealth officials should be authorised to disclose TAR/TAN/TCN information to the public and to State, Territory and Commonwealth officials when that disclosure is in the national or public interest. A decision to disclose based on those factors may be made by the relevant agency or departmental head or the relevant minister.**

12.26. Another issue, mentioned briefly above, was the concern from industry submitters that, if a request is made or notice issued to an individual employee of a DCP, that employee would be unable to discuss the request or notice with management or lawyers, thereby prohibiting the employee from seeking technical or legal advice. The Department of Home Affairs advised that it is not intended that an individual employee would receive a request or notice and be unable to discuss it with management or lawyers and stated that:

> *It is not now and never has been intended that individual employees would be asked or required to provide assistance without informing their employer. While an individual employee may receive a request or notice seeking assistance, for example where the individual is their organisation's law enforcement officer, it is the corporate entity not the individual who is being asked to assist. The individual can and should discuss the request or notice with their employer.*[479]

12.27. Submitters were also concerned that s 317ZF(3)(a)[480] did not permit SMEs to make disclosures to technical consultants about requests for technical assistance. In a written response to me following the hearing, the Department of Home Affairs advised that DCPs may be able to rely in this exception to the disclosure offence provided the external technical advice is required to comply with the request or notice to determine whether it complies with the protection in s 317ZG(1). This is of particular importance to small or sole trader DCPs which may have little in-house capacity to determine what technological steps are required to comply with such a request or notice. I consider it necessary to make this exception clear.

12.28. **I conclude that the information disclosure provisions should be amended so as to permit DCPs to obtain not merely legal advice but also technical advice in relation to requests or potential request of TARs and issue or potential issue of TANs and TCNs.**

Power to conduct joint investigations

12.29. Here I note the supplementary submission of the Law Enforcement Conduct Commission (LECC), noting there are multiple formal avenues for the LECC Inspector and the NSW Ombudsman to share information relevant to each other for the

---

[479] Hamish Hansford Home Affairs, Public Hearing, Canberra, 21 February 2020, p 191.

[480] *A person covered by paragraph (1)(b) may disclosure technical assistance notice information technical capability notice information or technical assistance request information:*

(a) *In connection with the administration or execution of this Part …*

purpose of their oversight functions.[481] The LECC supplementary submission noted that a similar provision could be considered within s 317ZRB of the *Telecommunications Act 1997* (Cth). While not specifically mentioning joint investigations, the existing legislation clearly contemplates overlapping roles between these agencies, which amendments to TOLA could enhance and clarify. So **I conclude that the capacity of the Commonwealth Ombudsman to undertake a joint investigation with State Ombudsman or Independent Commission Against Corruption oversight bodies such as Inspectors-General should be made explicit within s 317ZRB of the Telecommunications Act**.

Enhancing audit powers and capacities

12.30. **I conclude that agencies should be required to keep records of the number of requests they make of carriers or carriage service providers under s 313 of the Telecommunications Act and to report on those matters annually to the IPC.** While s 313 has existed for many years and was not directly impacted by TOLA, the keeping and reporting of this information will allow for monitoring and assessment as to the relationship between the powers enacted or amended by TOLA and the continuing power under s 313 of the Telecommunications Act. Over time, it will also permit the identification of trends, including as to whether – and if so, how – the availability of various TOLA powers impacts on the frequency of agencies' s 313 requests.

Definitions of 'serious Australian offence' and 'serious foreign offence'

12.31. The industry assistance powers in Part 15 of the Telecommunications Act, which Schedule 1 of TOLA introduced, can be exercised in relation to a 'serious Australian offence' (or a 'serious foreign offence'). Each of those terms is defined in s 317B of the Telecommunications Act as an offence punishable by a maximum term of imprisonment of 3 years or more or for life.

12.32. A number of stakeholders made submissions that the 'serious offence' threshold that the Telecommunications Act establishes – 3 years' imprisonment – is too low. These stakeholders represented a range of different interests and included the

[481] Law Enforcement Conduct Commission, Submission No 23 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 24 September 2019, 1, citing s 19A of the *Telecommunications (Interception and Access) (New South Wales) Act 1987* (NSW) and s 92A of the *Telecommunications (Interception and Access) Act 1979* (Cth).

combined industry group,[482] Atlassian,[483] the Australian Human Rights Commission,[484] Internet Australia,[485] BSA The Software Alliance[486] and the Law Council of Australia.[487]

12.33. Many of those stakeholders made the point that the 3-year imprisonment threshold captures a range of offences of much less severity than the offences to which agencies referred in making the case for the legislation (including, for instance, terrorism and predatory offences against children).

12.34. The Department of Home Affairs submitted as follows:

> *This offence threshold sufficiently limits the availability of industry assistance powers to the investigation and prosecution of serious crimes such as terrorism, child sex offences and other severe offences such as using a carriage service to menace, harass or cause offence*.[488]

12.35. While the Department of Home Affairs' submission is correct insofar as the threshold permits the exercise of the powers in respect of offences of that nature, I am not persuaded that the offence threshold 'sufficiently limits the availability of industry assistance powers to the investigation and prosecution of' those offences.

---

[482] Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, the Communications Alliance, Digital Industry Group Inc and Information Technology Professional Association, Submission No 15 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 September 2016, , 6 and 8.

[483] Atlassian, Submission No 17 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 18 September 2019, 4.

[484] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, [104]–[105].

[485] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, section 2.1.

[486] BHA The Software Alliance, Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (resubmitted for the purposes of this review), 9.

[487] Law Council of Australia, Submission No 45 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 6 November 2019, [20]–[22].

[488] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 20

Rather, the 3-year threshold captures a range of other, less serious offences. It is noteworthy that, apart from the offence of using a carriage service to menace, harass or cause offence,[489] each of the offences to which the Department of Home Affairs' submission refers carries a maximum term of imprisonment much greater than 3 years.

12.36. Overwhelmingly, stakeholders who made submissions on this point submitted that the definition of 'serious Australian offence' in s 317B of the Telecommunications Act should be amended so that it aligns with the definition of that term in s 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act).[490] Some submissions referred to the threshold for 'serious offence' under the TIA Act being an offence punishable by 7 years' imprisonment or for life.

12.37. While 7 years' imprisonment is a reference point for the definition of 'serious offence' in s 5B of the TIA Act, it is not as simple as that. The definition of 'serious offence' in s 5D of the TIA Act is extensive. It includes offences carrying a term of 7 years' imprisonment that involve conduct of a serious nature – for example, 'serious personal injury', 'serious arson', or 'serious fraud'. It also includes other offences which are brought within its scope because they are offences of particular nature (for example, murder, child sexual offences) without reference to maximum terms of imprisonment they carry.

12.38. The Department of Home Affairs submitted that it would not be appropriate to raise the threshold for the definition of 'serious Australian offence'. In respect of the threshold for 'serious offence' under s 5D of the TIA Act, it commented that:

> *These thresholds have been determined by Parliament to be sufficient to actually authorise intrusion on privacy and the collection of personal data – something which Schedule 1 does not do. Raising the offence threshold for using Schedule 1 powers would prevent its use in parallel with these other investigative tools and frustrate the legislation's policy intention.*[491]

12.39. In essence, the department's submission is that the higher threshold is only necessary where a power 'actually authorise(s) intrusion on privacy and the collection of personal data' and that industry assistance notices do not do so. This reflects the position more broadly adopted in the department's submission; namely, that it is not the industry assistance notice but, rather, a warrant which in fact

[489] Criminal Code (Cth), s 474.17.

[490] Some, but not all, made the same submission in respect of the definition of 'serious foreign offence'.

[491] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, [125].

authorises an intrusion on privacy. On that view, all an industry assistance notice does is to render that content comprehensible.

12.40. I am not persuaded that industry assistance notices do not authorise intrusion of privacy and the collection of personal data or that they will always be accompanied by a warrant. Without descending into detail, I have reviewed a selection of agencies' documentation as to how industry assistance powers have been deployed since TOLA commenced. I am not satisfied that the investigative steps they make possible can be characterised as less intrusive than telephone interception.

12.41. I see significant merit in aligning the definition of 'serious offence' under the Telecommunications Act and the TIA Act. To begin with, both the TIA Act and the Telecommunications Act concern the covert use of coercive powers in the investigation of certain types of offence. Because they have that fact in common, it is sensible that they use the same types of offence as the threshold for the exercise of powers. Further, risks arise from a proliferation of different standards for different powers, without any compelling reason for the distinction. Law enforcement officers are expected to exercise a range of different powers, in different jurisdictions, on application to different issuing authorities, who are tasked to apply different standards depending on the type of power involved. Adding another point of distinction between comparable powers – in terms of thresholds at which they become available for use – is liable to confuse and perhaps contribute to inadvertent excesses of power.

12.42. **I conclude that the definitions in TOLA of 'serious Australian offence' and 'serious foreign offence' should be amended so that they align with the definition in existing s 5D of the TIA Act. The effect of this is that, by and large, it would not be open to an agency to obtain an industry assistance notice in respect of an offence punishable by only 3 years' imprisonment.**[492]

Removal of power to redact the Ombudsman's report

12.43. Section 317ZRB of the Telecommunications Act deals with the Commonwealth Ombudsman's power to inspect records of interception agencies and to make a written report to the Minister for Home Affairs of any such inspection. Sub-section

[492] Aligning the definition of 'serious Australian offence' in the Telecommunications Act with the present definition in the TIA Act would be relatively straightforward. It would require only that Parliament to amend the definition of 'serious Australian offence' in s 317B of the Telecommunications Act to provide that that term has the same meaning as the meaning of 'serious offence' in s 5D of the Telecommunications Act, and to make equivalent amendments in respect of the definition of 'serious foreign offence'.

(6) requires the Minister for Home Affairs to cause a copy of any such report to be tabled in both houses of Parliament within 15 days of receiving the report.

12.44. Section 317ZRB(7) of the Telecommunications Act permits the Minister for Home Affairs to delete, from any copy of the report, 'information that, if made public, could reasonably be expected to (a) prejudice and investigation or prosecution, or (b) comprise any interception agency's operational activities or methodologies'.

12.45. Various stakeholders made submissions requesting that s 317ZRB(7) be repealed. The Commonwealth Ombudsman made the following submission: 'this power is not available to a Minister in any other legislation under which the Ombudsman may issue a report and, in our view, is inconsistent with the Ombudsman's role as an independent and impartial office'.[493]

12.46. The Commonwealth Ombudsman also submitted that the power is not necessary in light of s 317ZRB(4). That sub-section provides that a report 'must not include information which, if made public, could reasonably be expected to (a) prejudice an investigation or prosecution; or (b) compromise any interception agency's operational activities or methodologies'. As the Commonwealth Ombudsman observed, those are the same bases on which the Minister for Home Affairs is empowered to redact information. In other words, if the Commonwealth Ombudsman is properly performing its role, there will be nothing in the report for the Minister for Home Affairs to redact.

12.47. It is conceptually possible the Minister for Home Affairs may be aware – perhaps on the advice of an agency – that information included in the Commonwealth Ombudsman's report might compromise an investigation or prosecution or operational capability, but the Commonwealth Ombudsman is not aware of that risk. As a result, the Commonwealth Ombudsman may include such sensitive information in a report. However, I do not consider that a significant risk in practice. As the Commonwealth Ombudsman submitted:

> *Our Office routinely consults with agencies to identify whether a draft report contains operationally sensitive material that should be removed or amended before it is published. Further, the Office only inspects and reports on records that have ceased or expired so as to avoid any risk to ongoing operations.*[494]

12.48. The Commonwealth Ombudsman requested that s 317ZRB(7) be repealed. The Law Council of Australia expressly endorsed the Commonwealth Ombudsman's

---

[493] See Commonwealth Ombudsman, Submission No 14 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 September 2019, 3–4.
[494] Ibid 3.

submission on that point and made a recommendation to the same effect.[495] I am persuaded that it is not necessary or reasonable and proportionate that the Minister for Home Affairs be empowered to redact information from a report the Commonwealth Ombudsman makes available under s 317ZRB.

12.49. **As to the Ombudsman's powers of reporting, I conclude that s 317ZRB(7) should be repealed so that the Minister cannot remove material from an Ombudsman report under that provision.**

Schedule 2: Computer access warrants

Power to intercept communications for the purpose of a computer access warrant

12.50. As discussed earlier in this report, the reforms effected by Schedule 2 permit ASIO or a law enforcement officer to engage in limited telecommunications interception for the purposes of a computer access warrant, without obtaining a separate telecommunications interception warrant to do so.

12.51. The Department of Home Affairs submitted as follows in relation to that amendment:

> *It is often necessary to undertake limited interception for the purposes of executing a computer access warrant. Schedule 2 amended the law to permit the interception of a communication passing over a telecommunication system, if the interception is for the purposes of doing anything specified in the computer access warrant. In other words, any interception of communications would be incidental to executing a computer access warrant, including the concealment of access, and cannot be used for independent evidence or intelligence collection.*[496]

12.52. I accept the Department of Home Affairs' submission that, as a practical matter, some degree of interception is at times necessary for the purpose of executing a computer access warrant. That interception will be under the authority of a warrant – which, in the case of a law enforcement agency, is independently issued – albeit not a telecommunications interception warrant.

---

[495] Law Council of Australia, Submission No 45 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 6 November 2019, [104]–[108] (and see the Commonwealth Ombudsman's request at 3).

[496] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, [182].

12.53. Further, the power to intercept communications under that warrant is limited to that which is necessary for the purposes of the computer access warrant. The Department of Home Affairs submission acknowledges that 'officers will require an interception warrant to deal with intercepted communications beyond what is required to give effect to a computer access warrant'.[497]

12.54. As a result, I do not accept there is any real prospect of agencies using this power to circumvent the need to obtain a telecommunications interception warrant under the TIA Act. I consider the amendment is a proportionate response to the inefficient situation that previously prevailed, which required 2 separate warrants to lawfully access a computer.

12.55. **I conclude that agencies should retain the power to engage in limited telecommunications interception, for the purposes of a computer access warrant, without the need to obtain a separate warrant under the TIA Act authorising that interception.**

Steps to conceal something done under authority of a computer access warrant

12.56. The reforms effected by Schedule 2 granted to ASIO and to law enforcement the power to do anything reasonably necessary to conceal anything that has been done to a computer pursuant to a computer access warrant or a related authorisation.[498] This includes such things as entering premises where the computer is reasonably expected to be, entering any other premises for the purposes of accessing the first premises, and removing the computer from the place where it is situated.

12.57. The Department of Home Affairs submitted that '[c]oncealment of access is essential for preserving the covert nature of computer access warrants, and to protect law enforcement and intelligence technologies and methodologies'.[499]

12.58. The power to do those things is ordinarily limited to the duration of the warrant or authorisation and the 28 days that follow. However, where it is not practicable to do any of those things within that period, the legislation automatically extends that time period to the earliest time after that 28-day period at which it is reasonably practicable to take the steps. The power is not otherwise limited in time, so it might conceivably be executed some months or years later.

---

[497] Ibid [184].

[498] ASIO Act, ss 25A(8), 27A(3C), 27E(6); SD Act, s 27E(7).

[499] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, [186].

12.59. The Australian Human Rights Commission took issue with the extent of that power.[500] In broad terms, it submitted that accessing a computer or other device to take steps that conceal steps taken under the warrant or authorisation – at some indeterminate point, beyond a 28-day period after the warrant is in force – is a distinct intrusion on privacy from that which the warrant itself authorises, and one which ought to be separately authorised.

12.60. The Law Council of Australia also expressed concerns with the absence of a time limit on taking concealment actions.[501] While it welcomed the requirement to notify the Ombudsman of late steps to conceal a warrant, it submitted that, in its view, '[a] requirement to notify the Ombudsman is not a sufficient safeguard to ensure that a chief officer of a law enforcement agency cannot exercise powers that may authorise privacy-intrusive activities in the absence of the reasonable grounds threshold which underpins the initial warrant'.

12.61. It is significant that a computer access warrant authorises the taking of steps to conceal anything done under a warrant as a matter of course, without the need for separate application or authorisation. It is also significant to me that these steps are to be taken covertly, to conceal the fact something was done under the authority of a warrant. Further, those steps may lawfully be taken on premises other than – and which might have no connection with – the premises on which the computer or device was located at the time the computer access warrant was executed.

12.62. In light of these factors, I am persuaded that an agency should be required to seek external authorisation to exercise a concealment of access power, where that is to occur at any point beyond 28 days after the expiry of the warrant or authorisation. I consider it is important that an external decision-maker be given the opportunity at that point to consider the proposed step to conceal access, the likely privacy implications at the time and in the place where it is proposed to occur, and whether it is appropriate in light of the period of time that has passed and any developments in the investigation since that point.

12.63. **I conclude that an agency should be required to seek external authorisation to exercise a concealment of access power if it proposes to take that step more than 28 days after the warrant has expired.**

---

[500] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, [124]–[134].

[501] Law Council of Australia, Submission No 45 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 6 November 2019, [123]–[127].

Return of computers removed from warrant premises to those premises as soon as reasonably practicable

12.64. The reforms effected by Schedule 2 provide that, where a computer or other thing is removed from warrant premises in accordance with a computer access warrant (or authorisation), the computer or thing must ordinarily be returned 'within a reasonable period'.[502]

12.65. The Law Council of Australia submitted that the legislation should be amended to impose on agencies a fixed time limit for the return of a computer moved from warrant premises, on the basis that 'a reasonable time' is too imprecise.[503]

12.66. While I do not consider it is appropriate to impose a fixed time limit on the return of an item, I accept the Law Council's submission that a 'reasonable time' is not sufficiently precise. I consider it would be more appropriate for the legislation to require the return of an item 'as soon as is reasonably practicable'. Indeed the 'reasonably practicable' threshold is already used in the context of computer access warrants – for example, to identify the time at which an agency must take concealment of access steps in respect of a computer access warrant outside of the 28-day period following the warrant (the subject of the immediately preceding recommendation)[504] and the time at which ASIO is to retrieve a surveillance devices from warrant premises.[505]

12.67. This proposed amendment acknowledges that a fixed time limit is not necessarily appropriate – and may well be arbitrary – given what is a 'reasonable' time to retain an item may vary from case to case. Imposing a time limit by which an item must be returned might also have the inadvertent consequence of impliedly permitting the retention of an item until that time.

