PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

August 2021
CANBERRA

ISBN 978-1-76092-249-8 (Printed Version)

ISBN 978-1-76092-250-4 (HTML Version)

Contents

Terms of Reference

The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill) was introduced into the House of Representative by the Hon Peter Dutton MP, then Minister for Home Affairs on 3 December 2020 and was referred to the Committee on 7 December for inquiry and report.

Members

Chair

Senator James Paterson

Deputy Chair

Hon Anthony Byrne MP

Members

Senator the Hon Eric Abetz

Dr Anne Aly MP

Hon Mark Dreyfus QC MP

Senator the Hon David Fawcett

Ms Celia Hammond MP

Senator the Hon Kristina Keneally

Mr Julian Leeser MP

Senator Jenny McAllister

Mr Tim Wilson MP

Abbreviations

AAT	Administrative Appeals Tribunal
AIC	Australian Intelligence Community (comprising ASIO, ASIS, ASD, AGO, DIO and ONI)
AIIA	Australian Information Industry Association
ACIC	Australian Criminal Intelligence Commission (established as the Australian Crime Commission in the ACC Act)
ACC Act	*Australian Crime Commission Act 2002*
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
AFP Act	*Australian Federal Police Act 1979*
AHRC	Australian Human Rights Commission
ANAO	Australian National Audit Office
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
ATW	Account takeover warrant
AUSTRAC	Australian Transactions Reports and Analysis Centre
AWS	Amazon Web Services
CA	Communications Alliance
Crimes Act	Crimes Act 1914
CSCRC	Cyber Security Cooperative Research Centre

DDW	Data disruption warrant
DIGI	Digital Industry Group Inc
EM	Explanatory Memorandum
HRLC	Human Rights Law Centre
IGIS	Inspector-General of Intelligence and Security
IGIS Act	*Inspector-General of Intelligence and Security Act 1986*
Inspector-General	The individual holding the statutory position of Inspector-General of Intelligence and Security, under section 6 of the IGIS Act
Integrity bodies	The Ombudsman, the Australian Human Rights Commission, the Information Commissioner, the Integrity Commissioner, and the Inspector-General of the Australian Defence Force
IIR	2017 Independent Intelligence Review
IM Bill	Integrity Measures and Other Legislation Amendment (Intelligence Oversight) Bill 2020
INSLM	Independent National Security Legislation Monitor
IPO Bill	Telecommunications Legislation Amendment (International Production Orders) Bill 2020
ISA	*Intelligence Services Act 2001*
NAW	Network activity warrant
NIC	National Intelligence Community (comprising ASIO, ASIS, ASD, AGO, DIO, ONI, the ACIC, and the intelligence functions of the AFP, AUSTRAC and the Department of Home Affairs)
NSWCCL	New South Wales Council for Civil Liberties
Ombudsman	Commonwealth Ombudsman
Ombudsman Act	*Ombudsman Act 1976*
OAIC	Office of the Australian Information Commissioner
OIGIS	Office of the Inspector General of Intelligence and Security
ONI	Office of National Intelligence
PIA	Public Interest Advocate

PIM	Public Interest Monitor
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PJCLE	Parliamentary Joint Committee on Law Enforcement
PFA	Police Federation of Australia
PID	Public interest disclosure
PID Act	*Public Interest Disclosure Act 2013*
Privacy Act	*Privacy Act 1988*
QCCL	Queensland Council for Civil Liberties
Richardson Review	Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community
SD Act	*Surveillance Devices Act 2004*
SES	Senior Executive Service
TAR	Technical Assistance Request
The Bill	Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020
TIA Act	*Telecommunications (Interception and Access) Act 1979*
TOLA Act	*Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018*

List of Recommendations

Recommendation 1

6.21 The Committee recommends that, in line with the proposed expansion of the Inspector-General of Intelligence and Security's oversight role, the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 and, to the extent necessary, other legislation be amended to expand the oversight remit of the Parliamentary Joint Committee on Intelligence and Security to cover the intelligence functions of the ACIC (including, but not limited to, the use of network activity warrants by the ACIC).

Recommendation 2

6.26 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020) and, to the extent necessary, other legislation be amended to expand the oversight remit of the Parliamentary Joint Committee on Intelligence and Security to cover the intelligence functions of the AFP (including, but not limited to, the use of network activity warrants by the AFP).

Recommendation 3

6.29 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020) and, to the extent necessary, other legislation be amended to extend the oversight remit of the Inspector-General of Intelligence and Security's oversight to include all

intelligence functions of the AFP (including, but not limited to, not the use of just network activity warrants).

Recommendation 4

6.35 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 and, to the extent necessary, other legislation be amended to expand the inspection mandate and functions of the Commonwealth Ombudsman to cover – in explicit terms – the propriety of the AFP and ACIC's actions, practices, policies and activities under these new powers.

Recommendation 5

6.42 The Committee recommends that, where a Bill proposes to give operational or intelligence agencies specific new or expanded powers, those agencies should, in addition to providing input to any departmental submission, provide a separate unclassified submission to the Committee which should, at least, outline the necessity and proportionality of the proposed new or expanded powers. Such a submission should include, where appropriate, case studies on the current environment and how the use of any proposed new or expanded powers will assist the agency in the carrying out of its functions.

The Committee also recommends that the Department of Home Affairs not make any further submission to the Committee that purports to be authored by, or submitted on behalf of, the "Home Affairs Portfolio".

For the avoidance of doubt this recommendation should not preclude an agency providing a classified submission in addition to any unclassified submission.

Recommendation 6

6.48 The Committee recommends that, in support the proposed expansion of the Parliamentary Joint Committee on Intelligence and Security's oversight remit (see Recommendations 1 and 2), the AFP and the ACIC provide an unclassified annual report to the Committee which sets out:

- to the extent it is possible to do so in an unclassified report, similar information to what is required to be provided under section 3ZZVL of Schedule 3 of the Surveillance Legislation Amendment (Identify and

Disrupt) Bill 2020 (except that information should be provided in respect of all three of the new powers rather than just the account takeover warrants); and

- the offences in respect of which the warrants were sought or obtained.

This new reporting requirement should be supplemented by classified briefings to the Committee outlining the use of the new powers and their relationship both to each other and other existing powers provided to the AFP and ACIC.

Recommendation 7

6.50 The Committee recommends the INSLM Act be amended to provide for INSLM review of the data disruption, network activity and account takeover warrants introduced by the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 within three years of the Bill receiving Royal Assent.

The Committee further recommends that the INSLM Act be amended to require the INSLM to provide a copy of his or her report to the Committee at the same time the report is provided to the Minister.

Recommendation 8

6.55 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the Parliamentary Joint Committee on Intelligence and Security may conduct a review of the data disruption, network activity and account takeover warrants not less than four years from when the Bill receives Royal Assent to allow the Committee to take into account any report by the INSLM.

In addition the Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that each of the new powers sunset five years from the date on which the Bill receives Royal Assent.

Recommendation 9

6.58 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the issuing authority for all of the new powers introduced by the Bill, including emergency authorisations, must be a superior court judge (either of the Federal Court or

a State or Territory Supreme Court), except for Account Takeover Warrants which may be granted by an Eligible Judge per *Section 12 of the Surveillance Devices Act 2004* (Cth).

Recommendation 10

6.60 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to provide additional requirements on the considerations of the issuing authority to ensure the offences are reasonably serious and proportionality is maintained. The effect of any changes should be to strengthen the issuing criteria and ensure the powers are being used for the most serious of offending.

- This should include specific consideration as to whether the offending relates substantially to: offences against the security of the Commonwealth per Chapter 5 of the Criminal Code; offences against humanity including child exploitation and human trafficking per Chapter 8 of the Criminal Code; serious drug, weapons and criminal association offences per Chapter 9 of the Criminal Code; and money laundering and cybercrime offences per Chapter 10 of the Criminal Code. These examples are not exhaustive, but designed to reflect the intention of the Bill as seen through the Explanatory Memorandum and evidence to this Committee.

- This should include the nature of the offending and its relationship to other serious offences.

Recommendation 11

6.61 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the issuing authority, to the extent known, must consider the following:

- consideration to third parties specifically, including their privacy;

- specific consideration of privileged and journalistic information; and,

- specific consideration of privacy impacts, financial impacts, and the ability of individuals to provide or receive care.

Recommendation 12

6.71 The Committee recommends the Government commission a review of Commonwealth legislation to determine whether the concepts of "serious offence", "relevant offence" and other similar concepts:

- should be made consistent across different Acts of Parliament (noting that, for example, the definition of "serious offence" in the Telecommunications (Interception and Access) Act 1979 is different to the definition of "relevant offence" in the *Surveillance Devices Act 2004*; and

- whether the threshold for the concept of "serious offence" in all Commonwealth legislation should be – at a minimum – an indictable offence punishable by a maximum penalty of seven years' imprisonment or more, with a limited number of exceptions.

This body of work should inform the eventual electronic surveillance bill being considered by the Department of Home Affairs and other departments.

Recommendation 13

6.73 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that, in order to provide an emergency authorisation for disruption of data held in a computer:

- in addition to the matters set out in proposed section 28(1C) of the *Surveillance Devices Act 2004*, an authorising officer must be satisfied that that there are no alternative means available to prevent or minimise the imminent risk of serious violence to a person or substantial damage to property that are likely to be as effective as data disruption; and

- the authorising officer must consider the likely impacts of the proposed data disruption activity on third parties who are using, or are reliant on, the target computer and be satisfied that the likely impacts on third parties are proportionate to the objective of the emergency authorisation.

In addition, the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 should be amended so that, where an issuing authority declines to

retrospectively approve an emergency data disruption authorisation, the issuing authority may require the AFP or ACIC to take such remedial action as considered appropriate in the circumstances, including financial compensation.

Recommendation 14

6.77 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that any post-warrant concealment powers must be exercised within 28 days after the relevant warrant has expired unless the AFP or the ACIC (as applicable) has obtained the approval of a superior court judge to undertake post-concealment activities at a later date.

Consistent with the recommendation made by the INSLM, the superior court judge should be required to consider:

- how the AFP or the ACIC (as applicable) is proposing to conceal access;
- the likely privacy implications at the time and in the place where the concealment activity is proposed to occur; and
- whether, in all the circumstances, the concealment activity is appropriate.

In addition, and noting that the Committee did not receive evidence on concealment in relation to computer warrants, the Committee recommends that the Government consider whether the same amendment should be made in respect of computer access warrants in the *Surveillance Devices Act 2004* consistent with the recommendation made by the INSLM.

Recommendation 15

6.79 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that:

- for the purposes of proposed paragraphs 27KE(7)(b) and 27KE(12) (and any other relevant provision), a data disruption warrant may only authorise the AFP or ACIC to cause material loss or damage to other persons lawfully using a computer if the loss or damage is necessary to do one of the things specified in the warrant (i.e. it is not enough that the loss or damage is "justified and proportionate"); and

- the AFP and ACIC must notify the Commonwealth Ombudsman or IGIS (as appropriate) as soon as reasonably practicable if they cause any loss or damage to other persons lawfully using a computer.

The notification to the Commonwealth Ombudsman or IGIS (as applicable) must include, among other things, details of the loss or damage caused by the disruption activity and an explanation of why the loss or damage was necessary to do one of the things specified in the warrant.

Recommendation 16

6.80 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the power to temporarily remove computers and other things from premises under a data disruption warrant or a network activity warrant must be returned to the warrant premises as soon as it is reasonably practicable to do so.

Recommendation 17

6.82 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 should be amended to change the reporting requirements from the agencies to the Commonwealth Ombudsman from six-monthly to annually.

Recommendation 18

6.84 The Committee recommends that the Government introduce legislation to implement the Committee's recommendations in its report on press freedom as soon as possible.

In the meantime, the Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the issuing criteria for each of the proposed new powers requires the applicant, and the issuing authority, to consider the following matters in respect of any warrant that relates to – or may affect – a person working in a professional capacity as a journalist or a media organisation:

- the public interest in preserving the confidentiality of journalist sources; and

- the public interest in facilitating the exchange of information between journalists and members of the public to facilitate reporting of matters in the public interest.

Recommendation 19

6.85 Consistent with Recommendation 2 of the Committee's report on press freedom, the Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to require that – with respect to an application for a data disruption warrant, a network activity warrant or an account takeover warrant that is being sought in relation to a journalist or media organisation – a "public interest advocate" be appointed.

Recommendation 20

6.89 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to make clear the issuing criteria for an assistance orders also requires the issuing authority to be satisfied that:

- the order for assistance – and not just the disruption of data – is:
  - reasonably necessary to frustrate the commission of the offences that are covered by the disruption warrant; and
  - justifiable and proportionate, having regard to (i) the seriousness of the offences that are covered by the disruption warrant and (ii) the likely impacts of the data disruption activity on the person who is subject to the assistance order and any related parties (including, if relevant, the person's employer) and (iii) the likely impacts of the data disruption activity on other persons, including lawful computer users or clients of the person subject to the order; and
- compliance with the request is practicable and technically feasible (noting that these criteria are to be found in the industry assistance measures introduced by the Assistance and Access Act 2018).

Recommendation 21

6.91 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to require consideration by the

issuing authority, to the extent that is possible, of whether a person is, or has been, subject to other mandatory assistance orders (including mandatory assistance orders made under other Commonwealth legislation).

Having regard to the covert nature of mandatory assistance orders, and the fact that it may not be possible for the issuing authority or applicant to have knowledge of previous (or even concurrent) orders, the Committee further recommends that the Government develop a mechanism to ensure that individuals and companies are not subject to multiple mandatory assistance orders unless specific consideration is given to whether, in all of the circumstances, it is reasonably necessary and proportionate.

Recommendation 22

6.94 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to:

- impose a maximum period during with a non-emergency mandatory assistance order may be served and executed (and if the order is not served and executed within that period, the order will lapse and a new order must be sought);
- require all applications for a non-emergency mandatory assistance order to be made in writing;
- require all applications for a non-emergency mandatory assistance order to include, to the extent known key particulars, including the nature of the mandated assistance;
- prohibit the AFP and the ACIC, unless absolutely necessary, from seeking a non-emergency mandatory assistance order in respect of an individual employee of a company (i.e. assistance should only ever be sought from the company or business);
- set out the process that must be followed in respect of the service of a non-emergency mandatory assistance order on the specified persons, and link the commencement of an order to the date and time of service; and
- require that an issuing authority consider whether a person is, or has been subject, to a non-emergency mandatory assistance orders

(including mandatory assistance orders made under other Commonwealth legislation).

Recommendation 23

6.95 The Committee recommends that the Government make clear that no mandatory assistance order, including those defined in the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, can ever be executed in a manner that amounts to the detention of a person.

Recommendation 24

6.97 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to introduce good faith immunity provisions for both assisting entities and those employees or officers of assisting entities who are acting in good faith with an assistance order.

Recommendation 25

6.99 The Committee recommends the Explanatory Memorandum to the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to make it clear that decisions under the proposed new powers are not excluded from judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act).

For the avoidance of doubt, the Committee believes that no decision made in relation to data disruption warrants, network activity warrants and account takeover warrants should be exempt from judicial review under the ADJR Act.

Recommendation 26

6.101 The Committee recommends proposed paragraph 27KA(3)(b) of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to provide that the statement of facts and grounds accompanying all applications for data disruption warrants must specify the following matters to the extent that is possible:

- the acts or types of acts of data disruption that are proposed to be carried out under the warrant;
- the anticipated impacts of those specific acts or types of acts of disruption on the commission of the relevant offence (that is, how they are intended to frustrate that offence); and
- the likelihood that the relevant acts or types of acts of disruption will achieve that objective.

Recommendation 27

6.103 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that only individuals who satisfy the following requirements may apply for a data disruption warrant or an account takeover warrant:

- the person is a law enforcement officer in relation to the AFP or ACIC (as applicable) within the meaning of section 6A of the *Surveillance Devices Act 2004*;
- the person has been individually approved, by written instrument made by the AFP Commissioner or ACIC CEO (as applicable) to apply for data disruption warrants; and
- the relevant agency head is satisfied that the person possesses the requisite skills, knowledge and experience to make warrant applications, and the person has completed all current internal training requirements for making such applications.