12.68. It is also important to take into account practicalities, as the agency may have a limited window in time during which it can safely return an item without undermining the covert nature of the warrant, and it should not be pressed to do so where it is not practicable. An obligation to return an item 'as soon as reasonably practicable' allows those factors to be taken into account.

---

[502] ASIO Act, s 25A(4A); 27E(3A); see also SD Act, s 27E(2A). Where the computer access warrant has been obtained by ASIO, this is subject to a situation in which the return of the item would be prejudicial to security, in which case it is permissible to retain the item until that is no longer the case.

[503] Law Council of Australia, Submission No 45 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 6 November 2019, [117]–[122].

[504] ASIO Act, ss 25A(8)(k), 27A(3C)(k); SD Act, s 27E(7)(k).

[505] ASIO Act, ss 26B(5)(m), 27A(3A)(m).

12.69. For these reasons, **I conclude that the legislation should be amended to require that a computer or thing which is removed from warrant premises during the execution of a computer access warrant (or related authorisation) be returned to warrant premises if returning the computer or thing is no longer prejudicial to security[506] or, otherwise, as soon as is it reasonably practicable to do so**.

Schedules 3 and 4: Assistance orders

12.70. Schedules 3 and 4 largely amend the scope of the AFP's and ABF's respective powers[507] to request the issue of an assistance order. I summarise those amendments earlier in this report. Because TOLA did not introduce but, rather, merely expanded these agencies' existing powers to seek an assistance order,[508] I do not here consider whether these powers should exist; I have the much narrower task of reviewing the amendments that TOLA made.

12.71. For clarity, I use the term 'assistance order' here (as I do elsewhere in this report) to refer to orders made under s 3LA of the Crimes Act, s 201A of the *Customs Act 1901* (Cth), s 34AAA of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), or 64A of the *Surveillance Devices Act 2004* (Cth) (SD Act). However, my comments in this section are limited to the AFP's and ABF's powers, as I address ASIO's power separately in connection with Schedule 5 and I have no observations to make that are specific to the SD Act power.

12.72. Assistance orders are distinct from – and ought not be confused with – industry assistance orders under Part 15 of the Telecommunications Act, as amended by Schedule 1 of TOLA. Though there are many distinctions between assistance orders and industry assistance orders, chief among them is the fact that assistance orders issue in respect of an individual or natural person, not a DCP. Further, an individual who does not comply with an assistance order is liable to be criminally convicted and may be imprisoned.

12.73. Schedules 3 and 4 of TOLA did not introduce assistance orders. However, in my view, it is within the scope of this review to consider steps that could be taken to ensure the powers are exercised in a reasonable and proportionate matter. I consider the adoption of the following recommendations would better ensure that assistance

[506] In the case of a computer access warrant issued at the request of ASIO; there is presently no exception to this effect in respect of warrants issued to law enforcement officers under the SD Act.

[507] In respect of the AFP, under Crimes Act, s 3LA, and in respect of the ABF, under Customs Act, s 201A.

[508] For the time being, I hold aside orders under s 34AAA of the ASIO Act, which were introduced by Schedule 5 of TOLA, and which merit separate consideration.

orders the AFP and ABF seek and obtain are exercised in a reasonable and proportionate manner.

No need to change the way in which these orders are issued

12.74. The AFP's and ABF's powers in respect of an assistance order are limited in the first instance to a power to apply to a magistrate for the issue of the order. In addition, the new assistance orders under s 64 of the SD Act[509] in connection with a computer access warrant, or a related authorisation or order, are issued by an eligible judge or AAT member. An application must demonstrate reasonable grounds for suspecting that evidential material is contained on, or accessible from, the device and that the person in respect of whom it will be executed has relevant knowledge about the device. As a result, these powers have at all times been subject to approval external to the agency and in that respect are in a different category from the industry assistance powers that Schedule 1 of TOLA introduced.

12.75. In addition, there is some practical benefit in retaining magistrates as the persons empowered to issue orders of this nature. The submissions I have received from the agencies have made clear that these orders are ordinarily obtained at the same time as approaching a magistrate for the exercise of other coercive powers.

12.76. For instance, in the case of the AFP, a s 3LA warrant– which can only be executed in connection with a Crimes Act s 3E search warrant – is ordinarily sought from a magistrate at the same time as the s 3E search warrant in connection with which it is proposed to be executed. Similarly, an assistance order in connection with a computer access warrant is issued by 'an eligible judge or AAT member',[510] which is the same authority for the issue of the computer access warrant itself.

12.77. This is not only more efficient than requiring that an assistance order be obtained from a different person or body than the warrant to which it is connected but it also ensures the decision on whether or not to issue the order is made by a person who has the benefit of the detailed information provided in support of the warrant application.

12.78. On that basis, I do not consider it either necessary or practical for there to be any amendment to the way in which assistance orders are approved.

---

[509] As introduced by Schedule 2 to TOLA.

[510] SD Act, s 64.

Requirement for agencies to keep records of how many assistance orders they execute each year

12.79. At present, the applicable legislation does not require the AFP or the ABF to keep any records of how many assistance orders they seek, obtain or execute. In response to my request for information on the number of these orders[511] that the AFP executed during the relevant period,[512] the AFP indicated that it does not keep records of how many s 3LA assistance orders it obtains and serves. By contrast, the ABF does keep records of its use of assistance orders. In his response to a notice I issued seeking information on that agency's use of its assistance order power under s 201A of the Customs Act, the Commissioner of the ABF indicated that the ABF obtained 16 assistance orders and executed 8 of those orders during the period for which I sought information.[513]

12.80. I consider there are significant benefits in requiring that a record be kept of the number of assistance orders that are executed and therefore **I conclude that relevant agencies should keep a record of the number of assistance orders that are executed and provide them annually to the IPC**. Agencies indicate that assistance orders are frequently deployed to compel a person to provide access to the person's electronic devices. The Commissioner of the ABF stated, in response to my request for information on the topic, that the devices in respect of which that agency more commonly seeks assistance orders tend to be mobile phones, laptops and tablets and that the information or assistance the orders typically require include 'numerical passcodes, a gesture swipe or a text password' to enable access to the device.

12.81. A consistent theme throughout my review is the volume of revelatory information about a person that can be contained in a single device – in particular, a person's mobile phone, laptop and tablet. Providing access to such a device under compulsion is, in effect, providing investigators with access to all of the data that device contains, at least for the purpose of identifying what evidential material it contains.

12.82. While there might be legitimate operational reasons for requiring that a person provide that assistance in a given case, it is appropriate that there be a record kept as to the total number of such requests that are made – and perhaps the crime type under investigation in connection with each order – and that those records be made

[511] Made under s 24 of the INSLM Act.

[512] Being December 2018 (when TOLA came into force) and 10 February 2020 (the date I issued my notice).

[513] Being December 2018 (when TOLA came into force) and 10 February 2020 (the date I issued my notice).

public on an annual basis. This will permit the broader public to know how broadly these powers are being deployed and to note any trends that develop over time. This accountability will better ensure that the power is being deployed reasonably and proportionately.

12.83. It is not necessary to require that there be records kept of how many assistance orders are sought and obtained; only those that are executed. This is because assistance orders are apparently sought and obtained for a wide range of people who the investigating agency expects it might encounter at warrant premises, or who might be able to provide assistance, but in respect of whom the orders are never executed. This may be because, for instance, orders are obtained in respect of a number of people who might be able to provide the information in question but where only one person need ultimately provide that information. Likewise, there is no need to execute an order in respect of a person who voluntarily provides the information or assistance that the assistance order seeks (for instance, who provides the password to access a phone voluntarily, when requested to do so, so that there is no need to execute an assistance order seeking that information).

12.84. The coercive force of an assistance order does not come to bear until the point at which it is executed, as this is the point at which a person in respect of whom the order is executed is exposed to criminal sanction, including a term of imprisonment, for failing to provide the information or assistance it seeks. On that basis, **I conclude that there is no need to keep any record of or to report on the number of assistance orders that an agency obtains but which are not ultimately executed**.

12.85. Further, requiring that the AFP and ABF to report on the execution of their respective assistance orders will be consistent with s 94(2BC) of the ASIO Act. That provision mandates that the Director-General of Security's annual report include information as to the total number of orders made under s 34AAA(2) – the equivalent power to the AFP's and ABF's assistance order powers – during the reporting period.

Penalty for failure to comply with an assistance order should be monitored to identify trends

12.86. One of the more significant reforms to assistance orders effected by Schedules 3 and 4 was in relation to penalties. In particular, the legislation as amended now

contains both a general offence and an aggravated offence,[514] and an increased penalty now applies to the offence of failing to comply with an assistance order.[515]

12.87. During this review I issued notices[516] on those agencies that have the power to issue an assistance notice, together with the Commonwealth Director of Public Prosecutions (CDPP) (the Commonwealth agency responsible for prosecuting these offences[517]). I requested information on the number of criminal prosecutions, and ultimately convictions, for these offences and the sentences imposed in respect of those convictions; and also to seek agencies' views as to what effect (if any) the increase in the penalty for failing to comply with an assistance order has had on those metrics.

12.88. The information I received was inconclusive. The absolute number of prosecutions and convictions for breach of these offences is low. For instance, the CDPP response notes 63 charges in respect of the AFP's assistance order provision in the 17-year pre-TOLA period, 37 of which were discontinued, and ultimately 23 convictions. The CDPP reports that 9 of those convicted were sentenced to imprisonment, 4 were sentenced to a recognisance release order, 9 were given a fine and 1 was a juvenile.

12.89. During that same 17-year pre-TOLA period, in respect of the ABF's assistance order provision, the CDPP report notes there were 8 charges for failure to comply with an ABF assistance order, 6 of which were discontinued, 2 of which proceeded to conviction, and both of which resulted in a fine.

12.90. By way of comparison, at the date it responded to the notice I had issued, the CDPP had not recorded any charges for breach of any of the assistance order provisions in the period since TOLA commenced (and, it follows, no convictions or sentences were imposed). The CDPP commented that:

---

[514] Where the offence to which the relevant warrant relates comprises 'a serious offence or serious terrorism offence' in the case of the AFP's power (Crimes Act, s 3LA(6)(e)), or 'a serious offence' in the case of the ABF's power (Customs Act, s 201A(4)(e)).

[515] To 5 years' imprisonment or 300 penalty units or both for the general offences under the Crimes Act and the Customs Act, and to 10 years or 600 penalty units or both in the case of the aggravated offences under the Crimes Act and the Customs Act (Crimes Act, s 3LA(5) and (6); Customs Act, s 201A(3) and (4)).

[516] INSLM Act, s 24.

[517] State and Territory agencies may well prosecute these offences too, although no data was available to me during my review as to any prosecutions, convictions or sentences arising from any such prosecutions. Given that assistance orders are available in respect of Commonwealth warrants and in the course of Commonwealth investigations, I do not consider there is a significant possibility that a State or Territory agency has prosecuted any significant number of these offences.

> *the investigative process (including the arrest and charging of an accused) and referral of a brief to the CDPP can take some time and can be longer in more complex matters. Given the short post-TOLA period, it is difficult to discern any observable change in the statistics comparatively to the pre-TOLA period.*

12.91. As a result, it is not possible for me to discern any trend in charges laid, prosecutions, convictions or sentences at this point in time. The CDPP observed that:

> *in accordance with established sentencing principles, a sentencing court must have regard to the maximum penalty for an offence when determining an appropriate sentence. As a result of the increase to the maximum penalties enacted by TOLA, one would expect the sentences imposed for this type of offending to also increase in future. Increased penalties should act as an increased deterrent to would be offenders.*

12.92. While I accept the correctness of the CDPP's observation, in light of its significant prosecutorial experience, it is simply not possible at this point in time to determine whether that expectation is borne out in practice.

12.93. As a result, I cannot reach any conclusion on the necessity and proportionality of the increase in criminal penalties for failure to comply with an assistance order or of the introduction of aggravated offences.

12.94. The AFP submission provided 2 case studies of situations in which a person served with a s 3LA order provided the information it sought, apparently after being advised of 'the new penalties' that apply to those orders.[518] However, it is not possible to determine from those case studies whether either person would have complied with the person's respective s 3LA order had the penalty remained as it was prior to the reforms effected by TOLA.

12.95. **I conclude that agencies and external stakeholders should continue to monitor the prosecutions and convictions (to the extent that information is made publicly available) so as to permit any trends to be discerned as more time passes.** If my recommendation that the INSLM Act be amended to include TOLA in the list of own motion statutes, my successors can keep this matter in view.

Power to impose a monetary penalty in the alternative to a penalty of imprisonment

12.96. A further reform TOLA effected to these powers is to introduce a monetary penalty as an alternative to a penalty of imprisonment and therefore **I conclude that a**

[518] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, [67].

monetary penalty should be retained as an alternative to a penalty of imprisonment for failing to comply with an industry assistance order. I consider this facilitates the necessary and proportionate exercise of the power, as it gives the sentencing judge a range of sentences to impose on conviction and therefore a greater capacity to impose a reasonable and proportionate sentence in the circumstances of the case.

An assistance order does not authorise detention of a person

12.97. **I conclude that both s 3LA of the Crimes Act and s 201A of the Customs Act should be amended to state, for the avoidance of doubt, that neither authorises the detention of a person to whom the order applies where the agency in question does not otherwise have any lawful basis to detain the person.**

I set out my rationale for this recommendation when addressing the reforms effected by Schedule 5 of TOLA and, in particular, the introduction of s 34AAA of the ASIO Act.

Schedule 5: New ASIO powers

Conduct that results in serious personal injury to any person

12.98. Section 21A of the ASIO Act relevantly provides:

> ***21A Voluntary assistance provided to the Organisation***
>
> *Assistance provided in accordance with a request by the Director-General*
>
> *(1) If:*
>
> *(a) the Director-General requests a person or body to engage in conduct; and*
>
> *(b) the Director-General is satisfied, on reasonable grounds, that the conduct is likely to assist the Organisation in the performance of its functions; and*
>
> *(c) the person engages in the conduct in accordance with the request; and*
>
> *(d) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and*
>
> *(e) the conduct does not result in significant loss of, or serious damage to, property;*
>
> *the person or body is not subject to any civil liability for, or in relation to, the conduct …*
>
> ***Unsolicited disclosure of information etc.***
>
> *(5) If:*

(a) a person or body engages in conduct that consists of, or is connected with:

(i) giving information to the Organisation; or

(ii) giving or producing a document to the Organisation; or

(iii) making one or more copies of a document and giving those copies to the Organisation; and

(b) the person reasonably believes that the conduct is likely to assist the Organisation in the performance of its functions; and

(c) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and

(d) the conduct does not result in significant loss of, or serious damage to, property; and

(e) subsection (1) does not apply to the conduct;

the person or body is not subject to any civil liability for, or in relation to, the conduct.

Copies of, or extracts from, documents

(6) The Organisation may make and retain copies of, or take and retain extracts from, a document given or produced to the Organisation:

(a) in accordance with a request under paragraph (1)(a); or

(b) under paragraph (5)(a).

Subsections (1) and (5) have effect despite other laws

(7) Subsections (1) and (5) have effect despite anything in a law of the Commonwealth, a State or a Territory (whether passed or made before or after the commencement of this section) unless the law expressly provides otherwise.

12.99. Section 21A(1), in particular, is broad in scope. It provides that the Director-General of Security may 'request a person or body to engage in conduct' without any limitation as to the type of conduct – as 'conduct' is not defined – or of the duration of the request.

12.100. By contrast, s 21A(5) is limited to volunteering documents or information which ASIO may copy and retain. The *Acts Interpretation Act 1901* (Cth) gives a wide and technologically neutral meaning of a document, providing in s 2B that:

***document** means any record of information, and includes:*

(a) anything on which there is writing; and

> *(b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and*
>
> *(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; and*
>
> *(d) a map, plan, drawing or photograph.*

12.101. The Department of Home Affairs submitted as follows in relation to s 21A:

> *This power is necessary to indemnify those persons or bodies who provide necessary technical assistance to the Australian Security Intelligence Organisation voluntarily and therefore addresses the need to incentivise knowledgeable persons and bodies to provide this important assistance.*[519]

12.102. However, there is nothing in the terms of s 21A(1) to limit the scope of conduct for the purposes of the provision to 'technical assistance'. ASIO, of course, has recourse to a TAR, which is voluntary, for a DCP, but that does not encompass making a request of an entity that is not a DCP and, in particular, an individual.

12.103. Section 21A confers immunity from civil liability for those who assist ASIO. During my review I received various submissions which emphasised that the corollary of a provision conferring immunity from civil liability on person A is to extinguish person B's right to bring an action against person A to enforce his or her rights. Person B will have no opportunity to be heard on whether his or her rights ought to be extinguished in that way.

12.104. Thus, the fact s 21A is voluntary does not mean it should be unlimited in scope. While I accept that ASIO should be able to obtain the assistance set out in s 21A(5), I do not accept that s 21A(1) is necessary insofar as it encompasses conduct any wider than sub-s (5), not least because 'conduct' is undefined.

12.105. Section 21A(1) is both unnecessary and disproportionate. Given ASIO's other powers to obtain information and assistance, I consider it is only necessary for ASIO to have power under s 21A(1) to request what equally could be volunteered under s 21A(5).

12.106. **I conclude that the power to request conduct in s 21A(1) should be limited in scope to the conduct which can be volunteered under s 21A(5).**

---

[519] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, [214].

Significant loss of, or serious damage to, property

12.107. Next I note limitations in s 21A(1)(e) and s 21A(5)(e) – namely, that the civil immunity does not apply to conduct that results in significant loss of, or serious damage to, property.