Recommendation 28

6.104 The Committee recommends that paragraph 27KC of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that, rather than a judge having to be satisfied, that a data disruption warrant would be "justifiable and proportionate", the judge must be satisfied, to the extent possible at the time an application is made, that a data disruption warrant is:

- reasonably necessary to frustrate the commission of the offences referred to in the warrant application; and
- proportionate, having regard to:
  - the specific nature of the proposed disruption activities;
  - the proportionality of those activities to the suspected offending;
  - the potential adverse impacts of the disruption activities on non-suspects; and
  - the steps that are proposed to be taken to avoid or minimize those adverse impacts, and the prospects of those mitigating steps being successful.

Recommendation 29

6.106 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 and the IGIS Act be amended to make it clear that staff members of the Australian Signals Directorate are subject to IGIS oversight if they are seconded to the AFP or ACIC to execute a data disruption warrant for and on behalf of the AFP or ACIC.

Recommendation 30

6.109 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to strengthen the issuing authority considerations for network activity warrants, including by amending the definition of a "criminal network of individuals" to require there to be a reasonable suspicion of a connection between:

- the suspected conduct of the individual group member in committing an offence or facilitating the commission of an offence; and

- the actions or intentions of the group as a whole.

Recommendation 31

6.111 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to clarify that a decision-maker, and the issuing authority, must consider the privacy implications to the extent they are known, of a proposed network activity warrant.

To be clear, the committee does not believe that privacy considerations should be determinative in their own right, just that they should be considered.

Recommendation 32

6.113 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to require a sworn affidavit setting out the grounds of an application for an account takeover warrant (consistent with the delayed notification search warrants in the *Crimes Act*).

Recommendation 33

6.114 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to require an issuing authority to consider, to the extent that is possible at the time the application is made, whether a proposed account takeover warrant is likely to have an adverse impact on third parties, including a specific requirement to assess the likely:

- impacts on personal privacy;
- financial impacts on individuals and businesses;
- impacts on a person's ability to conduct their business or personal affairs; and
- impacts on a person's ability to have contact with family members or provide or receive care.

Recommendation 34

6.115 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be passed, subject to the amendments outlined above.

1. Introduction

1.1 The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill) was introduced into the House of Representatives by the Hon Peter Dutton MP, Minister for Home Affairs on 3 December 2020.

1.2 In his second reading speech Minister Dutton said:

> These key new powers are critical in enabling law enforcement to tackle the fundamental shift in how serious criminality is occurring online. Without enhancing the AFP and ACIC's powers, we leave them with out-dated ways of attacking an area of criminality that is only increasing in prevalence. This bill demonstrates the government's commitment to equipping the AFP and ACIC with modern powers that ensure serious criminality targeting Australians is identified and disrupted as resolutely in the online space as it is in the physical world.[1]

1.3 On 7 December 2020 the Minister for Home Affairs wrote to the Committee to refer the provisions of the Bill to the Committee for inquiry and report pursuant to section 29(b)(i) of the *Intelligence Services Act 2001* (the IS Act).

Conduct of the inquiry

1.4 The Committee resolved to undertake an inquiry into the Bill and details of the inquiry were uploaded to the Committee's website, www.aph.gov.au/pjcis, on 8 December 2020. Calls for submissions were announced the same day, with submissions requested by 12 February 2021.

---

[1] The Hon Peter Dutton MP, Minister for Home Affairs, *House of Representatives Hansard*, 3 December 2020, p. 9.

1.5 The Committee received 23 submissions and 9 supplementary submissions. A list of submissions received can be found at **Appendix A**.[2]

1.6 The Committee held a public hearing on 10 March 2021. A list of witnesses appearing at the hearing can be found at **Appendix B**.

1.7 Copies of submissions, the transcript from the public hearing and links to the Bill and Explanatory Memorandum, can be accessed at the Committee's website.

Report structure

1.8 In addition to this introductory chapter the report has five additional chapters being:

- Chapter 2 – General discussion and common issues;
- Chapter 3 – Data Disruption Warrants;
- Chapter 4 – Network Activity Warrants;
- Chapter 5 – Account Takeover Warrants; and
- Chapter 6 – Committee Comment

1.9 Chapter 2 will address issues common to all three warrant powers, whereas chapters three through five will discuss issues specific to each warrant type. From a Committee perspective there is substantial overlap legislatively and structurally between the three powers, and particularly so between the proposed network activity and data disruption warrants given they are proposed for the same act. This also reflects that many submissions discussed issues universal to the powers, with some addressing each proposed power specifically. For greater consistency the Committee has addressed uniform issues in chapter two.

1.10 Chapter 5 also discusses minor amendments, including to the Controlled Operations regime, proposed under this Bill that are distinct to the three new warrants outlined above.

---

[2] The submission provided by the Law Council of Australia was 165 pages with 57 recommendations. The Committee asked the Department of Home Affairs provide a supplementary submission addressing each of the Law Council's recommendations. As this report does not address each and every recommendation made by the Law Council interested parties may wish to see Law Council, *Submission 21*, and Department of Home Affairs, *Submission 9.1*.

Relationship with concurrent PJCIS inquiries and other Acts

1.11 The Bill most relevantly relates to the Committee's ongoing review of the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 (the IM Bill). Where this Bill focusses on equipping particular agencies with certain new powers, the IM Bill relates to oversight of multiple bodies including those proposed to receive the SLAID Bill powers more broadly. There are contingent measures built into both the SLAID and IM Bills to this point.

1.12 The IM Bill proposes to extend Inspector General of Intelligence and Security (IGIS) oversight to the Australian Criminal Intelligence Commission (ACIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC). Of note, the IM Bill proposes PJCIS oversight be extended to AUSTRAC and not the ACIC. The relevant provisions of the IM Bill are those that relate to the ACIC and AFP as the proposed recipients of new powers under the SLAID Bill.

1.13 These two Committee inquiries have been underway simultaneously and the Committee heard evidence from the IGIS who said their ability to provide oversight did not depend on one bill being passed first as the oversight provisions were included in both bills.[3]

1.14 Some submissions commented on the complex legislative landscape in which this Bill is a part of. The Digital Industry Group Inc (DIGI) said they were 'extremely concerned' that a number of *Telecommunications and Other Legislation Amendment Act 2018* (the TOLA Act) reviews were outstanding and recommended the Bill not proceed until the outstanding concerns under current reviews of the TOLA Act have been addressed. DIGI noted the Government had not yet responded to the Independent National Security Legislation Monitor's (INSLM) review of the TOLA Act and the PJCIS review of the Act had not been completed.[4]

1.15 The QCCL and others said it was not clear how these laws would interact with other proposed surveillance laws such as the Telecommunications

---

3 The Hon Dr Christopher Jessup QC, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 10 March 2021, p. 39.

4 DIGI, *Submission 20,* p. 1.

Legislation Amendment (International Production Orders) Bill 2020 (Cth) (the IPO Bill) which is also currently subject to review by this Committee.[5]

The threat environment and general requirement for new powers

1.16 The Australian Federal Police (AFP), Department of Home Affairs (Home Affairs) and ACIC set out to the Committee the current threat environment to provide context to the proposed powers as set out in the Bill. This context is universal across the three warrant types and will not be set out in full in later chapters which will focus more on the specific applicability of the particular proposed power to the threat context and its function within that context.