12.108. I can see no good policy reason to exclude from the scope of the immunity conduct that causes harm to property while permitting the immunity in respect of conduct that causes harm to a person, however unlikely that may be in practice. Also, I do not consider that sufficient protection is conferred on a person suffering personal injury as a result of conduct pursuant to a s 21A request or voluntary action by the fact that the immunity does not attach to conduct that amounts to an offence.[520] As the Inspector-General of Intelligence and Security (IGIS) submitted, as presently drafted:

> *Conduct constituting the tort of negligence would not be excluded from the immunity, since the civil standard for negligence falls short of criminal thresholds, but can result in loss of life and serious personal injury or harm.*[521]

12.109. It is not appropriate that a third party have no recourse for personal injury suffered simply because the person causing that harm did so at the request of the Director-General of Security or because the conduct would assist ASIO. Also, a person engaging in conduct should not be relieved of the need to consider his or her actions and to take whatever steps might be available to reduce the chance of personal injury to others. In this respect, I do not consider the provision as presently drafted to be proportionate to the national security threats that s 21A is designed to meet.[522]

12.110. On the other hand, I do not consider that the amendment should encompass *any* personal injury. A person who voluntarily engages in conduct, on the strength of an expected immunity, should not lose the benefit of that immunity because of a twisted ankle. It is appropriate that there be some *de minimis* threshold.

12.111. As ASIO submitted, the 'conferral of civil immunity provides individuals or bodies with assurance that they have legal protection for the activities they undertake to

---

[520] ASIO Act, s 21A(1)(d).

[521] Inspector-General of Intelligence and Security, Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 November 2019, 11.

[522] See Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, [78].

assist ASIO'.[523] It is worth noting here that s 21A(1)(e) refers to conduct that 'does not result in' harm, not conduct *likely* to result in harm. Therefore, even where there is no expectation that the conduct in question will cause harm, if it in fact does, then no immunity will be available to the person who engaged in that conduct.

12.112. My chief concern is that a person who suffers injury as a result of conduct that ASIO requests not be deprived of the right to pursue compensation for interference to his or her quality of life or ability to earn a living. Only injury of some significance will sound in compensation in any case. On that basis, I consider it appropriate to limit the exclusion to conduct that causes death or serious personal injury to a person.

12.113. **I conclude that s 21A(1)(e) and s 21A(5)(e) should be amended to confine the scope of that immunity from civil liability by requiring instead that 'the conduct does not result in *death of or serious personal injury to any person or* significant loss of, or serious damage to, property' (emphasis added).**

Removal of Director-General of Security's power to delegate an authorisation to a senior position-holder

12.114. During my review, several stakeholders submitted that the powers that s 21A of the ASIO Act confers on the Director-General represent a significant step. Previously, the power to confer immunity from civil liability on a person assisting ASIO was limited to the Attorney-General.[524] The new s 21A(1) represents a significant step because it now vests that power in the Director-General in respect of a request for voluntary assistance.[525]

12.115. The insertion of s 16A of the ASIO Act takes that another step further by permitting that function to be sub-delegated to a senior position-holder. The term 'senior position-holder' is defined in the ASIO Act to mean an ASIO employee or ASIO affiliate of a certain seniority[526] (in effect, a Senior Executive Service officer in the Australian Public Service).

12.116. ASIO's submission did not address this point.

12.117. **I conclude that s 21A arrangements should be approved by the Director-General of Security or a Deputy Director-General.**

---

[523] Ibid [65].

[524] See Inspector-General of Intelligence and Security, Submission No 37 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 30 October 2019.

[525] Ibid 5.1.1.

[526] ASIO Act, s 4.

Requests for voluntary assistance under s 21A(1)

12.118. The legislation is silent on the interaction between the new powers that Schedule 1 introduced and those that Schedule 5 introduced. More particularly, it is silent on the relationship between ASIO's power to request a person voluntarily engage in conduct for the purposes of s 21A(1) of the ASIO Act and its power to make a technical assistance request under Part 15 of the Telecommunications Act.

12.119. Also, the legislation does not address how a request for voluntary assistance under s 21A of the ASIO Act is to interact with ASIO's existing coercive warrant and detention powers.

12.120. The IGIS submitted that the ASIO Act should be amended to make clear that ASIO's power under s 21A does not extend to requesting assistance that is more properly the subject of a TAR or a warrant. The IGIS submitted as follows (emphasis in original):[527]

> *An express provision would ensure that section 21A requests can* only *be utilised in accordance with the policy intent, and that the intended use of section 21A is clearly communicated to all persons who may exercise powers under the provision, or who are affected by the exercise of those powers.*

12.121. ASIO's submission did not address this point.

12.122. The power to issue a TAR under Part 15 of the Telecommunications Act, as introduced by Schedule 1 of TOLA, includes a number of important safeguards. So do other powers under the ASIO Act. It is necessary to make clear that s 21A does not empower the Director-General to circumvent those protections by making the request under s 21A instead. Further, it is possible to envisage a situation in which a DCP declines to comply with a TAR, and an individual employee of the DCP is then approached with a request for voluntary assistance under s 21A(1). Given that s 21A(1) permits ASIO to confer civil immunity on the person, the DCP would probably have no civil recourse against the employee for taking that action.

12.123. I do not consider it necessary to include an equivalent provision for ASIO's warrants to the effect that a request under s 21A does not include anything for which ASIO would require a warrant. This is because a request for voluntary assistance under s 21A(1) and a coercive warrant are in 2 different categories. There may be situations in which ASIO might prefer to make a request for a person's voluntary assistance under s 21A(1) (which carries with it the benefit of limited immunity) before

---

[527] Inspector-General of Intelligence and Security, Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 November 2019, 10.

proceeding to obtain a coercive warrant if voluntary assistance is not forthcoming. In my view, it is appropriate that ASIO retain the power to do so.

12.124. **I conclude that s 21A(1) of the ASIO Act should be amended to make clear that nothing in s 21A authorises the Director-General to make a request of a person that is properly the subject of a TAR.**

An assistance order under s 34AAA of the ASIO Act does not authorise detention of a person

12.125. These provisions have been analysed earlier. In relation to s 34AAA, the AHRC made the following submission:

> *Section 34AAA(3) contemplates that a person subject to an assistance order can be required to attend a specified place to provide assistance. In such circumstances, the assistance order must specify the period within which the person must provide the assistance, but no maximum period is set. … there is a real question whether a person subject to an assistance order is effectively being detained during the period in which they are required to provide the assistance. While they may not be physically restrained, they are effectively prevented from leaving a specified place prior to the completion of the designated assistance task, under pain of criminal penalties. This might engage the prohibition on arbitrary detention in article 9 of the ICCPR.*[528]

12.126. The AHRC recommended that s 34AAA be amended to include protections akin to those that apply where a person is detained (including, for instance, a specified maximum period of detention, access to a lawyer and a family member, and the opportunity to have the order explained to him or her).[529]

12.127. The IGIS submission also addressed this point.[530] The IGIS submission focused on the fact that, if s 34AAA were to result in a person's detention, this might amount to an arbitrary deprivation of liberty. That submission stated the point as follows:

> *There is a question as to whether a person who is required to attend a place to provide information or assistance to ASIO under a section 34AAA order may be subject to a form of detention; and if so, whether there are adequate safeguards in new section 34AAA. These questions may arise if the person is led to believe that they are not free to leave the place of attendance if they sought to do so.*

---

[528] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, [121]–[122].

[529] Ibid Recommendation H.

[530] Ibid section 5.2.5.

> *For example, due to the physical obstruction of exit points; or an indication to the person that they would, or may, be arrested on suspicion of the offence in new subsection 34AAA(4) if they attempted to leave without attempting to provide the assistance or information.*[531]

12.128. During the public hearings, both the Director-General of Security and the representatives of the AFP were asked whether they considered their respective assistance order powers to amount to a power of detention. While the AHRC made its submission in relation only to the s 34AAA power and not the AFP's power,[532] the question was put to both agencies as the power about which the AHRC made its submission are relevantly in the same terms.[533] The Director-General of Security expressly rejected the proposition that s 34AAA gives rise to a power of detention. In response to a question expressly on that issue, he stated as follows: 'I don't accept that. Home Affairs is the administrating agency for our Act, they don't believe it is, and my advice is the same, we do not agree with that view'.[534]

12.129. The AFP took the question on notice and later responded by way of a detailed supplementary submission in writing. The AFP's response likened its s 3LA power to other powers that compel production or attendance, including production orders, summonses and subpoenas. The response further stated:

> *Section 3LA orders require a specified person to provide assistance. However, unless under arrest, the person is free to leave the company of the police officer executing the section 3LA order. Further, while a section 3LA order may require a person to attend at a particular location to provide assistance, the order does not provide a power for the person to be 'detained' for that purpose. … The AFP considers the use of section 3LA for the purpose of detaining a person would not constitute a proper use of the power.*[535]

---

[531] Ibid section 5.2.5.

[532] By contrast, the IGIS submission noted that the same issue arises in respect of Crimes Act s 3LA orders. However, the IGIS submission noted that 'an important distinction is that those orders are issued by a judicial officer rather than a Minister': IGIS submission, ibid section 5.2.5.

[533] Crimes Act, s 3LA(4); ASIO Act, s 34(3). ABF's assistance order power, under Customs Act, s 201A, does not contain a sub-section equivalent to these.

[534] Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 19.

[535] Australian Federal Police Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 1.

12.130. The AFP response makes the further point that it is lawful for a person to comply with a s 3LA order through his or her legal representative, and that information could be provided by telephone or email. I have not had any case law brought to my attention that suggests the agencies have interpreted this as a law of detention. I am persuaded by the agencies' submissions on these questions. While it is ultimately a court, rather than the agencies, that would finally determine the question, I consider that the agencies' clear position on the matter – which is now a matter of public record – is significant, and I hope it will be incorporated and reflected in their training and governance documents (to the extent that is not already the case).

12.131. For instance, as the IGIS suggests,[536] it may be appropriate for the position to be articulated in the Ministerial Guidelines for ASIO, which are due to be updated.

12.132. I assess that there is no real risk that ASIO's power will be construed or exercised as a power of detention, so I consider there is no need to introduce the safeguards that ordinarily apply to detention to which both the Australian Human Rights Commission and IGIS submissions refer. I note also that the IGIS submission states that 'IGIS will pay close attention to the proposed terms of an order sought by ASIO, in assessing whether the information and assistance sought is "reasonable and necessary" as required by new subsection 34AAA(1)'.[537] I presume this is a reference to the IGIS' review of the notices after they have issued. While this review would necessarily operate after the fact, it suggests that any trend toward the use of the power as a power of detention will be readily discerned.

12.133. On this basis, I do not recommend any amendment to the ASIO Act or the Crimes Act to introduce the protections for a person under detention.

12.134. However, **I conclude that the ASIO Act should be amended to expressly state, for the avoidance of doubt, that the power does not authorise the detention of a person to whom the order applies where ASIO does not otherwise have any lawful basis on which to do this**.[538]

---

[536] Inspector-General of Intelligence and Security, Submission No 37 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 30 October 2019, section 5.2.5.

[537] Ibid 65.

[538] I make the same recommendation in respect of the equivalent assistance order powers under the Crimes Act and the Customs Act above.

13. APPENDICES

Appendix A: Referral letters

PARLIAMENT OF AUSTRALIA
HOUSE OF REPRESENTATIVES

Dr James Renwick SC
Independent National Security Legislation Monitor
1 National Circuit
Barton ACT 2600

Dear Dr Renwick SC,

REVIEW AND REPORT OF THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018

Under section 7A of the *Independent National Security Legislation Monitor Act 2010* (INSLM Act) and paragraph 29(1)(b)(ii) of the *Intelligence Services Act 2001*, on behalf of the Parliamentary Joint Committee on Intelligence and Security, I refer the following matter to you for review and report by 1 March 2020:

> *A review of the operation, effectiveness and implications of amendments made by the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.

The enclosed reference sets out the precise terms of the referral.

To the extent possible, the Committee requests that a review is conducted in public and an unclassified report is produced to assist the Committee with its own review of the same Act due in April 2020.

The Committee is of the view that this referral will satisfy the current obligation under subsection 6(1D) of the *Independent National Security Legislation Monitor Act 2010*.

I note that the INSLM Act is silent on a reporting process for a review conducted on a matter referred by the Committee under section 7A of the INSLM Act, as opposed to a matter referred by the Prime Minister or the Attorney-General under section 7 of the INSLM Act. In the absence to requirements to the contrary, it is the expectation of the Committee that a report will be provided in the first instance to the Committee, as the referring authority.

Recognising that this will be a matter for the Committee formed in the 46th Parliament, it is the expectation of the current members that, as a matter of courtesy, the Committee would provide a copy of the embargoed report to the Prime Minister prior to its public release.

I have also written to the Prime Minister and the Attorney-General to notify them of the Committee's referral.

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY
PO Box 6021, Parliament House, Canberra ACT 2600 | Phone: (02) 6277 2360 | Fax: (02) 6277 2067
Email: pjcis@aph.gov.au | www.aph.gov.au/pjcis

PARLIAMENT OF AUSTRALIA
HOUSE OF REPRESENTATIVES

Reference under section 7A of the *Independent National Security Legislation Monitor Act 2010*

To: Dr James Renwick SC, Independent National Security Legislation Monitor

I, Mr Andrew Hastie MP, Chair of the Parliamentary Joint Committee on Intelligence and Security, under section 7A of the *Independent National Security Legislation Monitor Act 2010* and paragraph 29(1)(b)(ii) of the *Intelligence Services Act 2001*, and on behalf of the Committee, refer to you the following matter relating to national security and counter-terrorism:

> *the operation, effectiveness and implementation of amendments made by the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and whether that Act:*
>
> *(i) contains appropriate safeguards for protecting the rights of individuals; and*
> *(ii) remains proportionate to any threat of terrorism or threat to national security, or both; and*
> *(iii) remains necessary.*

I request that you provide your report on this matter to the Parliamentary Joint Committee on Intelligence and Security by 1 March 2020.

Dated: 26 March 2019

[redacted]

Mr Andrew Hastie MP

Chair, Parliamentary Joint Committee on Intelligence and Security

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY
PO Box 6021, Parliament House, Canberra ACT 2600 | Phone: (02) 6277 2360 | Fax: (02) 6277 2067
Email: pjcis@aph.gov.au | www.aph.gov.au/pjcis

PARLIAMENT OF AUSTRALIA

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY
Parliament House, Canberra ACT 2600 | Phone: (02) 6277 2360 | Fax: (02) 6277 8594 |
Email: pjcis@aph.gov.au

Dr James Renwick SC
Independent National Security Monitor
By email: [redacted]

Dear Dr Renwick

Extension of reporting deadline for Review of the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018

In August we corresponded regarding the possibility of extending the reporting date for your review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) until 30 June 2020. I notified you that the Committee was mindful to grant the extension, contingent on legislation passing Parliament which extended the deadline for the Committee's own review of the amendments made by the TOLA Act until 30 September 2020.

I am pleased to advise you that legislation extending the reporting deadline for the Committee's review passed the Parliament on 5 December 2019. As such, the Committee has resolved that your reporting deadline be extended until 30 June 2020.

Thank you for assisting the Committee with its review.

Please contact the Committee Secretariat [redacted] should you require further information about this matter.

Yours sincerely

[redacted]

Mr Andrew Hastie MP
Committee Chair

5 December 2019

Appendix B: List of submissions

Submission number	*Organisation or Individual*	*Submission date*
01	Independent Commissioner Against Corruption	27 September 2019
02	Australian Signals Directorate	11 September 2019
03	Independent Broad-based Anti-corruption Commission	12 September 2019
04	Riana Pfefferkorn	12 September 2019
05	International Civil Liberties and Technology Coalition	13 September 2019
06	Senetas Corporation Limited	13 September 2019
07	Office of the Victorian Information Commissioner	13 September 2019
08	Confidential Submission – Name withheld	
09	Confidential Submission – Name withheld	
10	Tasmania Police	13 September 2019
11	Digital Rights Watch and the Human Rights Law Centre	11 September 2019
12	The Australian Industry Group	13 September 2019
13	Media Entertainment and Arts Alliance	27 September 2019
14	Commonwealth Ombudsman	16 September 2019
15	Joint Submission (Communications Alliance, Ai Group, AIIA, DIGI, ITPA, AMTA)	16 September 2019
16	Northern Territory Police Force	17 September 2019
17	Atlassian	18 September 2019
18	Dr Isaac Kfir	18 September 2019
19	Google	20 September 2019
20	Office of the Australian Information Commissioner	20 September 2019
21	Australian Security Intelligence Organisation	23 September 2019
22	Department of Communications and the Arts	24 September 2019
23	Law Enforcement Conduct Commission (NSW) and the	24 September 2019

	Independent Commission Against Corruption (NSW) Submission	
24	Queensland Police Service	25 September 2019
25	BSA The Software Alliance	1 October 2019
26	Department of Home Affairs	3 October 2019
27	Australian Federal Police	4 October 2019
28	Dr Chris Culnane and Vanessa Teague	9 October 2019
29	Internet Australia	11 October 2019
30	Australian Human Rights Commission	16 October 2019
31	Simone Denereaz	17 October 2019
32	Access Now	21 October 2019
33	Confidential Submission – Name withheld	
34	Paul Templeton	24 October 2019
35	The Allens Hub for Technology, Law & Innovation	25 October 2019
36	Telstra	29 October 2019
37	Inspector-General of Intelligence and Security	30 October 2019
38	WiseLaw	4 November 2019
39	Confidential Submission – Name withheld	
40	Australian Criminal Intelligence Commission	4 November 2019
41	Amazon Web Services	5 November 2019
42	Cogito Group	5 February 2020
43	Science Party	5 November 2019
44	Confidential Submission – Name withheld	
45	Law Council of Australia	6 November 2019
46	Shogun Cybersecurity	11 November 2019
47	Electronic Frontiers Australia	13 November 2019
48	Confidential Submission – Name withheld	
49	Mozilla	31 December 2019
50	Cybersecurity Coalition	3 January 2020
51	Internet Architecture Board	24 January 2020
52	Fastmail Pty Ltd	31 January 2020
53	Global Network Initiative	1 February 2020

Appendix C: Public hearing program

PROGRAM – INSLM PUBLIC HEARING 20 & 21 FEBRUARY 2020
QT CANBERRA, EUREKA ROOM

THURSDAY 20TH FEBRUARY 2020

	TIME	SESSION
DAY 1	8:45am – 9:15am	**Acknowledgement of Country and Opening Statement – Dr Renwick CSC SC**
1st SESSION	9:15am – 9:50am	**Australian Security Intelligence Organisation (ASIO)** Mr Mike Burgess — Director-General of Security Mr Peter Vickery — Deputy Director-General, Enterprise Service Delivery
	9:50am – 10:30am	**Independent Commission Against Corruption (ICAC NSW)** Ms Bernadette Dubois — Executive Director, Investigation Division **Law Enforcement Conduct Commission (LECC NSW)** Mr Shane Butler — Director, Electronic Collection
	10:30am – 11:00am	Break - Morning Tea (PROVIDED)
2nd SESSION	11:00am – 11:45am	**Human Rights Commission** Mr John Howell — Director, Human Rights and Scrutiny Ms Ella Kucharova — Senior Lawyer
	11:45am – 12:15pm	**Internet Australia** Mr Paul Brooks — Chair, Internet Australia Ms Holly Raiche — Chair, Policy Committee Internet Australia Mr Keith Besgrove — Vice Chair, Internet Australia
	12:15pm – 1:00pm	LUNCH BREAK
3rd SESSION	1:00pm – 1:30pm	**Electronic Frontiers Australia** Mr Angus Murray — Chair, Policy Committee
	1:30pm – 2:00pm	**Atlassian** Mr Patrick Zhang — Head of IP, Policy and Government Affairs Ms Georgie Skipper — Director, Global Policy Mr Julian Lincoln — Partner, Herbert Smith Freehills Ms Anna Jaffe — Senior Associate, Herbert Smith Freehills
	2:00pm – 2:30pm	**Access Now** Ms Lucie Krahulcova — Policy Analyst, Australia and Asia Pacific
	2:30pm – 3:00pm	**Mozilla Corporation** Martin Thomson — Distinguished Engineer
	3:00pm – 3:15pm	Break - Afternoon Tea (PROVIDED)
4th SESSION	3:15pm – 3:45pm	**Communications Alliance, Ai Group, AIIA, AMTA, DIGI & ITPA** Mr Charles Hoang — Digital Capability & Policy Lead, Ai Group Mr John Stanton — CEO, Communications Alliance Ms Christiane Gillespie-Jones — Director Program Management, Communications Alliance Mr Chris Herrmann — President, Information Technology Professionals Association Mr Paul McInerney — Vice President, Information Technology Professionals Association
	3:45pm – 4:15pm	**AustCyber** Ms Michelle Price — Chief Executive Officer
	4:15pm	**Thank you and closing remarks – Dr Renwick CSC SC**

PROGRAM – INSLM PUBLIC HEARING 20 & 21 FEBRUARY 2020
QT CANBERRA, EUREKA ROOM

FRIDAY 21ST FEBRUARY 2020

	TIME	SESSION
DAY 2	**8:45am – 8:50am**	**Acknowledgement of Country and Opening Statement – Dr Renwick CSC SC**
5th SESSION	8:50am – 9:30am	**Law Council of Australia** Ms Pauline Wright — President Ms Olga Ganopolsky — Chair, Privacy Law Committee; Professor Peter Leonard — Member, Media and Communications Committee Dr Natasha Molt — Director of Policy, Policy Division
	9:30am – 10:00am	**The Allens Hub for Technology, Law & Innovation** Genna Churches — UNSW Law
	10:00am – 10:30am	**Independent Commissioner Against Corruption (ICAC SA)** Mr Rod Jensen — Director, Legal Services Mr Andrew Baker — Director, Investigations Mr Andrew Hewlett-Parker — Team Leader, Specialist Services
	10:30am – 10:45am	**Break - Morning Tea** (PROVIDED)
6th SESSION	10:45am – 11:15am	**BSA | The Software Alliance** Mr Jared Ragland — Senior Director, Policy APAC
	11:15am – 11:45am	**Australian Federal Police (AFP)** Mr Karl Kent — Deputy Commissioner, Capability Mr Ian McCartney — Deputy Commissioner, Counter-Terrorism
	11:45am – 12:30pm	**Department of Home Affairs** Hamish Hansford — Acting Deputy Secretary, Policy Rebecca Vonthethoff — Acting Assistant Secretary, National Security Policy
	12:30pm	**Thank you and closing remarks – Dr Renwick CSC SC**

Appendix D: Section 317E listed acts or things

317E Listed acts or things

(1) For the purposes of the application of this Part to a designated communications provider, ***listed act or thing*** means:

(a) removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider; or

(b) providing technical information; or

(c) installing, maintaining, testing or using software or equipment; or

(d) ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format; or

(da) an act or thing done to assist in, or facilitate:

(i) giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(ii) the effective receipt of information in connection with a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(e) facilitating or assisting access to whichever of the following are the subject of eligible activities of the provider:

(i) a facility;

(ii) customer equipment;

(iii) a data processing device;

(iv) a listed carriage service;

(v) a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service;

(vi) an electronic service;

(vii) a service that facilitates, or is ancillary or incidental to, the provision of an electronic service;

(viii) software used, for use, or likely to be used, in connection with a listed carriage service;

(ix) software used, for use, or likely to be used, in connection with an electronic service;

(x) software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network; or

(f) assisting with the testing, modification, development or maintenance of a technology or capability; or

(g) notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation; or

(h) modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider; or

(i) substituting, or facilitating the substitution of, a service provided by the designated communications provider for:

(i) another service provided by the provider; or

(ii) a service provided by another designated communications provider; or

(j) an act or thing done to conceal the fact that any thing has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

(i) enforcing the criminal law, so far as it relates to serious Australian offences; or

(ii) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or

(iii) the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

(2) Paragraph (1)(j) does not apply to:

(a) making a false or misleading statement; or

(b) engaging in dishonest conduct.

Appendix E: Analysis of submissions

13.1. I received more than 50 submissions from government, industry members, industry groups, human rights groups, and civil society ('submitters') during my review.[539] I have also held a number of private meetings, and public and private hearings with various submitters to discuss concerns relating to TOLA.

13.2. This appendix summarises key perspectives of submitters and Government agencies on each of the 5 schedules of TOLA. It summarises the key advice and concerns shared by submitters in relation to the questions of safeguards, necessity and proportionality that I am required to consider. It should be read with the submissions, which are at www.inslm.gov.au. I have considered all of these matters, even if not each is specifically mentioned in the report.

Schedule 1: Industry access framework

13.3. It is not surprising that the majority of submitters focused on the amendments contained in Schedule 1. A significant number of submissions provided by industry, industry groups and civil society expressed serious concerns about the impact of the industry access framework. I note that many submitters outlined concerns about the lack of safeguards limiting the additional powers enabled by Schedule 1 and questioned the *proportionality* of those powers to the current threat landscape. Unsurprisingly, submissions provided by government stakeholders, including law enforcement and intelligence agencies, contended to the contrary.

Does Schedule 1 contain appropriate safeguards for protecting the rights of individuals?

13.4. It is clear that there are 2 distinct and contrasting views on this question. Submissions provided by Government agencies advised that TOLA contains a number of appropriate and effective safeguards.[540] Submissions provided by industry members, industry groups, human rights groups and civil society expressed serious concerns in relation to the sufficiency and effectiveness of those safeguards.[541]

---

[539] All unclassified submissions to this review can be viewed on the INSLM website: <https://www.inslm.gov.au/submissions/tola>.

[540] See the following submissions to the review: ASIO, No 21 ([29]–[39], [49]–[57], [63]–[77]); AFP, No 27 ([7]–[46]); the Department of Home Affairs, No 26 (19–27); ASD, No 2 (p 2).

[541] See the following submissions to the review: AHRC, No 30 (for example, [5], [62], [80]–[84]); Law Council of Australia, No 45 (18–19, 11, 33, 37); BSA The Software Alliance, No 25 (4); Access Now, No 32 (18–20); Internet Australia, No 29 (item 3.4).

13.5. The following sections outline the different perspectives on a range of issues raised in the submissions. These issues are:

1. the 'reasonable, proportionate, practical and technically feasible' requirements
2. the 'systemic weakness' and 'systemic vulnerability' limitation
3. the independent assessment process open to Designated Communications Providers (DCPs) who receive a Technical Capability Notice (TCN)
4. the presence of secrecy provisions
5. the absence or inadequacies of judicial authorisation/review mechanisms
6. the oversight role of the Commonwealth Ombudsman
7. transparency and reporting requirements.

'Reasonable, proportionate, practical and technically feasible'

13.6. The Department of Home Affairs and the Australian Signals Directorate noted that a decision-maker cannot issue a notice unless satisfied that it is reasonable, proportionate, practical and technically feasible in the circumstances.[542] The department advised that the requirement to consider and apply this criterion provides a safeguard for industry members.[543]

13.7. The Department of Home Affairs

> *noted that the TOLA Act contains a list of criteria for decision-makers to apply in determining whether a notice is 'reasonable and proportionate' (section 317RA) and that the decision-maker should apply the department's Administrative Guidance to inform and interpret their application of this criteria.[544] Decision-makers have flexibility to determine the appropriate weight to give to each criteria as neither the TOLA Act nor the Administrative Guidance prescribes the particular weighting that the decision-maker should apply to*

[542] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019; Australian Signals Directorate, Submission No 2 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 September 2019.

[543] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 19–20.

[544] Ibid.

> *each criteria.*[545] *The criteria allow DCPs to present their interests, including commercial interests, for consideration by the decision-maker*.[546]

The reasonableness and proportionality test is balanced by the 'practicability and technical feasibility' criteria. These criteria relate to the 'real world' barriers to executing a notice, including the resources available to the DCP, so that if a notice requires action that is impractical or not technically feasible, it would be found to be impossible to execute and could not be issued.[547]

13.8. However, Internet Australia submitted that the reasonableness and proportionality criteria do not provide an adequate safeguard for industry members as decision-makers and offer 'little comfort to industry that the requirements form any type of safeguard.'[548] That submission stated that decision makers for TOLA powers:

a. will have a vested interest in issuing a notice, and may therefore apply the decision-making criteria subjectively[549]

b. are likely to place different priorities on each of the criteria compared to, say, an independent judicial officer[550]

c. are unlikely to possess the level of technical expertise necessary to accurately determine whether a notice is 'technically feasible.'[551]

'Systemic weakness' and 'systemic vulnerability'

13.9. Key government agencies, including the Department of Home Affairs, said that the privacy and security of individual users is protected by the creation of the 'systemic weakness' and 'systemic limitation' safeguard in sub-ss 317ZG(1) and (5).[552] Thus, a

---

[545] Ibid.

[546] Ibid.

[547] Ibid.

[548] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, [3.4.3].

[549] Ibid [3.4].

[550] Ibid [3.4.3].

[551] Ibid [3.4.3].

[552] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, [32]–[34]; Department of Home Affairs (see, for example, evidence at 189); ASIO (for example, its submission at [31]); Australian Signals Directorate, Submission No 2 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 September 2019, 3.

request or notice cannot be issued if it attempts to implement a systemic weakness into a form of electronic protection or to prevent the patching of an existing systemic vulnerability. This safeguard was added to TOLA to prevent requests from law enforcement and intelligence agencies that could jeopardise the security of technology and information for people who are not the direct targets of a notice.

13.10. The legislation as currently worded has made attempts, at least in the view of the Department of Home Affairs,[553] to implement this concept. Key examples are:

a. the references in s 317ZG(4A) to the prohibiting any act or thing 'that will, or is likely to,' jeopardise the security of any other person's information

b. the definition of 'electronic protection'

c. the definition of 'target technology'.

13.11. In his testimony in the public hearings that I held, Mike Burgess, the Director-General of Security, whilst noting that systemic weakness had different meanings to different people, went on to state:

> *I have no intention of introducing something that breaks the internet, no intention of introducing something that actually means whilst it may give me lawful access to Target A, I've now put every Australian's private communications at risk, because I would not do that.*[554]

13.12. It is true that the inclusion of a limitation was broadly supported by submitters; however, many expressed serious concerns about the definitions of 'systemic weakness' and 'systemic limitation'.[555] Submitters reported that the definitions are

[553] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019.

[554] See the evidence provided on behalf of ASIO by Mike Burgess: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 16.

[555] See the following submissions to the review: AHRC, No 30; International Civil Liberties and Technology Coalition, No 5; Atlassian, No 17; Digital Rights Watch & Human Rights Law Centre, No 11; The Allens Hub, No 35; the Law Council of Australia, No 45; Cogito Group, No 42; Google, No 19; Dr Chris Culnane and Associate Professor Vanessa Teague (University of Melbourne), No 28; Communications Alliance, No 15.

difficult to understand,[556] ambiguous,[557] unclear[558] and too narrow.[559] Senetas and Internet Australia said that the definitions bear no correlation with the common meaning of such terms as used by industry, academics and technology experts.[560]

13.13. Some submitters[561] argued that there was unnecessary duplication in the inclusion of the 2 terms 'systemic vulnerability' and 'systemic weakness' in the legislation. At the public hearing, Internet Australia reiterated industry concerns that:

> *[the legislation] includes technical definitions and terms such as 'systematic weakness' and 'systematic vulnerability' – which actually appear to be the same thing … and the term 'class of technology' which is ambiguous vague and subjective and doesn't actually mean anything to the technical audience.*[562]

13.14. Atlassian agreed, noting that it has 'significant concerns about the operation of the prohibition on systemic weakness and systemic vulnerability and the associated definitions in the [TOLA] Act'.[563]

13.15. The supplementary submission from the Department of Home Affairs addressed this concern regarding possible duplication between systemic 'weakness' and

---

[556] See the following submissions to the review: Internet Australia, No 29; Joint Industry Submission (Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, Digital Industry Group Inc., Information Technology Professionals Association), No 15.

[557] See the following submissions to the review: Internet Australia, No 29 (2); Dr Chris Culnane and Associate Professor Vanessa Teague (University of Melbourne), No 28; AHRC, No 30.

[558] See the following submissions to the review: Digital Rights Watch & Human Rights Law Centre, No 11; The Allens Hub, No 35.

[559] See the following submissions to the review: Joint Industry Submission (Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, Digital Industry Group Inc., Information Technology Professionals Association) No 15; BSA The Software Alliance No 25; Google, No 19 (3); Access Now, No 32 (13).

[560] See the following submissions to the review: Senetas, No 6; Internet Australia, No 29 ([3.3]).

[561] See the evidence provided during the public hearing on behalf of Internet Australia by Mr Brooks: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 55. See also the comment from Professor Leonard, on behalf of the Law Council, that the words were synonymous (ibid 144).

[562] Ibid 56 (Mr Brooks).

[563] Ibid 81 (Ms Skipper).

'vulnerability' directly. The department stated, 'there may be value in retaining both terms' because both terms are commonly used, interchangeably, in general cybersecurity public discourse, so it may be helpful to have that language reflected in the legislation.[564]

13.16. Moving beyond the question of duplication, on a technical level, submitters noted that the current definition states that a systemic weakness or vulnerability must affect a 'whole class of technology' in order to be prohibited.[565] The Australian Human Rights Commission (AHRC) noted that this term is not legislatively defined, and the description provided in the Supplementary Explanatory Memorandum does not clearly articulate how the boundaries of a class may be drawn, including how small or large a class may be.[566]

13.17. The AHRC also submitted that the requirement that a systemic weakness or vulnerability must affect a 'whole class of technology' sets a very high bar.[567]

13.18. The term 'whole' implies that the *entire* category of device or service must be affected before a systemic weakness can be established. For example, there may be circumstances where a measure has detrimental impacts on a *significant* number of users, but not *all* users, and therefore cannot be said to affect a 'whole' class.[568]

13.19. Other submitters noted that this may mean that DCPs could be compelled to introduce weaknesses or vulnerabilities that extend beyond the specifically targeted device to a much larger class – inevitably impacting on the privacy of other users.[569]

13.20. Atlassian submitted that it is unclear, on a practical level, how a systemic vulnerability or systemic weakness could be introduced into a particular application,

---

[564] Department of Home Affairs, Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3.

[565] See the following submissions to the review: Dr Chris Culnane and Associate Professor Vanessa Teague (University of Melbourne), No 28; AHRC, No 30; Internet Australia, No 29 ([3.3]).

[566] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 22.

[567] Ibid.

[568] Ibid.

[569] International Civil Liberties and Technology Coalition, Submission No 5 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 13 September 2019, 1.

targeted at a specific person, that would not 'be likely to' compromise the entire application or class of devices.[570]

13.21. Amazon Web Services similarly pointed out that 'the underlying assumption of the TOLA Act, that a security vulnerability can be created for a targeted technology without creating a systemic weakness or vulnerability, is technically flawed'.[571]

13.22. Cogito Group submitted that the definitions and the description of their effective use appears to be contradictory.[572] It was noted that:

> *given the complexity of the ICT services supply chain, it would be difficult to impose the selective introduction of a weakness into a particular application targeted at a specific person, any introduced weakness could create a weakness across all applications and devices within the class of applications and devices*.[573]

13.23. At the public hearing,[574] Professor Peter Leonard,[575] representing the Law Council, noted:

> *I think systemic is a redundancy which creates uncertainty. The other is class of technology and I'm not sure that even giving examples in the statute will assist to give any real guidance on words 'whole class' of technology. I have practised technology law for 35 years and I have no idea what a 'whole class' of technology is.*[576]

13.24. In its submission the Department of Home Affairs acknowledged that the definitions have been met with concern and noted that alternative definitions have been

---

[570] Atlassian, Submission No 17 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 18 September 2019, 4.

[571] Amazon Web Services, Submission No 41 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5 November 2019, 2.

[572] Cogito Group, Submission No 42 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5 February 2020, 2.

[573] Ibid.

[574] Echoed at the public hearing by the BSA Software Alliance: 'the other issue I wanted to flag with you was the importance of amending the definitions of "systematic weakness and systematic vulnerability" in the Act'.

[575] Principal Data Synergies and Professor of Practice UNSW Business School.