1.17 Home Affairs gave an overview of the threat environment, highlighting in particular the role of anonymising technologies and the dark web, two particularly relevant factors when considering the threat context:

> New and emerging technology continues to change the landscape in which criminals operate by providing new opportunities for countering law enforcement efforts, in particular by disguising activity and hiding identities. Technology that enables people to be anonymous online, whilst having legitimate uses, is increasingly used by criminals so that they can remain invisible to law enforcement. Often these technologies are cheap, commercially available and require little technical expertise, allowing the scale and sophistication of cyber-enabled crime to grow. The use of the dark web and anonymising technologies (such as bespoke encrypted devices) has made it easier than ever before for criminals to commit serious crimes at volume and across multiple jurisdictions. This has significantly degraded law enforcement agencies' ability to access communications, gather evidence, prevent crimes and conduct investigations.[6]

1.18 The AFP provided an in depth description of the threat environment/ Their submission covered anonymising and encrypted technologies, criminal activity on the dark web, and the subsequent impact on child protection investigations. The AFP also discussed the prevalent use of dedicated encrypted communications platforms by serious and organised crime groups. The AFP defined key terms as follows:

---

5 QCCL et al., *Submission 4*, p. 7.

6 Department of Home Affairs, *Submission 9*, p. 5.

> Increasing criminal use of the dark web and anonymising technology facilitates a wide array of serious, cyber-enabled crime, while creating significant challenges for law enforcement in identifying and locating offenders, and gathering admissible evidence.
>
> Firstly, the terms 'dark web' and 'anonymising technology' are not synonymous. 'Anonymising technology' refers to those technologies which can disguise a person's activities, location and true identity, while the 'dark web' refers to areas of the internet which cannot be accessed without specialised browsers or other software. These concepts are often linked, because anonymising technology is required to access the dark web.
>
> From the AFP perspective, both issues present significant challenges for law enforcement, as they both facilitate a wide variety of criminal activity, while providing offenders with the cloak of anonymity. The intersection of these issues is particularly concerning when investigating offences involving child abuse material.[7]

1.19 The ACIC broadly concurred with the AFP articulation of the threat environment and said:

> Criminals are increasingly using the dark web and dedicated encrypted communication platforms to facilitate and undertake a wide range of serious crimes, including money laundering, illicit drug and firearms smuggling, and the production and dissemination of child exploitation material.[8]

1.20 The ACIC said the electronic surveillance powers currently available to the ACIC were not sophisticated enough to identify and disrupt the totality of activities serious and organised crime entities were undertaking using these technologies. ACIC said the powers provided under the TOLA Act were required and important, but not solely sufficient to address this threat environment.[9] The ACIC said:

> More is needed to provide the ACIC and AFP with effective powers to combat the rising tide of cyber-enabled crime.[10]

1.21 The ACIC said the place of this Bill would be to complement the ACIC's existing powers by providing new avenues to gather information and

---

7 Australian Federal Police, *Submission 6*, p. 5.

8 Australian Criminal Intelligence Commission (ACIC), *Submission 23*, p. 1.

9 ACIC, *Submission 23*, p. 1.

10 ACIC, *Submission 23*, p. 1.

respond to serious crime occurring online and criminals using dedicated encrypted communication platforms.[11] They said all the new powers would be used to develop understanding and gathering intelligence on serious and organised crime entities using these technologies to cover their activities.[12]

1.22 The Carly Ryan Foundation also set out the threat environment:

> The investigation of alleged crimes is not immune to technological creep, and law enforcement are increasingly dealing with digital aspects of criminality amongst many crime types: terrorism, domestic violence, stalking and harassment, and importantly for the Foundation, child exploitation. Units that specialise in online and cybercrime are best placed in understanding what tools they require to keep the Australian community safe. [13]

1.23 The Carly Ryan Foundation said the current amount of child exploitation was absolutely extraordinary and had risen with COVID-19. They described the issue as a pandemic and said the proposed Bill would help prevent the further victimisation of children.[14]

Organised crime use of dedicated encrypted communications

1.24 The AFP said intersection of encryption and anonymising technology was most evident in Dedicated Encrypted Communications Platforms (DECPs) which were designed for, and marketed to, organised criminals as tools to avoid law enforcement detection.[15]

1.25 The AFP said organised criminal networks were increasingly using DECPs to facilitate a wide variety of serious offending. They said DECPs were modified handsets that had ordinary functions removed allowing for bespoke encrypted applications to ensure anonymous contact between handsets. Providing a practical example outlining the relationship between this Bill and the TOLA Act, the AFP said the TOLA Act was able to identify how many DECPs were present in Australia but not who is using them or where they were being used. This Bill would assist the AFP in this latter question.[16]

---

11 ACIC, *Submission 23*, p. 2.

12 ACIC, *Submission 23*, p. 3.

13 Carly Ryan Foundation, Submission 1, p. 2.

14 Ms Sonya Ryan, Carly Ryan Foundation, *Committee Hansard*, Canberra, 10 March 2021, p. 15.

15 Australian Federal Police, *Submission 6.1*, p. 4.

16 Australian Federal Police, *Submission 6.1*, p. 4.

1.26 The AFP said internationally DECP networks had been taken down and some DECP providers had provided information on law enforcement evasion to their users.[17]

1.27 The ACIC concurred with the comments made by the AFP and said the dark web and encrypted communications had allowed serious and organised crime groups to more effectively conceal their criminal activity.[18]

The Bill

1.28 The following section gives a brief overview of the Bill as described in the Explanatory Memorandum (EM). A more detailed discussion of the powers proposed in the Bill will be given in Chapters 2 – 5.

1.29 The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 will amend the *Surveillance Devices Act 2004* (the SD Act), the *Crimes Act 1914* (the Crimes Act) and associated legislation to introduce new powers for law enforcement agencies that the Government state will 'enhance the ability of the AFP and the ACIC to combat online serious crime.'[19] It has specifically been designed for the most serious crimes. Of note, these are powers for law enforcement agencies rather than necessarily law enforcement powers themselves. The relevance of this point will be discussed later.

1.30 The Bill introduces three new powers for the AFP and the ACIC exclusively. They are:

- Data disruption warrants (DDWs) to enable the AFP and the ACIC to disrupt data by modifying, adding, copying or deleting in order to frustrate the commission of serious offences online;
- Network activity warrants (NAWs) to allow agencies to collect intelligence on serious criminal activity being conducted by criminal networks; and
- Account takeover warrants (ATWs) to provide the AFP and the ACIC with the ability to take control of a person's online account for the purposes of gathering evidence to further a criminal investigation.

17 Australian Federal Police, *Submission 6.1*, p. 5.

18 ACIC, *Submission 23*, p. 1.

19 Explanatory Memorandum, p. 2.

Schedule 1 – Data disruption warrants

1.31 Schedule 1 amends the SD Act to introduce DDWs. These warrants will allow the AFP and the ACIC to disrupt criminal activity that is being facilitated or conducted online by using computer access techniques.

1.32 A DDW will allow the AFP and the ACIC to add, copy, delete or alter data to allow access to and disruption of relevant data in the course of an investigation for the purposes of frustrating the commission of an offence. This will be a covert power also permitting the concealment of those activities. Whilst this power will not be sought for the purposes of evidence gathering, information collected in the course of executing a data disruption warrant will be available to be used in evidence in a prosecution.

1.33 The intended purpose of the DDW is to offer an alternative action to the AFP and the ACIC, where the usual circumstances of investigation leading to prosecution are not necessarily the option guaranteeing the most effective outcome. For example, removing content or altering access to content (such as child exploitation material), could prevent the continuation of criminal activity by participants, and be the safest and most expedient option where those participants are in unknown locations or acting under anonymous or false identities. Under these circumstances, it may be prudent for the AFP or the ACIC to obtain a data disruption warrant.

1.34 Applications for DDWs must be made to an eligible Judge or nominated Administrative Appeals Tribunal (AAT) member. A DDW may be sought by a law enforcement officer of the AFP or the ACIC if that officer suspects on reasonable grounds that:

- one or more relevant offences are being, are about to be, or are likely to be, committed, and
- those offences involve, or are likely to involve, data held in a computer, and
- disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more of the relevant offences previously specified that involve, or are likely to involve, data held in the target computer.

1.35 An eligible Judge or nominated AAT member may issue a DDW if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant and the disruption of data authorised by the warrant is justifiable and proportionate, having regard to the offences specified in the application. The issuing authority will consider, amongst other things, the

nature and gravity of the conduct targeted and the existence of any alternative means of frustrating the commission of the offences.

1.36 Information obtained under DDWs will be 'protected information' under the SD Act and be subject to strict limits for use and disclosure. Consistent with existing warrants in the SD Act, compliance with the DDW regime will be overseen by the Commonwealth Ombudsman.

Schedule 2 – Network activity warrants

1.37 Network activity warrants will allow the AFP and the ACIC to collect intelligence on criminal networks operating online by permitting access to the devices and networks used to facilitate criminal activity.

1.38 These warrants will be used to target criminal networks about which very little is known, for example where the AFP or the ACIC know that there is a group of persons using a particular online service or other electronic platform to carry out criminal activity but the details of that activity are unknown. NAWs will allow agencies to target the activities of criminal networks to discover the scope of criminal offending and the identities of the people involved. For example, a group of people accessing a website hosting child exploitation material and making that material available for downloading or streaming, will be able to be targeted under a network activity warrant.

1.39 Intelligence collection under a NAW will allow the AFP and the ACIC to more easily identify those hiding behind anonymising technologies. This will support more targeted investigative powers being deployed, such as computer access warrants, interception warrants or search warrants.

1.40 Network activity warrants will allow the AFP and the ACIC to access data in computers used, or likely to be used, by a criminal network over the life of the warrant. This means that data does not have to be stored on the devices, but can be temporarily linked, stored, or transited through them. This will ensure data that is unknown or unknowable at the time the warrant is issued can be discovered, including data held on devices that have disconnected from the network once the criminal activity has been carried out (for example, a person who disconnected from a website after downloading child exploitation material).

1.41 The AFP and the ACIC will be authorised to add, copy, delete or alter data if necessary to access the relevant data to overcome security features like encryption. Data that is subject to some form of electronic protection may

need to be copied and analysed before its relevancy or irrelevancy can be determined.

1.42 Applications for network activity warrants must be made to an eligible Judge or nominated AAT member. A NAWmay be sought by the chief officer of the AFP or the ACIC (or a delegated Senior Executive Service (SES) member of the agency) if there are reasonable grounds for suspecting that:

- a group of individuals are engaging in or facilitating criminal activity constituting the commission of one or more relevant offences, and
- access to data held in computers will substantially assist in the collection of intelligence about those criminal networks of individuals in respect of a matter that is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

1.43 There are strict prohibitions on the use of information obtained under a NAW. Information obtained under a NAW is for intelligence only, and will not be permitted to be used in evidence in criminal proceedings, other than for a breach of the secrecy provisions of the SD Act. Network activity warrant information may, however, be the subject of derivative use, allowing it to be cited in an affidavit on application for another investigatory power, such as a computer access warrant or telecommunications interception warrant. This will assist agencies in deploying more sensitive capabilities, with confidence that they would not be admissible in court.

1.44 The Inspector-General of Intelligence and Security (IGIS) will have oversight responsibility for NAWs given their nature as an intelligence collection tool. This approach departs from the traditional model of oversight by the Commonwealth Ombudsman of the use of electronic surveillance powers by the AFP and the ACIC. However, the approach is consistent with the oversight arrangements for intelligence collection powers available to other agencies, including the Australian Security Intelligence Organisation (ASIO) and the Australian Signals Directorate (ASD).

1.45 The Bill also provides that the IGIS and the Commonwealth Ombudsman will be able to share information where it is relevant to exercising powers, or performing functions or duties, as an IGIS or Ombudsman official. This ensures that where a matter may arise during an inspection that would more appropriately be dealt with by the other oversight body, a framework is in place for the transfer of NAW information, allowing efficient and comprehensive oversight to occur.

Schedule 3 – Account takeover warrants

1.46 The Bill inserts account takeover warrants into the Crimes Act. These warrants will enable the AFP and the ACIC to take control of a person's online account for the purposes of gathering evidence about serious offences.

1.47 Currently, agencies can only take over a person's account with the person's consent. An account takeover power will facilitate covert and forced takeovers to add to their investigative powers.

1.48 An AFP or ACIC officer may apply to a magistrate for an ATW to take control of an online account, and prevent the person's continued access to that account. Before issuing the ATW, the magistrate will need to be satisfied that there are reasonable grounds for suspicion that account takeover is necessary for the purpose of enabling evidence to be obtained of a serious Commonwealth offence or a serious State offence that has a federal aspect. In making this determination, the nature and extent of the suspected criminal activity must justify the conduct of the account takeover.

1.49 This power enables the action of taking control of the person's account and locking the person out of the account. Any other activities, such as accessing data on the account, gathering evidence, or performing undercover activities such as taking on a false identity, must be performed under a separate warrant or authorisation. Those actions are not authorised by an account takeover warrant. The ATW is designed to support existing powers, such as computer access and controlled operations, and is not designed to be used in isolation.

1.50 The Bill will require the agencies to make six-monthly reports to the Commonwealth Ombudsman and the Minister for Home Affairs on the use of account takeover warrants during that period. There are also annual reports to the Minister for Home Affairs that are required to be tabled in Parliament.

Schedule 4: Controlled operations

1.51 Schedule 4 will introduce minor amendments to Part IAB of the Crimes Act to enhance the AFP and the ACIC's ability to conduct controlled operations online.

1.52 In particular, the Bill amends the requirement for illicit goods, including content such as child abuse material, to be under the control of the AFP and the ACIC at the conclusion of an online controlled operation.

1.53 This is intended to address how easy data is to copy and disseminate, and the limited guarantee that all illegal content will be able to be under the control of the AFP and the ACIC at the conclusion of an online controlled operation.

Schedule 5: Minor corrections

1.54 Schedule 5 will make minor technical corrections to the SD Act and the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

2. General discussion and common issues

2.1 The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill) proposes the introduction of two new warrants into the *Surveillance Devices Act 2004* (the SD Act) and one new warrant into the *Crimes Act 1914* (the Crimes Act). This section of the report addresses issues universal, or near-universal to the three proposed powers despite the warrants themselves having specific differences and belonging to different Acts. Where chapter three to five will address warrant-specific issues, this chapter addresses issues common across the warrant types and broader issues.

2.2 This chapter will discuss the necessity and proportionality of the powers, the offences to which they apply, the assistance order framework, oversight and review of the powers. These are all issues considered by the Committee to be overarching matters across the proposed warrants rather than power-specific issues.

A new type of power

2.3 The Law Council said the Bill represented a change in focus for the Australian Federal Police (AFP) and Australian Criminal Intelligence Commission (ACIC), saying:

> The bill proposes major and, respectfully, novel expansions of the existing powers of the AFP and ACIC, which merit detailed scrutiny. The new powers

> depart sharply from the traditional focus of investigative powers on the collection of admissible evidence of specific offences.[1]

2.4 The AFP however said prosecution and criminal action was only one function of the AFP itself with the Commissioner telling the Committee:

> I want to emphasise that disrupting crime is a core business for the AFP. There is a misconception that disrupting crimes means that an investigation will never proceed to prosecution. This is simply not true. Many of our disruption efforts still result in the prosecution of offenders.
>
> The best example of this is our unrelenting efforts in covering illegal drugs imported to Australia. We can simply seize the drugs at the border and arrest an offender or two, if we identify them at that point, but we can also take a different approach to disrupt the harmful effects of drugs in our community. We seek to discover who sent the drugs, who bought them and their distribution points. We take law enforcement action at an appropriate time, but we also disrupt the immediate impact of drugs entering our community, identify a larger number of offenders and have a better chance of reducing future harm.
>
> But, in the online environment, we're far more restricted in how we can track illegal activities in this way. We can assume an identity and interact with offenders. We can get targeted warrants to intercept their communications and access their data, and, with the TOLA industry assistance framework, we can get help to open the front door. But we've still got one hand tied behind our back because we cannot identify what their distribution point is and what criminal network they belong to; understand what they are communicating, due to encryption; move things around inside their network – that is, modify data – or take control of their distributors to collect evidence. And, in many cases, we may not even know where the distribution network is. [2]

2.5 The AFP additionally said:

> Criminals should not be able to conduct serious crimes online and get away with it just because our laws have not kept pace with changes in technology.[3]

2.6 From an administrative and resourcing perspective Telstra said the powers were new and a 'significant change' to existing carrier and internet service

---

1 Dr Jacoba Brasch QC, President, Law Council of Australia (Law Council), *Committee Hansard*, Canberra, 10 March 2021, p. 2.

2 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 47.