[576] Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 142.

presented for consideration.[577] Notably, an amendment was moved in the Senate, but not passed, in February 2019.

13.25. The department said that issues with the proposed definitions were identified at that time.

13.26. These concerns led the department to conclude that 'potential areas of ambiguity identified with the alternative proposals suggests that these alternatives may not be clearer than the existing construction. It may be that no formulation is possible that satisfies all stakeholders'.[578]

13.27. In its written response[579] to my follow-up questions on the definitions, the Department of Home Affairs noted that the current formulations of the protections against systemic weakness, though contentious, were the result of consultation with multiple stakeholders and the recommendations of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and that alternative approaches, however appealing to particular critics, may be found wanting when exposed to broader consultation.

13.28. In relation to concerns about a DCP being compelled to introduce weaknesses or vulnerabilities that extend beyond a specifically targeted device, in its supplementary submission, the Department of Home Affairs referred to earlier advice that 'the industry assistance framework does not allow agencies to ask providers to create vulnerabilities that affect a "*whole class of technology*"'.[580] There is some circularity to these arguments, and industry is not comforted that these limitations provide adequate protection because they say the definitions[581] are imprecise and not understood.

13.29. At the public hearing, the Department of Home Affairs conceded that the present construction in the legislation is complex. But it urged a cautious approach, noting

---

[577] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 13.

[578] Ibid.

[579] Dated 23 December 2019.

[580] Supplementary submission dated 12 March 2020.

[581] '*Target technology requires clearer guidance as well in terms of how brood the scope of this is. For instance is this an individual instance of say Facebook Messenger on a single device dictated by a Mac address or is it more like a computer definition in the SD Act … Target technology requires consideration*': Angus Murray, Electronic Frontiers: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 71-72.

that 'a more prescriptive or specific model raises significant risks like failing to protect cyber security by not applying equally across technologies and making the industry assistance framework impossible in practice for agencies to use'.[582] Nonetheless, the department went on to indicate that:

> *the Government is open to look at what you find throughout your evidence and consider alternative models put forward by both you and the PJCIS*.[583]

13.30. Before moving on from the issue of systemic vulnerabilities and weaknesses, I note at this point that there have already been attempts to amend this aspect of the legislation. A bill from Senator the Hon Kristina Keneally proposed (amongst other things) repealing the definitions of electronic protection, systemic vulnerability/ weakness, and target technology. It sought to amend s 317ZG, including by prohibiting 'any act or thing that would or may create a material risk that otherwise secure information would or may in the future be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party'. It also proposed 'otherwise secure information' include references to information about any person who is not the subject of an investigation to which the notice relates (or any person who is not communicating directly with that subject).[584]

13.31. Further, a Bill from Senator Jenny McAllister proposed an alternative form of the systemic weakness limitation, including, among other things, removing the concept of electronic protection from the limitation, and prohibiting a notice from requiring actions 'that would render systemic methods of authentication or encryption less effective'. The Senate agreed to that amendment, but the Bill lapsed when the 45th Parliament was prorogued.[585]

Independent assessment

13.32. Government submitters noted that a key safeguard provided by Schedule 1 is the option for DCPs to seek an independent assessment of a TCN. If an assessment is requested by a DCP, the Attorney-General must appoint 2 assessors to review the TCN and prepare a report. One assessor must have technical knowledge and

---

[582] Hamish Hansford Home Affairs: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 189.

[583] Ibid.

[584] Telecommunications Amendment (Repairing Assistance and Access) Bill 2019 (Cth), s 5 (see in particular proposed new sub-ss (4) and (5) of s 317ZG).

[585] Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 (Cth), amendment proposed in Sheet 8642, s 5 (see in particular proposed new sub-s (3) of s 317ZG).

expertise and the other must have previously served as a judge. This combination was designed to provide an objective, technically informed review mechanism.

13.33. A significant number of stakeholders expressed concern that the Attorney-General must only 'have regard' to the report prepared by these assessors when considering whether to proceed and issue the TCN.[586] The Attorney-General is not required to refrain from issuing the TCN if the assessors determine that it should not be given.

13.34. Submissions noted that the assessment could be ignored in practice, as it is not binding on the Attorney-General.[587] The AHRC reported that a 'non-binding form of assessment severely diminishes the integrity of the process and the utility of engaging experts with technical knowledge and a degree of independence to review proposed TCNs'.[588] Similarly, the Communications Alliance advised that 'a mere consideration of the report produced by both assessors is inadequate'.[589]

13.35. Google noted:

> *The standard of review by which the assessors may review a TCN is notably vague. Assessors decide whether a TCN 'should be given', by 'consider[ing]' given enumerated factors and 'consult[ing]' with three parties. However, it is unclear how much deference the assessors should give the original ministerial action or what standard the assessors must reach in order to overturn that action.*[590]

[586] See the following submissions to the review: AHRC, No 30 (69–70); OVIC, No 7 ([3.4.2]); Internet Australia, No 29 ([3.4.2]); Communications Alliance and DIGI, No 15 (13); OAIC, No 20 ([23]); Law Council of Australia, No 45 (22); Google, No 19 (4).

[587] See the following submissions to the review: AHRC No 30 ([69]); OVIC No 7 ([5]); Law Council of Australia, No 45 ([70]–[74]).

[588] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, [70].

[589] Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, Digital Industry Group Inc., Information Technology Professionals Association, Submission No 15 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 September 2019, 6.

[590] Google, Submission No 19 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 20 September 2019, 4.

13.36. Internet Australia also questioned the robustness of this safeguard, given that both assessors are appointed by the Attorney-General rather than an independent authority.[591]

13.37. Further, the AHRC and the Office of the Australian Information Commissioner (OAIC) noted that this safeguard only applies to TCNs and not to other forms of technical assistance, namely TANs. It was contended that TARs and TANs have the same potential to be onerous on the DCPs who receive them and may equally intrude on the rights of third parties.[592]

13.38. At the public hearing, industry representatives expressed concern at the lack of independence in the dispute resolution process. Issues identified included:

a. a lack of technical expertise could lead open up a 'Pandora's box' of unintended harm[593]

b. the ability of agencies to circumvent the consultation period[594]

c. that the finding is not binding on the Attorney-General.[595]

Secrecy provisions

13.39. A number of submissions expressed concern about the secrecy provisions associated with the industry assistance framework.[596] In light of the language used in s 317F(1)–(3), industry members and industry groups are concerned that the secrecy provisions may mean that individual employees could receive a TAN or TCN

[591] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, [3.4.2].

[592] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 70.

[593] Internet Australia: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 55.

[594] Communication Alliance: Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 116.

[595] Hamish Hansford (Department of Home Affairs): Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 201.

[596] See the following submissions to the review: Google, No 19 (5); Law Council of Australia, No 45 (14); Atlassian, No 17 (3).

and be required to disclose information or change systems without informing their employer. Industry noted their understanding that private employees would need to perform their own administration and execution of the notice to preserve the confidentiality required by the secrecy provisions.[597]

13.40. The Law Council also expressed concern that a DCP, or employee of a DCP, could not disclose information about a notice to anybody other than those provided for in TOLA.[598] The list included in TOLA does not include bodies such as the OAIC. It was also noted that, if an employee did disclose information, they would have committed an offence that carries a penalty of 5 years' imprisonment and they would be unable to use a public interest defence.[599]

13.41. On a different point, Cogito Group expressed concern over the potential for Schedule 1 to 'turn our best and most trusted employees into insider threats'.[600] It was contended that TOLA could potentially allow agencies to 'commandeer' staff within their organisation.[601]

13.42. The Department of Home Affairs advised that it is not intended that an individual employee would receive a request or notice and be unable to discuss it with management or lawyers.

13.43. At the public hearing, the Department of Home Affairs stated that:

> *It is not now and it has never been intended that individual employees would be asked or required to provide assistance without informing or consulting their employer. While an individual employee may receive a request or notice seeking assistance, for example where the individual is their organisation's law enforcement liaison officer, it is the corporate entity, not the individual, who is being asked to assist. The individual can and should discuss the request or notice*

---

[597] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, [3.1].

[598] Law Council of Australia, Submission No 45 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 6 November 2019, 14.

[599] Ibid.

[600] Cogito Group, Submission No 42 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5 February 2020, 2.

[601] Ibid.

with their employer, as required, to consider and provide the requested assistance.[602]

13.44. Submitters were also concerned that s 317ZF (3)(a)[603] did not permit SMEs to make disclosures to technical consultants about requests for technical assistance. In a written response to me following the hearing, the Department of Home Affairs advised that DCPs may be able to rely on this exception to the disclosure offence provided the external technical advice is required to comply with the request or notice to determine whether it complies with the protection in s 317ZG(1).

Judicial authorisation and review

13.45. A significant number of submissions expressed concerns about the lack of prior judicial authorisation, or the adequacy of subsequent judicial review, of notices issued under Schedule 1.[604] This issue was often viewed in light of other concerns with TOLA, such as secrecy provisions, the impact on industry and the perceived subjectivity of the decision-making criteria.

13.46. Some submissions stated that the absence of judicial involvement at the authorisation stage leaves providers vulnerable to subjective decision-making and bias from government officials who have a vested interest in issuing notices.[605] Submitters also expressed concern that decision-makers may apply the decision-

---

[602] Hamish Hansford (Department of Home Affairs): Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 191.

[603] *A person covered by paragraph (1)(b) may disclosure technical assistance notice information technical capability notice information or technical assistance request information;*

(b) *In connection with the administration or execution of this Part …*

[604] See the following submissions to the review: AHRC, No 30 (Pt 5.1); OAIC, No 20 ([25], [27]); Law Council of Australia, No 45 ([82]–[84]); Amazon Web Services, No 41 (3); Cogito Group, No 42 (3); Internet Australia, No 29 (16); Google, No 19 (4–5); Access Now, No 32 (6–7); Atlassian, No 17 (3–4); WiseLaw, No 38 ([5]–[10]); Joint Industry Submission (Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, Digital Industry Group Inc., Information Technology Professionals Association), No 15 (5, 7).

[605] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, [3.4.4].

making criteria subjectively and could be informed by evidence that is not available to the relevant DCP.[606]

13.47. As noted previously, submitters noted that the validity of a notice depends on the issuer's interpretation of TOLA, their analysis of the facts and their weighting of the various factors to which the Act requires them to give consideration.[607] Additionally, Amazon Web Services noted that there is no requirement for the assessment – that is, the manner in which the decision was made – to be documented to ensure consistent application of the Act.[608]

13.48. Additionally, Access Now expressed concern that the provisions for delegating authority to issue a notice may result in a considerable number of officials holding the appropriate delegations,[609] which, it said, compounds the potential for Schedule 1 powers to be misused or used in a manner that has unexpected or unintended consequences. It concluded that the delegation provisions give a potentially large number of government officials 'an unchecked level of power to unilaterally approve invasive activities with unpredictable and potentially dangerous outcomes'.[610]

13.49. Many submitters also expressed concern about the lack of options to seek judicial review once a notice has been issued.[611] TOLA does not provide for merits review in the Administrative Appeals Tribunal (AAT) or otherwise of decisions made under Schedule 1, and excludes judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth).[612] This also means that there is no duty to provide a

---

[606] See the following submissions to the review: BSA, No 25 (4); Amazon Web Services, No 41 (3).

[607] BSA, Submission No 25 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 1 October 2019, 19.

[608] Amazon Web Services, Submission No 41 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5 November 2019, 3.

[609] Access Now, Submission No 32 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 21 October 2019, 7.

[610] Ibid 19.

[611] See the following submissions to the review: Amazon Web Services, No 41 (p 3); Google, No 19 (5); BSA, No 25 (4–5); AHRC, No 30 ([64(c)]); International Civil Liberties and Technology Coalition, No 5; Access Now, No 32; WiseLaw, No 38; Joint Industry Submission (Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, Digital Industry Group Inc., Information Technology Professionals Association), No 15.

[612] See the following submissions to the review: OVIC, No 7; Communications Alliance, No 15; Office of the Australian Information Commissioner, No 20.

statement of reasons on request under s 13 of that Act.[613] (Of course, there remains the constitutionally entrenched right to seek forms of judicial review under s 75(v) of the Australian Constitution and its analogue in s 39B of the Judiciary Act.)

13.50. Given the potential consequences associated with actioning a notice, submitters suggested that DCPs should have the option to appeal a decision to the Federal Court (as opposed to judicially review or seek declaratory relief).

13.51. The Department of Home Affairs submits that there is an important distinction between TANs and TCNs, and warrants or other like instruments. This distinction is said to relate to the difference between technical 'access' and the capacity to obtain 'content'. TANs and TCNs do not provide agencies with the ability to obtain content without an underlying warrant.[614] Instead, notices issued under Schedule 1 provide a tool for ensuring that the content obtained under a warrant is accessible and comprehensible. Given warrants are issued by judicial officers, it was submitted that additional judicial authorisation for notices (to provide access) is unnecessary. At the public hearing, industry representatives reiterated their concerns. During its evidence the AHRC conveniently put the requirements for prior independent review to be credible:

> *So the guarantee of independent and the perception of independence is crucial. And there is also the question of who is technically well-qualified to make good decisions. And again judges or former judges of superior courts are uniquely well-qualified to make the kinds of decisions that would be made under the regime under review.*[615]

13.52. However, the Department of Home Affairs was not moved, reiterating the bright-line distinction between content obtained by warrants and industry assistance under TOLA.[616]

---

[613] AD(JR) Act, Schedule 1, (daaaa).

[614] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 16–17.

[615] John Howell (AHRC): Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 42.

[616] '*It is important though to remember that industry assistance powers do not by themselves allow agencies to obtain content or telecommunications data'* ; Hamish Hansford (Department of Home Affairs): Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 189.

13.53. In a supplementary submission following the hearing, Atlassian supported an AAT model, noting that the advantages included:

- *the ability to appoint technical experts as members and to specify how the Tribunal will be constituted for the approval or review (that is by way of a presidential member sitting with one of more such experts in each case with relevant knowledge or experience in the technical issues at hand); and*
- *critically the availability of reasons for the findings made by the Tribunal, which will provide useful guidance (guardrails) to both the Government and industry for the application of the measures in the Act.*[617]

External oversight

13.54. A number of submissions from Government noted that a further safeguard is provided by external oversight bodies.

13.55. The AFP noted that the Commonwealth Ombudsman has specific oversight responsibilities under TOLA.[618] Thus, law enforcement agencies must notify the Commonwealth Ombudsman within 7 days of issuing, varying, revoking or extending a notice. The Commonwealth Ombudsman may also inspect the records of law enforcement agencies, including the AFP, to determine compliance with these requirements and provide a written report on the results of the inspections to the Minister for Home Affairs. Additionally, the Commonwealth Ombudsman is exempted from the unauthorised disclosure provisions in TOLA, which protect industry assistance request and notice information.

13.56. The Australian Security Intelligence Organisation (ASIO) and Australian Signals Directorate (ASD) noted the oversight role of the IGIS.[619] The Director-General or Attorney-General must notify the IGIS of the revocation of a request or notice issued by ASIO within 7 days of the revocation. The IGIS must also be notified within 7 days of the extension of a TAN or TCN. ASIO advises that these reporting requirements provide additional safeguards and ensures the IGIS has oversight of the exercise of all of ASIO's powers under Schedule 1.

---

[617] Atlassian, Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 2 March 2020, 4.

[618] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, 6.

[619] See the following submissions to the review: ASIO, No 21 ([26]); ASD, No 2 (3).

13.57. Despite these safeguards, numerous submitters considered these mechanisms to be inadequate. The Media and Entertainment Alliance advised that 'other than the remote prospect of compliance audit conducted by the Ombudsman, nowhere is it proposed that detailed public scrutiny of requests, notices, orders, and warrants will be possible'.[620]

Lack of transparency and reporting

13.58. Submitters also reported concerns in relation to the lack of transparency and reporting mechanisms permitted under TOLA.[621]

13.59. At present, s 317ZF(13) authorises DCPs to release public transparency reports that disclose the aggregate number of notices received during a 6-month period. In addition, the Minister for Home Affairs is required to produce a written report each financial year listing the numbers of each type of request or notice issues.[622]

13.60. However, DCPs are prohibited from disclosing additional information in their own transparency reports about the nature of the notices they have received – for example, the nature of the capabilities they have been asked to develop or the type of assistance they are being compelled to provide.

13.61. Internet Australia noted that releasing such transparency reports would be entirely voluntary on the part of DCPs and could not be relied upon to build a complete and accurate picture of the use of Schedule 1 powers.[623]

13.62. Internet Australia noted that the report provided by the Minister for Home Affairs must only list the number of each type of request or notice issued. The reports will not provide information on the types of matters they were issued for.[624]

13.63. Submitters recognised that there are legitimate reasons, such as ongoing operations, to *delay* disclosing details related to the content of a notice.[625] However,

---

[620] Media and Entertainment Alliance, Submission No 13 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 27 September 2019, 6.

[621] See the following submissions to the review: The Allens Hub, No 35 (1–2, 5); Google, No 19 (5).

[622] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, [3.4.4].

[623] Ibid.

[624] Ibid.

[625] Google, Submission No 19 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 20 September 2019, 5.

they reiterated that transparency is absolutely critical to enable the broader public to understand how the authorities are using the powers provided by Schedule 1.[626]

Are the powers necessary?

13.64. I have been assisted by a number of submissions in determining whether the powers enabled by Schedule 1 are *necessary* in their current form. The submissions provided by Government explained the necessity of the framework for responding effectively to modern technological challenges, including encrypted communication.

13.65. I note that many submissions provided by industry submissions acknowledged these complex challenges and agreed that appropriate mechanisms to manage the threat environment are required, although some chose not to comment on whether the assistance framework was *necessary* given their lack of access to information to inform such an assessment.[627]

13.66. The key submissions I received in relation to the necessity of Schedule 1 concerned:

a. the current threat environment and associated technological challenges for law enforcement and intelligence agencies

b. the capacity for TOLA to meet its objectives

c. the manner in which TOLA was passed by Parliament.

d. the availability of the powers to the ICACs.

Impact of the current threat environment

13.67. A number of submissions said that the powers provided by Schedule 1 are necessary due to the current threat landscape.