3 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 48.

provider (ISP) warrant processes and capabilities which would require the development of new warrant management processes to enable carriers and ISPs to provide assistance in executing the warrants.[4]

2.7 Twitter noted this Bill placed the new powers across two existing acts and commented on the consequences of this. Twitter said data disruption warrants (DDWs) and network activity warrants (NAWs) amended the SD Act whereas account takeover warrants (ATWs) amended the Crimes Act. Twitter said this led to divergent approaches to accountability, issuing authorities, and extraterritorial application causing 'inconsistent and irreconcilable standards'.[5] Home Affairs said this was to maintain conformity with existing powers and they deliberately considered where each power should be placed in existing acts.[6]

2.8 The powers were described as extraordinary by the Law Council because:

> They go further than collecting evidence for prosecution into a realm where they are actively doing things to that data, either by way of preventing access or by destroying it, which would include destroying other peoples' property, their computers and so on, so that's a big next step. It's extraordinary in this other way because of the operation of computers. Computers now do everything for us. They are so directly involved in all of our personal, business and other lives that there's a vast field of information there available for people to collect if they're authorised to do that.[7]

2.9 The Digital Industry Group Incorporated (DIGI) said the Bill should be viewed as an extension of the *Telecommunications and Other Legislation Amendment Act* (the TOLA Act) because the Bill 'provides law enforcement with greatly expanded powers that increases the incentive to use the tools available to them under the TOLA Act.[8] DIGI said the Bill was inexplicably linked with the TOLA Act as a service provider could be required to provide the same assistance under an Assistance Order from this Bill and a Technical Assistance Notice under the TOLA Act. DIGI said assistance requested under the Bill would not receive the same protections and processes built

---

4 Telstra, *Submission 16*, p. 2.

5 Twitter, *Submission 11*, p. 4.

6 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs (Home Affairs), *Committee Hansard*, Canberra, 10 March 2021, p. 50.

7 Dr David Neal SC, Co-Chair National Criminal Law Committee, Law Council, *Committee Hansard*, Canberra, 10 March 2021, p. 10.

8 DIGI, *Submission 20,* p. 1.

into the TOLA Act. DIGI recommended the Government make clear the intended relationship between this Bill and the TOLA Act.[9]

Necessity and proportionality of the powers

2.10 Several submissions discussed both the necessity and proportionality of these powers, which were often characterised as extraordinary and novel. It was generally accepted that these powers were new and there was a requirement for the AFP and ACIC to address the threats identified above. There was then substantial debate as to whether these powers were an appropriate means of addressing the threat landscape.

2.11 The Australian Information Industry Association (AIIA) said:

> The AIIA supports the intent behind this legislation that seeks to disrupt and frustrate the commission of serious offences online. The AIIA joins with other industry groups in urging the government to ensure that the guardrails and thresholds associated with this legislation are managed appropriately and that the government considers no only the civil liberty implications of the Bill but also the feasibility and implications of assistance and compliance for the technology sector on both an individual and global level.[10]

2.12 It was from this starting point that the debate moved to whether the powers were necessary and proportional in terms of the Bill itself. More specifically, the Law Council said there were two components to necessity. Firstly whether the powers themselves were necessary compared to existing powers, and secondly the necessity for a particular warrant in particular circumstances for a particular case. It was the general argument of the Law Council that necessity was not present in this Bill.[11]

2.13 The Law Council said the necessity of the proposed powers had not been clearly or adequately established as a threshold issue.[12] The Law Council said they were concerned the proposed scope of the new powers was disproportionately broad compared to the threats of serious and organised

---

9 DIGI, *Submission 20,* p. 4.

10 Australian Information Industry Association (AIIA), *Submission 17*, p. 1.

11 Dr David Neal SC, Co-Chair National Criminal Law Committee, Law Council, *Committee Hansard*, Canberra, 10 March 2021, p. 10.

12 Law Council of Australia, *Submission 21*, p. 9.

cybercrime to which they are directed.[13] In relation to child exploitation and terrorism offences the Law Council said:

> That really is at the heart of the cautious approach that we're adopting towards this. We can see, in some instances, such as child pornography and probably terrorism offences, just to take the two cases that are signalled the whole issue of the necessity of this and the proportionality of it is much clearer because of the seriousness of the offences.[14]

2.14 Home Affairs said the tradecraft of criminals had evolved alongside communications technology. They said the growing use of the dark web and anonymising technologies was hampering investigations into serious crimes and existing electronic surveillance powers did not allow agencies to fully engage in the fight against serious crimes. They said:

> Investigations into online criminality must adapt if our agencies are to continue to do the job we expect of them – keeping Australians safe.[15]

2.15 The Human Rights Law Centre (HRLC) made the following observation of surveillance powers such as these:

> Surveillance powers intrude on individual privacy, have a chilling effect on the exercise of political rights and disproportionately impact marginalised and vulnerable communities. Each time further surveillance powers are contemplated, this committee and other oversight bodies should ask whether the proposed powers are (a) strictly necessary, (b) carefully contained and (c) fully justified. We believe that the bill in its present shape does not satisfy those criteria.[16]

2.16 The Law Council made an observation that was shared amongst many submissions, that law enforcement agencies needed powers that were adapted to the specialised context of cyber-enabled offences, but the necessity and proportionality of these powers required careful scrutiny.[17] The Law Council said:

---

13 Law Council of Australia, *Submission 21*, p. 10.

14 Dr Jacoba Brasch QC, President, Law Council, *Committee Hansard*, Canberra, 10 March 2021, p. 4.

15 Ms Cath Patterson, Deputy Secretary (Strategy and Law Enforcement), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 46.

16 Mr Kieran Pender, Senior Lawyer, Human Rights Law Centre (HRLC), *Committee Hansard*, Canberra, 10 March 2021, p. 1.

17 Law Council of Australia , *Submission 21*, p. 9.

> We're also concerned that the new powers are disproportionately broad compared to the threats of serious and organised cybercrime to which they are directed.[18]

2.17 There was substantial debate between submissions as to the necessity and proportionality of the powers. The Cyber Security Cooperative Research Centre (CSCRC) said the extraordinary powers were proportionate and appropriate to the threat.[19] The NSW Council for Civil Liberties (NSWCCL) discussed the 'cumulative effect of repeated widening of the powers of law enforcement and spy agencies to monitor Australians.'[20] DIGI said they believed the Bill did not adhere to the principles of proportionality or necessity.[21] The HRLC said:

> The explanatory memorandum and commentary by the minister indicate that the powers are intended to only be used in cases of the most severe wrongdoing, yet the bill doesn't reflect that.[22]

2.18 The Uniting Church in Australia Synod of Victoria and Tasmania (the Uniting Church) said surveillance and covert operations by law enforcement agencies against severe crimes were already permitted in the offline world and were an essential tool in law enforcement agencies' ability to curb serious organised crime.[23] The Uniting Church said:

> It is the view of the Synod that the Commonwealth Government would not be honouring its human rights obligations under the treaties it is party to if it were to give ultimate priority to the right to privacy of those suspected of committing serious human rights abuses and crimes to the point of undermining the ability of law enforcement agencies to be able to effectively prevent such abuses and crimes.[24]

2.19 The Uniting Church further said:

> We are increasingly seeing people using technology and being provided with technology tools to defeat law enforcement. Some of those providers are

---

18 Dr Jacoba Brasch QC, President, Law Council, *Committee Hansard*, Canberra, 10 March 2021, p. 2.

19 Cyber Security Cooperative Research Centre (CSCRC), *Submission 14*, p. 3.

20 NSWCCL, *Submission 3*, p. 5.

21 Digital Industry Group Inc (DIGI), *Submission 20,* p. 2.

22 Mr Kieran Pender, Senior Lawyer HRLC, *Committee Hansard*, Canberra, 10 March 2021, p. 2.

23 The Uniting Church in Australia (Synod of Victoria and Tasmania) (Uniting Church), *Submission 13*, p. 5.

24 Uniting Church, *Submission 13*, p. 9.

> wilfully engaging helping to defeat law enforcement efforts. So there is a need to look at powers that allow law enforcement to protect the basic human rights of Australians – and hopefully collaborate more globally to protect the human rights of others, because, when an Australian is using a live webcam to abuse a child in the Philippines, that's something we should be actively trying to stop.[25]

2.20 The Cyber Security Cooperative Research Centre (CSCRC) said:

> We are now at a critical point where we as a society need to decide what kind of world we want to live in. Central to this must be the notion that all crime, whether committed online or offline, should be treated the same and the rule of law must be applied equally. If passed, this legislation will play a key role in countering serious cyber-enabled crime…While the powers contained within the bill are undoubtedly extraordinary they are proportionate and appropriate in relation to the scale and seriousness of the threat posed.[26]

2.21 The CSCRC further outlined the requirement of the powers, noting 'as it stands bad has the upper hand. The criminals are the ones with power'.[27]

2.22 Some submissions questioned the requirement for the powers all together with the New South Wales Council for Civil Liberties saying 'it is far from clear there is any shortcoming with existing powers that creates the need for additional powers'.[28] The NSWCCL said given ATWs in particular were intended to support existing powers that it would indicate ATWs were not justified when weighed against 'potential pitfalls'.[29]

2.23 The Office of the Australian Information Commissioner (OAIC) said the powers were 'wide-ranging and coercive in nature'.[30] Specifically the OAIC said:

> These powers may adversely impact the privacy of a large number of individuals, including individuals not suspected of involvement in criminal activity, and must therefore be subject to a careful and critical assessment of their necessity, reasonableness and proportionately. Further, given the privacy

---

25 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church in Australia (Synod of Victoria and Tasmania) (Uniting Church), *Committee Hansard*, Canberra, 10 March 2021, p. 15.

26 Ms Rachael Falk, CEO, Cyber Security Cooperative Research Centre (CSCRC), *Committee Hansard*, Canberra, 10 March 2021, p. 22.

27 Ms Rachael Falk, CEO, CSCRC, *Committee Hansard*, Canberra, 10 March 2021, p. 22.

28 New South Wales Council for Civil Liberties (NSWCCL), *Submission 3*, p. 4.

29 NSWCCL, *Submission 3*, p. 5.

30 Office of the Australian Information Commissioner (OAIC), *Submission 19*, p. 2.

> impact of these law enforcement powers on a broad range of individuals and networks, they should be accompanied by appropriate privacy safeguards. The OAIC considers that the Bill requires further consideration to better ensure that any adverse effects on the privacy of individuals which result from these coercive powers are minimised, and that additional privacy protections are included in the primary legislation.[31]

2.24 The Queensland Council for Civil Liberties, Liberty Victoria, Electronic Frontiers Australia and the Australian Privacy Foundation (QCCL et al.) said the Bill provides similar power to that introduced by the TOLA Act.[32]

2.25 The Law Council recommended amending the Bill to introduce a sunset clause of three years and a PJCIS statutory review of the powers prior to the sunset date.

Human rights and journalist concerns

2.26 The QCCL and others said they did not believe Australia had an adequate federal human rights framework and if the Bill came into effect that Australians did not have sufficient safeguards of their fundamental rights to protect them from abuse of power by authorities.[33] The HRLC said the absence of a 'robust human rights framework' meant they could not endorse the expansion of AFP and ACIC powers to include these warrants.[34]

2.27 Home Affairs said there was an error in the explanatory memorandum (EM) regarding human rights compatibility and the human rights compatibility statement would be amended accordingly.[35]

2.28 Mr Paul Templeton said there were no provisions in the Bill for journalists which could damage the person and their reputation which would affect their career.[36]

2.29 Home Affairs said DDWs, NAWs and ATWs apply 'equally to all individuals, including lawyers and journalists, noting that the powers can only be used where rigorous legislative thresholds are met'. Home Affairs

---

31 OAIC, *Submission 19*, pp. 2-3.

32 Queensland Council for Civil Liberties, Liberty Victoria, Electronic Frontiers Australia and the Australian Privacy Foundation (QCCL et al.), *Submission 4*, p. 2.

33 QCCL et al., *Submission 4*, p. 2.

34 HRLC, *Submission 15*, p. 4.

35 Department of Home Affairs, *Submission 9*, p. 23.

36 Mr Paul Templeton, *Submission 1*, p. 1.

additionally noted all three powers did not override the principle of client-legal privilege.[37]

Applicable offences

2.30 All three new powers apply to 'relevant offences'. For ATWs this is at proposed section 3ZZUJ, for NAWs this is at proposed section 27KK(1)(b)(ii), and for DDWs this is at proposed section 27KA(1)(a) of the Bill.

2.31 While NAWs and DDWs are proposed to be included in the SD Act and ATWs are proposed to be included in the Crimes Act, the definition of relevant offence within each is substantively the same and as such is addressed as a universal issue across the three powers. The definition for NAWs and DDWs, by virtue of being in the SD Act, is slightly broader than ATWs in the Crimes Act. The definitions of relevant offence across the three new proposed powers are defined and clarified in **Appendix C** (Relevant Offences) which shows the relationship between this Bill and existing acts.

2.32 It is worth highlighting the definition of 'relevant offence' is already categorised in existing legislation, namely the Crimes Act and the SD Act and what this Bill proposes is to extend those existing categories to the new powers rather than defining or creating a new term. For an ATW a relevant offence is a serious Commonwealth offence or a serious State offence that has a federal aspect. For DDWs and NAWs a relevant offence is the above, as well as several other offences listed in section 6 (Definitions) of the SD Act.

2.33 Home Affairs said the definition of relevant offence was not static and would expand when Parliament enacts new offences that meet the three-year threshold, or increased the maximum penalty for an existing offence. They said:

> Given the speed with which technology and digital crimes are evolving, listing specific Commonwealth and State and Territory offences as 'relevant offences' would require frequent legislative amendment and would cause the threshold to be out of data as State and Territory legislative changes are made.[38]

2.34 While the EM clearly articulated the purpose of these powers to be towards the most serious of offending, as many submissions noted the definition of

---

[37] Department of Home Affairs, *Submission 9.1*, p. 31.

[38] Department of Home Affairs, *Submission 9.1*, p. 6.

'relevant offence' is significantly more broad than just the offences listed in the EM as being the focus for these powers. This issue of relevant offences was perhaps one of the most substantial for this inquiry, with many submissions arguing that the category was too broad and encompassed too many minor offences.

2.35 The Committee heard evidence that debated what a serious offence was, evidence about how minor offences are an important strategy for law enforcement dismantling of serious organised crime, and evidence for legislative coherence and consistency. In simple terms the oft-repeated argument from Government was that these new powers would be placed within the existing warrant frameworks with common definitions to ensure legislative consistency. The equally commonly repeated argument from industry and other groups was that these powers were extraordinary and therefore the existing categories were not appropriate.

2.36 The AFP said the relevant offences definition meant the powers could only be used for offences under investigation that carried a penalty of three years' imprisonment or more.[39] The NSWCCL also said the warrants would apply to any Commonwealth offence with a maximum term of imprisonment of three years or more. NSWCCL however said:

> This is an extraordinary catch-all, encompassing fauna importation, fraud, and importantly, such vaguely worded offences as 'communication and other dealings with inherently harmful information by current and former Commonwealth officers' under sections 121 and 122 of the Criminal Code.[40]

2.37 The NSWCCL recommended ATWs in particular be restricted to specific offences such as child sexual abuse, terrorism, and trafficking of drugs and firearms and the application of ATWs to any Commonwealth offence with a maximum term of imprisonment of three years or more be removed.[41]

2.38 The QCCL and others said the Bill would operate in contexts other than just national security by section 3ZZUK of the amendment which defines 'relevant offence' as a serious Commonwealth offence or a serious State offence that has a federal aspect.[42] QCCL and others said this included

---

39 AFP, *Submission 6*, pp. 17-18.

40 New South Wales Council for Civil Liberties (NSWCCL), *Submission 3*, p. 4.

41 NSWCCL, *Submission 3*, p. 6.

42 QCCL et al, *Submission 4*, p. 3.

numerous offences and provided an exhaustive summary of applicable offences.[43]

2.39 The Uniting Church noted the AFP would be unlikely to target minor offences due to their own resourcing constraints:

> Either you take the view that law enforcement agencies will appropriately target their resources – so even though you can cite all these offences that are more minor and take the view that law enforcement will waste resources chasing them instead of more serious offending – or you trust them to use it more actively in well-targeted means.[44]

Division by category of offending

2.40 Several submissions discussed the idea of amending the Bill and the de facto definition of relevant offence in the Bill to encompass certain offence types or categories. The practical effect of this amendment would be not to draw the definition of relevant offence from the Crimes Act or SD Act but to establish a new category of offences specifically for the purposes of these powers.