13.68. Notably, the AFP advised that it needs assistance to ensure its existing powers do not become ineffective and that technology cannot be used to thwart the investigation of serious crimes.[628] It stated that the framework has 'provided significant operational benefit to address a number of emerging and urgent operational issues and facilitated production engagement on potential technical

---

[626] See the following submissions to the review: The Allens Hub, No 35; Google, No 19 (5).

[627] Riana Pfefferkorn, Submission No 4 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 12 September 2019, 5.

[628] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, 10.

options. This has been, and continues to be, of significant value to the AFP's investigative effectiveness'.[629]

13.69. ASIO similarly said that TOLA is 'an essential enabler of its ability to stay abreast of the technical development that might otherwise render its powers ineffective. The mechanisms the Act introduced have offered significant utility to date, and ASIO continues to make operational use of these capabilities'.[630]

13.70. I note that ASD, Queensland Police Service, Tasmania Police and Northern Territory Police Force also value the benefits of the powers enabled under TOLA; however, at this stage the powers have not been used. A number of these agencies continue to consider how the powers may be used and provide appropriate training to officers.[631]

Whether the Act will meet its objectives

13.71. In its submission, Google questioned the policy objective behind the scope of TOLA. It said that it is unlikely that those who commit serious crimes will be using enterprise platforms to communicate with other offenders.[632] Google suggested that the law should be scoped in light of what the agencies know of how these offenders are communicating with each other.[633]

13.72. Dr Isaac Kfir of the Australian Strategic Policy Institute (ASPI), making a submission in a personal capacity, echoed these observations in the national security sphere, noting that the new generation of violent extremists seem to adapt quickly to counterterrorism measures, which could make TOLA redundant in countering terrorists if they are using tools and equipment not covered by the Act.[634]

---

[629] Ibid 55.

[630] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, 83.

[631] LECC, Submission No 23 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 24 September 2019.

[632] Google, Submission No 19 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 20 September 2019, 4.

[633] Ibid.

[634] Isaac Kfir, ASPI, Submission No 18 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 18 September 2019.

13.73. Access Now said that undermining encryption will not solve law enforcement problems and that principles of sovereignty and criminal incentives will likely drive criminals and terrorists towards forms of technology that are beyond the reach of any mandated access mechanism, such as TOLA, leaving those who are less technically sophisticated or financially privileged to bear the brunt of any insecurity caused by TOLA.[635]

13.74. A similar argument was presented by Shogun Cybersecurity, which advised that the type of people (for example, criminals or terrorists) that the Government is targeting with TOLA have other options to privately communicate. It was said that they are capable of creating tools that the authorities have no visibility or understanding of.[636] It was contended that, in the long term, TOLA will in fact make it harder for authorities to stop criminal behaviour, as it will drive criminals away from 'commodity products,' while making other users more vulnerable.[637]

13.75. Dr Chris Culnane and Associate Professor Vanessa Teague from the University of Melbourne advised that it is plausible that targets of the legislation will adapt and learn to circumvent the assistance framework. As such, they concluded:

> *It is our opinion that a reasonably competent adversary could avoid the risk of interception with minimal technical knowledge, and the use of commodity off-the-shelf components. If that is the case, any benefit [associated with the TOLA Act] would be greatly reduced, nearing zero, with a high price paid in terms of privacy, freedom and cybersecurity. Such a trade-off should be considered unacceptable in a modern functioning democracy*.[638]

13.76. Access Now added that there are other means to assist law enforcement – there are many questions at the intersection of crime and technology and, as the PJCIS has recognised, those questions cannot be addressed in isolation.[639] They require

---

[635] Access Now, Submission No 32 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 21 October 2019, 4.

[636] Shogun Cybersecurity, Submission No 46 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 November 2019, 4.

[637] Ibid 4–5.

[638] Dr Chris Culnane and Associate Professor Vanessa Teague (University of Melbourne), Submission No 28 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 9 October 2019, 4.

[639] Access Now, Submission No 32 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 21 October 2019, 4.

careful consideration and investment, including in education and training for law enforcement and research into rights-respecting mechanisms to streamline cross-border requests for data needed. Experts have identified strategies to help law enforcement without undermining encryption. Access Now suggested that these provide a 'better starting point for these conversations and a good path for further investigation'.[640]

Manner in which the Act was passed

13.77. Although I am sure all submitters understand that it is no part of my role to question the parliamentary process, for the benefit of the PJCIS and Government I nevertheless record consistent concern with what was seen by many submitters as a lack of consultation and undue speed in enactment of TOLA.

13.78. Senetas also questioned the necessity of the Act in its current form in light of the response to its passing. Their submission stated:

> *In late 2018, the Minster, the Department and the Director General of ASIO, claimed that the passing of the legislation in early December 2018 was urgent and that further consideration of its impacts and consequences could not be allowed to delay its passing. It was suggested by these parties at the time that the Christmas/New Year holiday season represented a high-risk period and that the legislation was necessary to better protect the community. However, the Submission to the PJCIS by the Department of Communications in July 2019 states that the Department has yet to complete the development of guidelines in relation to the exercise of the authority of the Minister of Communications.*
>
> *Under the Act, the Communications Minister must authorize the issuing of a TCN (and other matters). The fact that there are no guidelines related to the use of this power – more than seven months after the legislation has been passed – must be of serious concern. It is understood that similar practical implementation issues are still being resolved within the Department of Home Affairs as well as in other agencies able to use this legislation.*
>
> *Detective Superintendent Arthur Kopsias of the NSW Police is responsible in that state for enforcing this legislation. In an article published by the AFR on 12 March 2019, he commented that he was unaware of the provisions of the Act prior to it being passed. As a consequence, he didn't 'have a clue how to implement it.'*
>
> *Clearly this must raise questions about the accuracy of the claimed need for urgency in passing the legislation, and more importantly, if it was actually*

[640] Ibid.

necessary at all, given the failure of the bureaucracy to move quickly to bring it into force.[641]

Are the powers proportionate?

13.79. Government agencies submitted that:

a. the powers provided by Schedule 1 are proportionate to the current threat environment

b. the evolving nature of the threat environment and the prevalence of encrypted forms of communication means that the powers enabled by Schedule 1 must remain in their current form.

13.80. I have, above, set out my findings based significantly on notices issued to DCPs and evidence taken from the relevant agencies.

13.81. However, a significant number of submissions, particularly from industry, said that these powers are not proportionate to the aims of TOLA.

13.82. The key issues raised by submitters in relation to *proportionality* were:

1. the impact of Schedule 1 on the commercial interests of Australia's technology and communications industry
2. the definition of 'Designated Communications Provider'
3. the threshold for 'serious offence'
4. the impact on Australia's national security interests
5. the unintended consequences caused by modified technology
6. the potential for conflict of law.

Impact on Australia's technology and communications industry

13.83. Submitters said that the passing of TOLA has had significant consequences for the commercial interests of Australia's technology and communication providers overseas.[642] Submissions reported that there is more than simply global confusion

[641] Senetas, Submission No 6 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 13 September 2019, 11.

[642] See the following submissions to the review: Cogito Group, No 42 (4); Australian Industry Group, No 12 (3).

or misunderstanding about the operation of TOLA, and instead there is real damage being done to Australia's industry.[643]

13.84. Cogito Group said that:

a. TOLA would adversely impact on the global competitiveness of the Australian cybersecurity sector, as international customers will not want to procure software, services or companies with potential vulnerabilities[644]

b. international competitors are able to use TOLA to create a competitive advantage against Australian companies: companies in the US, for example, are able to say to consumers that Australian developed products cannot be trusted and are not secure by design.[645]

13.85. Senetas:[646]

a. expressed serious concern over what it sees as the damage of the Act to Australia's reputation in international markets, and the resulting loss of exports, jobs and technical expertise

b. submitted that TOLA has damaged the reputation and trust of Australian technology developers and manufacturers. This has negatively impacted exports, local research and development, manufacturing, start-ups and education.

13.86. Telstra submitted that, as a notice may require a DCP to supply sensitive technical information, including software source code and service design documentation,[647] sharing this type of commercially sensitive information could, of itself, present a security risk if it ends up in the wrong hands.[648] While there are provisions in the

[643] See the following submissions to the review: Australian Industry Group, No 12 (2); Joint Industry Submission (Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, Digital Industry Group Inc., Information Technology Professionals Association), No 15, (3).

[644] Cogito Group, Submission No 42 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5 February 2020, 1.

[645] Ibid 4.

[646] Senetas, Submission No 6 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 13 September 2019, 1.

[647] Telstra, Submission No 36 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 29 October 2019.

[648] Ibid.

Act's framework obliging agencies to keep the information confidential, Telstra noted that this will not itself provide a commercial remedy to the DCP if their information is compromised (for example, if sensitive commercial information about an upcoming product is released or new features are disclosed).[649]

13.87. Internet Australia submitted as follows:

> *In August 2018 the Australian government banned companies 'likely subject to extrajudicial directions from a foreign government that conflict with Australian law' from participating in Australian future telecommunications infrastructure, and in particular from 5G mobile networks. This ban was largely interpreted and confirmed by Huawei and ZTE as aimed at Chinese-controlled equipment providers. …*
>
> *The Act has put in place a regime where Australian companies will be subject to the same suspicions, and effectively viewed by the international community as subject to the very same concerns around undisclosed surveillance and surreptitious bypassing of security and privacy functions at the request or direction of the Australian government. Australian manufacturers of communications hardware, developers of Australian communications software systems, every Australian telecommunications provider active in a foreign country, and in fact every Australian website involved in ecommerce to international markets could be suspected to be insecure by international markets. Under the current structure of the Bill, these concerns and suspicions will arise just by virtue of the legislation existing, even if the legislation is not used.*[650]

13.88. Cogito Group was concerned about the impact of TOLA on individual employees. If global companies now view Australian staff as 'insider threats', this is likely to discourage investment of global technology firms into Australian personnel. It was said that TOLA has disrupted and constricted the employability and export of Australian technology staff and products.[651]

---

[649] Ibid 4.

[650] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, 16–17.

[651] Cogito Group, Submission No 42 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5 February 2020, 2–3.

13.89. I specifically note Cogito Group's advice that, due to these perceived risks, it has felt it necessary to divert product development to its New Zealand office. It was reported that 'this means less Australians will be employed due to this law'.[652]

13.90. Similarly, Atlassian submitted:

> *The uncertainty about the ability for individual employees to be compelled to give assistance and the prohibition on disclosing TCN information has caused much anxiety among Australian technology workers and global companies with employees in Australia. It has led to certain American technology companies characterising their Australian staff as potential 'insider threats'. This has undermined Atlassian's efforts to recruit talent to Australia and is likely to discourage global technology firms from investing in Australian personnel.*[653]

Definition of 'Designated Communications Provider'

13.91. Several submissions said that the existing definition for 'Designated Communications Provider' is overly broad.[654] The Explanatory Memorandum explains that the term refers to the 'full range of participants in the global communications supply chain, from carriers to over-the-top messaging providers'.[655] One submission reported that this definition could affect 'hundreds of thousands, if not millions, of individuals in Australia and around the world'.[656] Another said that the current definition is so broad that it has the potential 'to capture most of the global supply chain, including organizations that have virtually no link to Australia.'[657]

13.92. Internet Australia said that the inclusion of component manufacturers and suppliers is unnecessary and inappropriate given their inability to control or know where their

---

[652] Ibid 3.

[653] Atlassian, Submission No 17 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 18 September 2019, 3.

[654] See the following submissions to the review: International Civil Liberties and Technology Coalition, No 5 (section 2.2); Internet Australia, No 29; BSA The Software Alliance, No 25 (7); Electronic Frontiers Australia, No 47 (10); Shogun Cybersecurity, No 46 (2); Access Now, No 32 (13–14).

[655] Explanatory Statement, 35.

[656] International Civil Liberties and Technology Coalition, Submission No 5 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 13 September 2019, 6.

[657] BSA, Submission No 25 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 1 October 2019, 16.

products may be used. Inclusion only serves to drive up costs for these businesses and individuals. Even those that might be caught up under this definition will incur significant costs obtaining legal advice and developing processes and procedures for dealing with a request that may never eventuate.[658]

13.93. Google said that this wide definition 'works against the Government's longstanding commitment to cloud first policies by undercutting trust in technology providers, increasing costs, slowing down cloud adoption and weakening security'.[659]

Threshold for 'serious offence'

13.94. A number of submissions said that the thresholds for using the powers enabled by Schedule 1 is too low.[660] At present, the legislation can be applied to preventing or investigating criminal offences that carry a prison sentence of as little as 3 years. One submission points out that this captures 'relatively innocuous offences such as making a prank call'.[661]

13.95. Submitters also noted that this 3-year threshold is out of step with the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), which defines 'serious offence' as an offence punishable by imprisonment for life or for a period, or a maximum period, of at least 7 years.[662]

13.96. Internet Australia stated, regarding TOLA's definition of a serious offence:

> *This is inconsistent with the threshold already defined in s5D of the Telecommunications (Interception and Access) Act 1979 … which defines serious offence comprehensively, including offences such as murder, kidnapping, child exploitation and other offences punishable by life or maximum of 7 years imprisonment.*

---

[658] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, section 2.2.

[659] Google, Submission No 19 to Independent National Security Legislation Monitor, Review of the Telecommunications and Other Legislation (Assistance and Access) Act 2018 (TOLA), 20 September 2019, 3.

[660] See the following submissions to the review: Communications Alliance, No 15 (6); Internet Australia, No 29 (section 2.1); Law Council of Australia, No 45, (8, 11–12); Atlassian, No 17 (4).

[661] Digital Rights Watch & Human Rights Law Centre, Submission No 11 to Independent National Security Legislation Monitor, Review of the Telecommunications and Other Legislation (Assistance and Access) Act 2018 (TOLA), 11 September 2019, 7.

[662] See the following submissions to the review: Digital Rights Watch & Human Rights Law Centre, No 11 (7); Internet Australia, No 29 (section 2.1).

> *The powers granted under the Assistance and Access Act are highly intrusive, and have been described as being required to help combat highly serious matters such as terrorism and child exploitation … However the inconsistency between these two definitions has created the perverse outcome that crimes considered not serious enough for the TIAA Act are considered to be serious enough for this TOLA Act.*[663]

13.97. The Law Council noted that although the threshold of 3 years was recommended by the PJCIS in 2018 Advisory Report on the Bill,[664] it remains of the view that the threshold is too low for the application of the powers. At the public hearing, the Department of Home Affairs[665] pointed out that there are many exemptions in the TIA Act, and some offences included in it carry a 2-year term of imprisonment:

> *the reason why we landed at three years is because it's the assistance to an investigation, potentially and that it is not access to the content.*

The risk of undermining national security interests

13.98. Stanford University's Dr Riana Pfefferkorn submitted that:

a. Encryption and other cybersecurity measures help to protect national security interests, whereas, by undermining cybersecurity, TOLA risks harming those interests.[666]

---

[663] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, section 2.1.

[664] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Australian Government, Canberra, 2018) Ch 2, 'Committee comment and recommendations' <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1/section?id=committees%2freportjnt%2f024247%2f26913>.

[665] Hamish Hansford (Department of Home Affairs): Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 206.

[666] Riana Pfefferkorn, Submission No 4 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 12 September 2019, 4.

b. The basic issue with access mechanisms intended for use by law enforcement and intelligence agencies is that they are susceptible to discovery and abuse by other actors.[667] These actors may use the access to damage national security.[668]

c. By passing TOLA, the Australian Government is opening itself to exploitation by using the same products and services it is forcing to be less secure – whether that is a smartphone, cloud storage or messaging applications and so on.[669]

13.99. Similarly, Amazon Web Services noted that the deliberate creation of a means of accessing otherwise secure data via a notice would create weaknesses and vulnerabilities that create opportunities for other actors – including those with malicious intentions – to access the same data. Their submission notes that 'if anyone creates a vulnerability in a technology that allows access to otherwise secure data then that vulnerability is capable of being exploited by another party with the knowledge and means to do so'.[670]

13.100. The Office of the Victorian Information Commissioner (OVIC) raised similar concerns, noting that TOLA operates on an underlying assumption that only agencies identified under the Act will be able to utilise weaknesses created under TCNs. However, there is a well-documented risk that malicious actors may take advantage of any weaknesses created.[671]

13.101. Access Now also reported that undermining encryption hurts security – every proposal for a mechanism to allow law enforcement to bypass encryption has been found to have security flaws 'that could, if deployed, cause grave damage to people, governments, and infrastructure'.[672] It could also have consequences that we cannot anticipate today.[673]

---

[667] Ibid.

[668] Ibid.

[669] Ibid.

[670] Amazon Web Services, Submission No 41 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5 November 2019, 2.

[671] OVIC, Submission No 7 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 13 September 2019.

[672] Access Now, Submission No 32 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 21 October 2019, 4.

[673] Ibid.

13.102. A number of submissions highlighted the benefits of encryption for protecting the general population from criminal activity online.[674] They advised that encryption promotes freedom of expression, commerce, privacy and user trust and helps protect data from bad actors. Encryption and related techniques are used to build increased security for financial transactions and to protect the private communications of end users.

13.103. Internet Australia outlined the benefits of encryption:

> *Encryption is all around us. It hides usernames and passwords from prying eyes, protects the information exchanged every time a person uses an ATM or swipes a credit card, conducts a purchase from a smartphone, makes a call from a mobile phone, or presses a key fob to unlock a car. It is a versatile technology, increasingly pervasive in our daily lives, and critical to the security of much of what we do. It is critical for all global commerce, banking, and securities markets. Automatic software updates for billions of end-user devices depend on strong encryption and authentication to prevent the update process being maliciously hijacked.*
>
> *For these reasons, the Internet development community is actively working to update all internet communications systems and underlying infrastructure to include strong encryption and authentication by default.*[675]

13.104. Internet Australia similarly pointed out that reducing the security of devices – or even increasing doubts about whether the security has been compromised – reduces the ability of citizens and businesses to rely on the entire system to keep them safe.[676] It was emphasised that there is 'no digital lock that only "good guys" can open and "bad guys" cannot'.[677] They point out that '"lawful access" capabilities created using this legislation and the powers provided under a TCN or TAN will make it easier for others, including criminals and hostile governments, to gain access to sensitive data stored on the same types of devices'.[678]

---

[674] Ibid. See also the following submissions to the review: International Civil Liberties and Technology Coalition, No 5 (2); Internet Australia, No 29 (section 1.2); BSA, No 25 (1); Senetas, No 6 (1).

[675] Internet Australia, Submission No 29 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 11 October 2019, section 1.1.

[676] Ibid 1.2.

[677] Ibid.

[678] Ibid.

The potential for unintended consequences due to modified technology

13.105. Submissions outlined the potential for unintended consequences across communications and technological networks as a result of the assistance framework.

13.106. Telstra submitted that:

a. A notice may require a piece of network equipment supplied by a third party, but distributed by Telstra, to be 'modified'.[679] Given the secrecy provisions in TOLA, these modifications would be completed without the knowledge of providers and may result in an adverse impact to its network and/or its customers.[680] Such effects could include service degradation, network faults, or other impacts on business, or on non-target customers.[681]

b. While the immunity provisions of the framework protect the DCPs providing the assistance/capability under the notice, there is no protection for providers elsewhere in the supply chain if they, or their customers, are adversely impacted by the use of that 'modified' piece of equipment or software.[682] Neither is there any provision for sharing of information or testing of modified equipment or software with the downstream DCPs to reduce the risk of unintended consequences.[683] Therefore, the use of notices presents the risk of issues developing within communication networks that providers will be poorly placed to understand and rectify.

The potential for conflict of laws

13.107. Amazon Web Services noted that notices issued under Schedule 1 could require technology providers to do acts in Australia that violate the laws of other countries in which they operate. It recommends amending s 317ZB(5) such that a DCP has a defence for noncompliance with a notice if it can prove that compliance, either in Australia or in a foreign country, would contravene the law of a foreign country.[684]

---

[679] Telstra, Submission No 36 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 29 October 2019, 3.

[680] Ibid.

[681] Ibid.

[682] Ibid.

[683] Ibid.

[684] Amazon Web Services, Submission No 41 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5 November 2019, 3, 4.

13.108. Atlassian's supplementary submission also noted its continuing concern about the interaction of TOLA with foreign laws. Its concerns include the limitations on the statutory defence only being available to DCPs where they are located in a foreign country and compliance with a notice would breach the laws of that country. Atlassian considered that concern has special significance in the context of these powers, 'given that it may be practically difficult to determine *where* an act or thing must be done' noting 'the globally distributed and interconnected nature of today's supply chain'.[685]

13.109. I note that parties in Australia are able to apply to the courts for injunctions and declarations should they consider that a notice compelling certain actions would force their counterparts in another country to breach that other country's laws.[686]

Schedule 2: Computer access warrants

13.110. I received far fewer submissions on the impact of the computer access warrants provided for in Schedule 2. Those from law enforcement and intelligence agencies detailed the importance and necessity of these warrants in responding to the current threat environment. Conversely, members of industry and human rights groups expressed concerns about the scope and breadth of the warrants and the potential for intrusion on rights.

Does Schedule 2 of the Act contain appropriate safeguards for protecting the rights of individuals?

13.111. I note that the key safeguards relating to computer access warrants relate to the requirements for obtaining a warrant in the first place. The following sections detail these requirements, first for law enforcement agencies and then for ASIO.

Warrant process for law enforcement agencies

13.112. Submissions provided by the Department of Home Affairs and law enforcement agencies advised that there are appropriate restrictions and safeguards embedded into the process for obtaining a computer access warrant, as well as the rules for using a warrant once obtained.

13.113. First, law enforcement officers can seek a computer access warrant only if an officer has reasonable grounds to suspect that a relevant offence has been or will be committed; an investigation is or will be underway; and access to data is necessary

[685] Atlassian, Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 5.

[686] See, for example, *Bank of Valletta PLC v National Crime Authority* [1999] FCA 1099; (1990) 90 FCR 565.

to obtain evidence of the offence or information about the offenders. The warrant itself must be issued by a judge or member of the AAT. This decision-maker must be satisfied of the grounds for the application and have regard to a number of factors, including the extent to which the privacy of any person is likely to be affected by the warrant.[687]

13.114. The Department of Home Affairs particularly noted that a computer access warrant does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer except in circumstances where doing so is necessary for the execution of the warrant. It also notes a warrant does not authorise causing any other material loss or damage to other persons lawfully using a computer except where necessary for concealment.[688]

13.115. The Department of Home Affairs additionally advised that the chief officer of the relevant law enforcement agency must revoke the warrant if it is no longer required to obtain evidence of the offence.[689] The chief officer also has an obligation to ensure that access to data is then discontinued.

13.116. Further, the unauthorised disclosure of information about, or obtained under, a computer access warrant is an offence. The maximum penalty for the offence is 2 years' imprisonment or 10 years if the disclosure endangers the health or safety of any person or prejudices an investigation into an offence.[690]

13.117. Finally, the Department of Home Affairs pointed out that the use, recording and communication of information obtained in the course of intercepting a communication in order to executive a computer access warrant is restricted. Where agencies want to gain intercept material for its own purpose, they must be issued with the relevant warrant under the TIA Act.[691]

---

[687] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 23.

[688] Ibid 24.

[689] Ibid.

[690] Ibid.

[691] Ibid.

The warrant process for ASIO

13.118. Similarly, submissions from the Department of Home Affairs and ASIO noted that there are appropriate restrictions and safeguards built into the process allowing ASIO to obtain a computer access warrant and to use the warrant once issued.[692]

13.119. ASIO noted that all its warrants are issued by the Attorney-General. In terms of issuing a computer access warrant, the Attorney-General must be satisfied that there are reasonable grounds for believing that access to data held in a computer will substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security.[693]

13.120. Additionally, ASIO notes that, for each warrant issued by the Attorney-General, the Director-General is required to provide the Attorney-General with a written report on the extent to which action taken under the warrant has assisted ASIO in carrying out its functions.[694]

13.121. ASIO advised that TOLA includes specific prohibitions in relation to each new power under Schedule 2, specifying that the relevant sub-sections do not authorise the doing of a thing that is likely to materially interfere with a communication in transit, or the lawful use by other persons of a computer (unless necessary to do one or more of the specified things), or cause any other material loss or damage to other persons lawfully using the computer. In addition, if a computer of other thing is removed under a power, it must be returned when no longer prejudicial to security, or within a reasonable period. Anything done to conceal the fact that anything has been done under warrant must be undertaken while the warrant is in force, within 28 days after it ceases to be in force, or at the earliest time after that 28-day period at which it is reasonably practicable to do so.[695]

13.122. ASIO further noted that Schedule 2 made amendments to s 24(4) of the ASIO Act to make clear that the new provisions under s 25A, s 27A and s 27E are within the definition of 'relevant device recovery provisions' for the purposes of s 24. This provides a safeguard against the arbitrary exercise of the range of activities permitted by the new provisions by requiring the person or class of persons exercising these powers to be approved by the Director-General personally. If, as at the end of a prescribed post-cessation period of a warrant, it is likely that a post-

[692] See ibid 23–24 and the discussion below for the ASIO submission.

[693] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, 8.

[694] Ibid 9.

[695] Ibid 8.

cessation concealment activity will be done in connection with the warrant, the Director-General must give the Attorney-General a written report on the extent to which the activity will assist in carrying out its functions.[696]

13.123. Additionally, ASIO noted that IGIS conducts regular inspections of ASIO warrants, on a sampling basis, and performs regular inspections of ASIO activities as part of its oversight function. The IGIS may also conduct detailed inquiries and is also able to consider any complaints received from persons affected by, or otherwise involved in, the exercise of ASIO's powers.[697]

Are the powers necessary?

13.124. Submissions provided by law enforcement and intelligence agencies emphasised the necessity of computer access warrants for managing the current threat environment.

13.125. In particular, ASIO advised:

> *Methods of computer access must evolve to match changes in both target technology and the operational environment, and do not conform to one single model of operation. ASIO considers that the new powers in Schedule 2 of the Act provide an update to ASIO's computer access warrant regime necessary to keep pace with technology.*
>
> *The new mechanisms provided under Schedule 2, have enhanced the operational effectiveness of ASIO's computer access warrant regime within the current technical context. There is no reason to anticipate a change in the nature of our operations such that these mechanisms will not continue to provide significant benefit into the future.*[698]

13.126. The AFP further noted that computer access warrants are necessary for allowing law enforcement agencies to effectively and efficiently search electronic devices and content of devices. It reported that computer access warrants address significant gaps in capabilities under existing legislation.[699] Its submission outlines the challenges associated with data surveillance devices and obtaining historical evidential material stored on a computer.

---

[696] Ibid 9.

[697] Ibid.

[698] Ibid 10.

[699] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, 11.

13.127. The AFP reported that the powers provided by Schedule 2 overcome these issues by allowing law enforcement agencies to intercept communications to facilitate access to relevant data, including access to premises (including third-party premises), to remove a computer or device, and the doing of anything reasonably necessary to conceal anything done under the warrant to protect the covert nature of computer access warrants and covert capabilities.[700] This may include the deletion of access logs or software installed to facilitate the access and search for relevant data. The AFP advised:

> *This is essential to ensure that the persons that are the subject of the investigation are not prematurely alerted to the police investigation potentially resulting to the destruction or interference with evidence, counter measures being developed to identify police methodologies, alerting of other participants or fleeing prior to police intervention or criminal proceedings being instituted.*[701]

13.128. The AFP provided the following case study to illustrate how computer access warrants are used:

> *[The AFP conducted an] investigation into the use of a carriage service to make a threat of telephony style attacks against the Australian public and government telecommunications infrastructure. This was a parallel investigation to Victoria Police investigation of sabotage offences against Victoria Police stations and their Private Automatic Branch Exchange (PABX) telephony systems. Following the confirmation of a target computer suspected of enabling the commission of the offending, AFP obtained a CAW. The CAW enabled the AFP to covertly acquire the contents of multiple systems used by the offender in the commission of a variety of offences. Information obtained under this warrant informed various affidavits, identified multiple further avenues of Police enquiry and filled significant evidentiary gaps in relation to the alleged offending and better directed Police resources in relation to this investigation. Further a significant proportion of the material obtained under the CAW is relied on in a brief of evidence in relation to the accused.*[702]

Are the powers proportionate?

13.129. A number of submissions said that the scope of action that may be taken with a computer access warrant is not proportionate to the threat environment. The main areas of concern were:

1. the breadth of powers enabled by the warrants

[700] Ibid 12.

[701] Ibid.

[702] Ibid.

2. the breadth of concealment of access powers associated with actioning the warrants
3. the potential issues associated with emergency authorisation for the warrants
4. the potential for computers to be removed from premises.

Breadth of the computer access warrants

13.130. The AHRC and Law Council of Australia detailed their concern that computer access warrants represented a 'significant' broadening or expansion in the powers available to law enforcement agencies and ASIO.[703]

13.131. The Media Entertainment and Arts Alliance submitted that a recent example of overreach was the AFP's execution of a warrant at the headquarters of the Australian Broadcasting Corporation. The warrant allowed the AFP to 'use any other computer or communication in transit to access the relevant data; and if necessary to achieve that purposes[sic] – to add, copy, delete, or alter other data in the computer'. The Media Entertainment and Arts Alliance considers the ability for warrants to allow a Government agency to 'add, copy, delete or alter' information on a computer system an 'outrageous and frightening development in Australia'. That submission noted that the AFP's keyword search terms initially captured 9,214 emails and documents, which was submitted to be example of 'a very wide net being cast'.[704]

Breadth of the concealment of access powers

13.132. In their submissions, the AHRC and Law Council of Australia expressed concern about the 'concealment of access' powers that attach to computer access warrants.[705] These powers permit law enforcement agencies and ASIO to do 'anything reasonably necessary to conceal the fact that anything has been done under the warrant' (s 25A(8)(c)).

13.133. It was noted that the time frames provided for these concealment activities include any time while the warrant is in force, within 28 days after it ceases to be in force or 'at the earliest time after that 28 day period at which it is reasonably practicable'.

---

[703] See the following submissions to the review: Law Council of Australia, No 45 (8); AHRC, No 30 (26).

[704] Media, Entertainment and Arts Alliance, Submission No 13 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 27 September 2019, 5.

[705] See the following submissions to the review: AHRC, No 30 (29); Law Council of Australia, No 45 (32).

The AHRC considered that this unclear time limitation means the powers have the potential to apply very broadly.[706]

13.134. The Law Council considers that the absence of a time limit by which concealment of access powers may be exercised may authorise privacy-intrusive activities in the absence of the 'reasonable grounds' threshold which underpins the initial warrant.[707]

Emergency authorisations

13.135. The Law Council also expressed concern that the amendment to s 32(4) of the *Surveillance Devices Act 2004* (Cth) (SD Act) permits telecommunication interceptions under computer access warrants which have received emergency authorisation, meaning they have not been approved by an eligible judge or a nominated AAT member, and these warrants can be issued for a much broader range of offences.[708]

13.136. The Law Council further expressed concern that the temporary removal of computers and other things pursuant to s 25A of the ASIO Act and s 27E of the SD Act is too broad.[709] It was reported that this power would allow the Attorney-General, judge or nominated AAT member to authorise the temporary removal of computers or other things from premises for the purpose of entering specified premises or gaining entry to, or exiting, specified premises. The Law Council said that it is unclear why this power is necessary or justified and recommended the temporary removal power should be limited to the purpose of obtaining access to 'relevant data' under the ASIO Act and SD Act provisions.[710]

Schedule 3: Law enforcement search powers

13.137. I did not receive many submissions on the impact of Schedule 3. The majority of information provided related to whether the powers were necessary to manage the current threat landscape.

---

[706] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, 29.

[707] Law Council of Australia, Submission No 45 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 6 November 2019, 32.

[708] Ibid 30.

[709] Ibid 31.

[710] Ibid 10.

Does Schedule 3 contain appropriate safeguards for protecting the rights of individuals?

13.138. The Department of Home Affairs detailed the safeguards associated with the use of powers under Schedule 3. Similar to Schedule 2, these safeguards relate to the process associated with obtaining the warrant in the first place.

Safeguards for modernised Crimes Act search warrants

13.139. The Department of Home Affairs reported that the search warrants are supported by strong safeguards to ensure they are only issued to meet legitimate law enforcement objectives and that law enforcement do not adversely affect privacy and the integrity of the data or device.[711]

13.140. The department noted that warrants must be approved by an independent issuing officer employed by the court. To grant the warrant, the judicial offer must be satisfied that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, evidential material on the premises or person.[712]

13.141. In their submission, the Media Entertainment and Arts Alliance pointed out that the test that the judicial officer must only suspect, on reasonable grounds, that evidential material is held on a device has the potential to facilitate fishing expeditions by law enforcement agencies.[713] That is, the burden for obtaining the warrant is so low that the communications data of a large number of citizens could be accessed.

13.142. There is a substantial body of case law regarding judicial officers suspecting on reasonable grounds (and cognate expressions). That case law has arisen through a variety of statutory provisions that empower police to, for example:

a. arrest a person without warrant based on a reasonable suspicion of commission of an offence

b. apply for a warrant to conduct a search upon there being reasonable grounds for suspecting that this would yield evidence of the commission of an offence.[714]

---

[711] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 24.

[712] Ibid.

[713] Media, Entertainment and Arts Alliance, Submission No 13 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 27 September 2019, 5.

[714] See, for example, Crimes Act, ss 3E, 3T, 3W, 3WA and 3ZE.

13.143. It is worthwhile mentioning that body of law here. As I have noted previously, when a statute prescribes that there must be 'reasonable grounds' for suspecting, it requires facts which are sufficient to induce that state of mind in a reasonable person.[715]

13.144. In *Hussien v Chong Fook Kam*, the Privy Council observed:

> *Suspicion in its ordinary meaning is a state of conjecture or surmise where proof is lacking: 'I suspect but I cannot prove'*.[716]

13.145. The facts which reasonably ground a suspicion may be quite insufficient reasonably to ground a belief, yet some factual basis for the suspicion must be shown.[717] Where a suspicion arises from idle speculation and has no foundation on the facts, it is not a reasonable one.[718]

13.146. In *Queensland Bacon Pty Ltd v Rees*, Kitto J observed that:

> *[a] suspicion that something exists is more than a mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust, amounting to a 'slight opinion, but without sufficient evidence".'*[719]

13.147. Additionally, the Department of Home Affairs noted that a warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt, or obstruct a communication in transit or the lawful use by other persons of a computer.[720] An exception to the limitation is where the actions are necessary to execute the warrant by, for example, overwriting existing metadata attached to relevant files.[721]

13.148. In its supplementary submission and in response to a question on notice, the AFP stated it 'does not use, and does not consider' s 3LA of the *Crimes Act 1914* (Cth) 'as a detention or quasi-detention power' and that the use of s 3LA for the purpose of detaining a person would not constitute a proper use of the power. Whilst such orders are issued by a magistrate and the magistrate may also determine if any

---

[715] *George v Rockett* [1990] HCA 26; (1990) 170 CLR 104, 115.

[716] *Hussein v Chong Fook Kam* [1970] AC 942, 948.

[717] *George v Rockett* [1990] HCA 26; (1990) 170 CLR 104, 115.

[718] *Brebner v Seager* (1926) VLR 166, 170 (Mann J).

[719] *Queensland Bacon Pty Ltd v Rees* (1966) 115 CLR 266, 303 (citing the definition in the *Chamber's Dictionary*).

[720] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 25.

[721] Ibid.

conditions are to be placed on the requirement to provide information, the AFP commented that:

> *unless under arrest, the person is free to leave the company of the police officer executing the section 3LA order. Further, while a section 3LA order may require a person to attend at a particular location to provide assistance, the order does not provide a power for the person to be 'detained' for that purpose. Should a person choose not to comply with that order, the executing police officer may consider arrest under section 3W of the Crimes Act should the circumstances fit, however this is an independent power to the section 3LA order.*[722]

13.149. A joint supplementary submission from the Department of Home Affairs and the AFP dealt with how such issues would relate to minors. It noted that whether someone was a minor would be stated in the warrant, that TOLA does not change the previously existing processes and protections afforded to persons the subject of a warrant, and that other non-compulsory methods would generally be used to begin with. However, that submission noted:

> *[It] may be appropriate for a person under the age of 18 to be named in the 3LA order, as the registered owner or user of a computer (which could include a smartphone), following due consideration by the issuing Magistrate*.[723]

Safeguards for increased Crimes Act assistance order penalties

13.150. The Department of Home Affairs noted that a number of pre-existing conditions in s 3LA(2) must be met before a magistrate can grant an order to allow enforcement to compel a person to give assistance accessing data; TOLA did not amend these safeguards. These conditions include that the magistrate is satisfied that there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device, the specified person is connected to the device, and the specified person has relevant knowledge to enable them to access the device.[724]

---

[722] Australian Federal Police, Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 1.

[723] Department of Home Affairs, Supplementary Submission to the Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), Page 5 (Attachment B).

[724] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 26.

Are the powers necessary?

13.151. I note the AFP's advice that it has used the search warrant provisions provided by Schedule 3 to collect evidence from electronic devices found during search warrants. It was reported that advances in technology, such as smartphones, Chromebooks, cloud-hosted storage, backup storage and file sharing means that it is increasingly difficult for law enforcement agencies to identify where digital evidence will be hosted. Further, increasing data volumes and security being applied to data, including encryption, means that accessing and identifying relevant data is taking longer.[725]

13.152. The AFP reported that the amendments to allow officers to 'add, copy, delete or alter' data on a device during a search warrant is a necessary part of interaction with modern electronic devices such as smartphones, which do not permit the removal of data storage to readily attach to a writeblocker as traditionally occurred with removable storage from desktop computers.[726] As a result, electronic devices are increasingly required to be powered on and specialist software installed to enable access and preservation of relevant data, thereby necessitating the need to add, copy, delete or alter data. Data such as passwords and other security features may be required to be altered or removed (that is, reset or deleted) to enable access and identification of relevant data. The provisions to 'add, copy, delete or alter' data does not extend to other purposes such as deletion or altering of illegal possessed material (such as child exploitation or classified documents) or to mislead or prevent ongoing access by co-offenders.[727]

13.153. The AFP reported that the ability to overtly and remotely access data enables the use of higher speed equipment and larger bandwidth network connectivity to search and copy relevant data than may otherwise be available at the premises nominated in the warrant.[728] Increasingly, the AFP was required to spend large periods of time onsite at warrants to access, search and copy relevant data prior to TOLA.

13.154. The AFP also explained that the hyper-connectivity of modern technology and increasing data volumes means that most modern devices will remotely store account-based data. This account-based data can be a rich source of evidence and

[725] Australian Federal Police, Submission No 27 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 4 October 2019, 12.

[726] Ibid.

[727] Ibid.

[728] Ibid.

may include information that has subsequently been deleted and is therefore no longer accessible through examination or seizure of the device.[729]

13.155. In light of the benefits of these uses, the AFP submitted that the provisions 'remain necessary to ensure the AFP can access intelligible communications needed for investigation and prosecution of serious crime into a future where the way in which individuals (and businesses) store, use and engage with data has and continues to be increasingly remotely hosted'.[730]

Are the powers proportionate?

Proportionality of search warrants to the current threat environment

13.156. Similar to the AFP's advice on the necessity of these powers, the Department of Home Affairs advised that the enhancements made to search warrants in both the Crimes Act and Customs Act directly reflect the realities of interrogating digital devices. As the changes have been made to reflect modern technological challenges, the Department of Home Affairs considers them to be 'naturally proportionate'.[731]

Proportionality of assistance orders to the current threat environment

13.157. The Department of Home Affairs reported that pre-existing provisions in the Crimes Act enabled law enforcement to compel people to assist in providing data held in a device.[732] Schedule 3 amended the law to ensure that the penalties for noncompliance with an assistance order reflect the potential ramifications for the security of the community.

13.158. The department advised that, under the previous regime, offenders frequently refused to comply with an assistance order in instances where the evidence on their device may lead to a more severe penalty than noncompliance with the order.

13.159. The department provided an example where an individual was prosecuted on 13 charges relating to the control of multiple child sexual abuse websites he used to distribute and facilitate the production of child pornography material. He received total effective sentence of 15 years and 6 months' imprisonment with a non-parole period of 10 years. For the offence under the s 3LA of the Crimes Act, he was

[729] Ibid 13.

[730] Ibid 13.

[731] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 28.

[732] Ibid.

sentenced to 6 months' imprisonment. The department noted that this sentence must be considered in the context of the overall sentence.[733]

13.160. The department advised that Schedule 3 introduced a tiered approach to enforcement which ensures the penalties are reflective of the gravity of noncompliance with an assistance order. The department considers this enforcement structure to be 'proportionate and ensures the penalties for non-compliance are reflective of the potential harm it may cause to innocent Australians'.[734]

Schedule 4: Australian Border Force powers

Does Schedule 4 contain appropriate safeguards to protect individual rights?

13.161. Similar to my analysis of Schedule 3, the key safeguards associated with the use of the powers provided by Schedule 4 relate to the process associated with obtaining the warrant and enforcing assistance orders.

The warrant process for giving modernised Customs Act search warrants

13.162. The Department of Home Affairs advised that appropriate safeguards are built into the warrant process. This process requires a judicial officer to ensure a warrant is only issued when necessary to meet the ABF's objectives and is proportionate to the potential offence. The judicial officer must also believe, on reasonable grounds, that the computer or data storage device is evidentiary material and that the seizure is necessary to prevent the concealment, loss or destruction of that item.[735]

13.163. Further, the Department of Home Affairs noted that the addition, deletion or alteration of data is not authorised when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless specified in the warrant. The addition, deletion or alteration of data is also not authorised when those actions are likely to cause any other material loss or damage to other persons lawfully using a computer.[736]

Conditions for increased Customs Act assistance order penalties

13.164. The Department of Home Affairs noted that a number of conditions in s 201A(2) must be met before a magistrate grants an order to allow officials to compel a person to give assistance accessing data. These conditions include that the

[733] Ibid.

[734] Ibid 29.

[735] Ibid 25.

[736] Ibid.

magistrate must be satisfied that there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device, the specified person is connected to the device, and the specified person has relevant knowledge to enable them to access the device.[737]

13.165. The department also noted that the ABF must make an application in an affidavit setting out the reasons why these powers are needed.[738]

Are the powers necessary?

13.166. The Department of Home Affairs advised that the provisions included in Schedule 4 are necessary for ensuring the ABF is equipped to respond to modern challenges. The department provided analysis supporting the necessity of these amendments, including:

> *Schedule 4 enabled judicial officers to issue warrants authorising the Australian Border Force to search or frisk a person if they are satisfied that there are reasonable grounds for suspecting that the person possesses, or will possess in the next 72 hours, a computer or data storage device that is evidential material.*
>
> *…*
>
> *Under previous laws, the Australian Border Force could only obtain a judicial authorisation for a search warrant relating to a search of premises. The amendments were made in recognition that information is often stored on devices, held physically by persons, and that an ability to access this information may impede legitimate investigations and prosecutions*.[739]

13.167. I did not receive advice from stakeholders contending that these powers were not necessary.

Are the powers proportionate?

13.168. The Department of Home Affairs advised that the enhancements made to search warrants in the Customs Act are proportionate to the challenges the ABF faces.[740] I received no advice from other stakeholders questioning the proportionality of these provisions.

---

[737] Ibid 26.

[738] Ibid.

[739] Ibid 33.

[740] Ibid [168] and [203]–[210].

Schedule 5: Australian Security Intelligence Organisation powers

13.169. In contrast to Schedules 3 and 4, I have received a number of submissions in relation to the safeguards, necessity and proportionality of Schedule 5 powers.

Does Schedule 5 contain appropriate safeguards to protect individual interests?

13.170. I have received submissions as to:

1. the safeguards embedded into the process for obtaining requests
2. the potential for compliance with a notice to amount to a form of detention
3. the oversight of ASIO by the IGIS
4. the existence of ASIO's reporting obligations
5. the risk of individuals not being protected if they comply with TARs rather than TANs or TCNs.

Safeguards embedded into the process for obtaining requests

Section 21A: Voluntary requests

13.171. The Department of Home Affairs advised that the Director-General is responsible for issuing requests for voluntary assistance under s 21A. To issue these requests, the Director-General must be satisfied, on reasonable grounds, that the conduct is likely to assist ASIO in the performance of its functions.

13.172. In addition, s 21A(8) allows the Director-General to give an evidentiary certificate certifying the factual basis necessitating the assistance provided. The certificate should detail how the relevant conduct was likely to assist ASIO in the performance of its functions.[741]

Section 34AAA: Assistance orders

13.173. The Department of Home Affairs noted that a s 34AAA order allows the Director-General to request the Attorney-General to make an order requiring a person to provide information or assistance to ASIO that is reasonable and necessary to allow ASIO to access, copy or convert data held in computers or data storage devices. However, this means a s 34AAA order can only apply to a computer or data storage device already accessible to ASIO pursuant to a warrant or authorisation.[742]

[741] Ibid [159]–[160].

[742] Ibid [163].

13.174. Additionally, the Department of Home Affairs noted that a person may only be issued with an order if they are reasonably suspected of being involved in activity prejudicial to security, or a person who is otherwise connected to the device. The person must also have relevant knowledge of the device or computer network.[743]

Complying with an order amounting to detention

13.175. In its submission, ASIO advised that Schedule 5 amended Part III of the ASIO Act (s 21A request) to provide ASIO with the power to request persons or bodies to engage in conduct to assist ASIO in the performance of its functions. However, ASIO firmly noted that it has no powers of compulsion. It was noted that any person or body who received a request can choose not to comply.[744]

13.176. However, in addition to voluntary requests, Schedule 5 gives ASIO the power to require a person to provide information or assistance to ASIO (s 34AAA request). Submitters expressed concern that, if a person is *required* to provide assistance, this may arguably amount to arbitrary arrest or detention of a person.[745]

13.177. IGIS noted that, if a person departs a place where they are *compelled* to provide assistance, they will have committed an offence. Further, s 34AAA does not impose a time limit on the duration of which a person is required to attend a place to provide assistance. The AHRC advised that, while a person may not be physically restrained, it appears they would effectively be prevented from leaving a specified place prior to the completion of the designated assistance task (under pain of criminal penalties).

13.178. I note that the AHRC advised that these circumstances, in their view, may engage the prohibition on arbitrary detention in Article 9 of the *International Covenant on Civil and Political Rights*. Additionally, IGIS and the Law Council point out that there are few, if any, safeguards against this risk, particularly in the absence of judicial oversight.[746]

13.179. Additionally, the AHRC expressed concern that the assistance provisions enabled under Schedule 5 do not make provisions for the kinds of protections available to people who are subject to questioning warrants or questioning and detention

---

[743] Ibid [164].

[744] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, [63]–[64].

[745] See the following submissions to the review: IGIS, No 37 (64); Law Council of Australia, No 45 ([149]–[150]); AHRC, No 30 ([122]).

[746] See the following submissions to the review: IGIS, No 37 (9); Law Council of Australia, No 45 ([149]).

warrants under Part III, s 34AAA, of the ASIO Act.[747] For example, the new assistance order regime under s 34AAA of the ASIO Act does not make provision for a person to contact a lawyer or family member; there is no maximum period prescribed for the giving of assistance; there is no obligation on officers to explain the nature of the assistance order and what it requires; there is no obligation on officers to explain how to make a complaint to the IGIS or to challenge the making of the assistance order in court; there is no obligation to make an interpreter available if necessary; and there is no statutory obligation to treat the person humanely and with respect for their human dignity.[748]

13.180. During the public hearing I put this prospect – of assistance provided under a s 34AAA request potentially amounting to detention – to the Director-General of Security, Mr Mike Burgess. He did not accept that proposition, noting that the advice he has received is in accordance with the administrating agency for the ASIO Act, the Department of Home Affairs, which also does not accept the proposition.[749]

13.181. As discussed above, similarly the AFP does not consider s 3LA of the *Crimes Act 1914* (Cth) as a detention or quasi-detention power.

Oversight by IGIS

13.182. In terms of safeguards, ASIO noted that it is obliged to notify the IGIS within 7 days of making a request for assistance under s 21A of the ASIO Act. This 'acts as an important safeguard and ensures each and every use of this power is subject to oversight by the IGIS' (ASIO Act, s 21A(3A)).[750]

---

[747] See, for example, the discussion in the report of the second INSLM (the Hon Roger Gyles AO) on (i) the prospect of indefinite detention arising under execution of detention and questioning powers; and (ii) person is being questioned: Roger Gyles AO, Independent National Security Legislation Monitor, *Certain Questioning and Detention Powers in Relation to Terrorism* (Australian Government, Canberra, 2017) 7.34, 7.36.

[748] Australian Human Rights Commission, Submission No 30 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 16 October 2019, [121]–[123].

[749] Independent National Security Legislation Monitor, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), Public Hearing Transcript, 19.

[750] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, [70].

Reporting obligations

13.183. ASIO advised that it is required to include a statement in its annual report of the total number of requests made under ss 21A and 34AAA (that requirement being s 94(2BC) of the ASIO Act).[751]

Validity of voluntary requests

13.184. Section 21A provides civil immunities for assistance provided voluntarily in accordance with a request from the Director-General, so long as certain listed requirements are met.

13.185. The Law Council expressed concern about the potential for ASIO to request voluntary assistance, avoiding the need to otherwise obtain special powers warrants that would require ministerial authorisation under the ASIO Act. This may create a risk that an aggrieved person will not have access to a legally enforceable remedy given the availability of the immunity of civil liability. It would also reduce the safeguards involved in requiring ASIO to obtain ministerial approval. The Law Council recommended that, where ASIO would otherwise require ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request for the same assistance.[752]

Are the powers necessary?

13.186. The Department of Home Affairs reported:

> *The rapidly evolving nature of technology, including the prevalence of encryption, is impacting the Australian Security Intelligence Organisation's ability to gain access to data stored on computer devices and networks. This data is critical for the Australian Security Intelligence Organisation to better understand the national security threat environment.*[753]

13.187. The Department of Home Affairs continued to advise that Schedule 5 addressed this issue by allowing the Director-General to request the Attorney-General to make an order requiring a person to provide information or assistance in specific circumstances.[754]

---

[751] Ibid [69].

[752] Law Council of Australia, Submission No 45 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 6 November 2019, 11 and 36.

[753] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 35.

[754] Ibid.

13.188. The Department of Home Affairs explained that the types of assistance that ASIO may seek with these powers include 'compelling a target or a target's associate to provide the password, pin code, sequence or fingerprint necessary to unlock a phone subject to a section 25 computer access warrant'.[755] This power, therefore, enables ASIO to compel those capable of providing ASIO with knowledge or assistance to access data to do so.

13.189. Further, ASIO reported that it operates in a contemporary environment that is characterised by continually evolving technology and ubiquitous encryption. Under these circumstances, ASIO will increasingly need to call upon the assistance of others to fulfil its functions. The new mechanisms provided under Schedule 5 allow ASIO to engage voluntary support, where available, and compel assistance under circumstances where it is necessary to do so.[756]

Are the powers proportionate?

13.190. A number of submissions discussed the proportionality of the powers provided in Schedule 5. The key concerns raised were:

1. the issue of proportionality that is embedded in Schedule 5 of the Act
2. the cessation of action where issuing grounds no longer exist.

Proportionality to the threat environment

13.191. The Department of Home Affairs advised that:

> *[Assistance orders (s 34AAA) are] directed towards the legitimate objective of ensuring that the Australian Security Intelligence Organisation can give effect to warrants which authorise access to a device. The Australian Security Intelligence Organisation's inability to access a device can frustrate operations to protect national security. The measures are a reasonable and proportionate response to the challenges brought about by new technologies, including encryption.*[757]

13.192. The Department of Home Affairs advised that the Attorney-General's guidelines specify that any information obtained by ASIO is to be obtained in accordance with several principles. These include that 'any means used for obtaining information

[755] Ibid 36.

[756] Australian Security Intelligence Organisation, Submission No 21 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 23 September 2019, [81].

[757] Department of Home Affairs, Submission No 26 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 3 October 2019, 29.

must be proportionate to the gravity of the threat posed and the probability of its occurrence'.[758] As information-gathering powers, both new powers provided by Schedule 5 are subject to these guidelines.

The Department of Home Affairs also noted that it is standard internal practice for ASIO to consider proportionality when making decisions.[759]

Cessation of action where issuing grounds no longer exist

13.193. The IGIS submitted that there is no obligation on the Director-General of Security to immediately take all necessary steps to cease executing a compulsory assistance order if the underlying warrant has expired or if the issuing grounds have otherwise ceased to exist.[760] Section 34AAA(3D) obliged the Director-General to inform the Attorney-General if satisfied that the grounds on which an order was made have ceased to exist, and s 34AAA(3E) obliged the Attorney-General to revoke the order if satisfied that the grounds on which the order was made have ceased to exist.[761] However, the IGIS points out that, unlike the obligation that applies to ASIO's special powers warrants, there is no immediate obligation on the Director-General to take such steps as are necessary to ensure that action under the order is discontinued.[762]

13.194. Similarly, there is no requirement for the Director-General of Security to delete records or copies of information obtained under an assistance order if the Director-General is satisfied that it is no longer required for the purpose of ASIO's functions and powers.[763] This is an obligation under s 31 of the ASIO Act in relation to information obtained under an underlying special powers warrant. However, not all information obtained under a compulsory assistance order would be covered by s 31 (such as log-in credentials, biometric information).[764]

---

[758] Ibid.

[759] Ibid.

[760] Inspector-General of Intelligence and Security, Submission No 37 to Independent National Security Legislation Monitor, Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA), 30 October 2019, 13–14.

[761] Ibid.

[762] Ibid.

[763] Ibid 10.

[764] Ibid.