2.41 The Law Council recommended eligible offences should be: limited specifically to match the stated policy intent of targeting criminality of the most serious and harmful kind; and prescribed exhaustively in primary legislation so that the addition of further kinds of offences is subject to specific Parliamentary approval.[45]

2.42 The Law Council said these offences should be: indictable, punishable by a maximum penalty equivalent to the threshold for telecommunications interception warrants pursuant to section 5D(2)(a) of the *Telecommunications (Interception and Access) Act* (the TIA Act) (according to the Law Council being seven years' imprisonment or more); and the offence covers certain subject-matter. The subject-matter required would be: offences against the security of the Commonwealth per Chapter 5 of the Criminal Code; offences against humanity and related offences in Chapter 8 of the Criminal Code (including child exploitation and human trafficking); and possibly certain offences in Chapter 9 of the Criminal Code (including serious drug, weapons and criminal association offences) and possibly certain offences in Chapter

---

43 QCCL et al., *Submission 4*, pp. 3-4 citing section 15GE(2) of the *Crimes Act*.

44 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, Canberra, 10 March 2021, p. 16.

45 Law Council of Australia, *Submission 21*, pp. 46-47.

10 of the Criminal Code (including certain money laundering and cybercrime offences).[46]

2.43 QCCL and others additionally recommended the definition of 'relevant offence' be re-defined to include an exhaustive list of specific serious offences.[47] The CSCRC recommended the Bill specify types of crime to which the Bill applies. CSCRC said this would 'allay fears of misuse of the warrants for less serious crimes and perceptions of legislative creep'.[48] The CSCRC suggested the inclusion of classes of offences that are defined for the powers but noted there could be technical drafting issues that presented in doing so.[49]

2.44 When asked about their preference of either limiting relevant offences to a category of offences or an imprisonment term, the Law Council said their preference would be to have both. The HRLC said whilst they also preferred a category and minimum term classification, if they had to decide between the two they would preference relevant offences being a category of offences.[50]

2.45 Home Affairs said the danger of carving out particular offences would be the risk of missing things.[51] The Uniting Church additionally said:

> The danger with drafting really tightly is there might be very serious human rights abuses and harms occurring to people and wider concerns that then go unaddressed – offending that basically isn't tackled because the police lack the powers to gather the evidence eventually and to even understand what is going on.[52]

2.46 Countering these issues directly the AFP said limiting the powers to specific listed offences was 'not workable'. They noted the importance of the three-year threshold for online offences in particular, saying:

---

46 Law Council of Australia, *Submission 21*, p. 47.

47 QCCL et al., *Submission 4*, p. 7.

48 CSCRC, *Submission 14*, p. 8.

49 Ms Rachael Falk, CEO, CSCRC, *Committee Hansard*, Canberra, 10 March 2021, p. 23.

50 Dr Jacoba Brasch QC, President, Law Council and Mr Kieran Pender, Senior Lawyer, HRLC, *Committee Hansard*, Canberra, 10 March 2021, p. 7.

51 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskfroce), Department of Home Affairs, *Committee Hansard*, 10 March 2021, p. 49.

52 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, Canberra, 10 March 2021, p. 19.

> A three-year threshold ensures we can investigate all relevant telecommunications and computer offences in the Criminal Code where the majority of offending will be facilitated using computer networks and where evidence will be held in computers.[53]

2.47 The AFP provided the example of outlaw motorcycle gangs where as part of the dismantling process the AFP could disrupt offences within their logistics or administration arms such as importing drugs or money laundering. The AFP said the purpose in these instances would be to 'attack the outer perimeter of these organised crime networks' which would allow the AFP to dismantle these networks.[54] Furthermore, the AFP said:

> We're looking at organised crime and organised crime is not focused on one particular form of criminality; we're looking at polycrime. The syndicates we are investigating now are involved in a range of criminality and we need flexibility in the legislation to apply that legislation to those types of groups.[55]

2.48 The Uniting Church said determining what a serious offence was and what offences these powers should be applied to was a debatable exercise. They provided the example of illegal logging which could have a severe impact on a community in a developing nation but was subject to a relatively minor penalty in Australia.[56] The Uniting Church said:

> Trying to list all the crimes that the new warrants should cover would be a massive undertaking, as it would require a review of all laws and an assessment of which would be considered to cover serious criminal conduct.[57]

2.49 Home Affairs said the debate over what a serious offence was had already been answered by Parliament in existing legislation. They said:

> We have then added additional safeguards to say that it is not enough to go and get a warrant because it is three years; it has to be of such nature and

---

53 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 49.

54 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 52.

55 Mr Ian McCartney, Deputy Commissioner (Investigations), AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 50.

56 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, Canberra, 10 March 2021, p. 16.

57 Uniting Church, *Submission 13.1*, p. 2.

> gravity in terms of the conduct constituting those offences that that information can be sought.[58]

2.50 The AFP said issues of seriousness would be taken into account by the issuing officer for the powers as outlined by Home Affairs in their evidence to the Committee.[59]

Division by minimum term of imprisonment

2.51 Several submissions discussed or debated the prospect of amending the definition of 'relevant offence' to in effect raise the minimum term of imprisonment from three years to a higher threshold. There was not an agreed upon higher threshold with several submissions proposing different minimum terms of imprisonment. Again, this would have the effect of creating a new category and definition of relevant offences specific to these three particular warrants.

2.52 The HRLC said they did not put a number of years on what they thought would be improved proportionality because they believed it was a more holistic analysis. The HRLC said:

> You could imagine a much stricter bill that still had a three-year threshold or you could imagine a bill with a higher threshold that retained other dimensions of it. We would say there are multiple levers that can be used together to improve the proportionality.[60]

2.53 Fastmail said these warrants were no less intrusive than the TIA Act and the criteria for application of their powers should be similar. Fastmail said to obtain data under the SD Act the offence needed to have a minimum penalty of two to three years whereas under the TIA Act the minimum penalty required was seven years. Fastmail said 'specifying severity by length of penalty is in keeping with past acts and creates clarity for law enforcement and the judicial system'. [61]

2.54 Home Affairs said raising the offence threshold to an offence punishable by a maximum penalty equivalent of seven years or more was inappropriate.

---

58 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 52.

59 Mr Ian McCartney, Deputy Commissioner (Investigations), AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 50.

60 Mr Kieran Pender, Senior Lawyer, HRLC, *Committee Hansard*, Canberra, 10 March 2021, p. 3.

61 Fastmail Pty Ltd (Fastmail), *Submission 10*, p. 2.

They said it would result in a number of serious offences not being captured by the warrants and provided several examples of offences that would not be covered such as: using a carriage service to menace, harass or cause offence; associating with a terrorist organisation; failing to report child sexual abuse offences; and conduct by Commonwealth officers causing harm to Australian interests.[62]

2.55 Home Affairs quoted the Comprehensive Review of the Legal Framework of the National Intelligence Community (the Richardson Review) which noted that raising the offence threshold for electronic surveillance warrants to apply to seven-year offences would have 'no particular principled basis, and would amount to simply adopting a 'highest common denominator' approach'.[63]

2.56 Where Home Affairs used one part of the Richardson Review to support their argument, they noted another part that was in contradiction with the current Bill. They noted the Richardson Review recommended raising offence thresholds for electronic surveillance powers to five years which would be 'out of step' with the current electronic surveillance framework. Home Affairs said they were currently considering how to implement these recommendations from the Richardson Review.[64]

2.57 The Communications Alliance recommended the threshold for the offence be raised to 'serious offence' in line with the offence threshold of the TIA Act.[65] The TIA Act defines a serious offence at section 5D. Telstra also recommended the threshold be raised to 'serious offence'.[66] DIGI noted the Independent National Security Legislation Monitor (INSLM) had previously recommended the offence threshold in the TOLA Act be raised to 'serious offence' in line with the TIA Act.[67]

2.58 Home Affairs said it was a misnomer to equate a seven year threshold with the TIA Act as there were a range of exceptions that included three and five

62 Department of Home Affairs, *Submission 9.1*, p. 7.

63 Department of Home Affairs, *Submission 9.1*, p. 7.

64 Department of Home Affairs, *Submission 9.1*, p. 7.

65 Communications Alliance, *Submission 12*, p. 3.

66 Telstra, *Submission 16*, p. 2.

67 DIGI, *Submission 20,* p. 2.

year offences.[68] The Uniting Church said raising the threshold to seven years was inappropriate:

> You basically say people who are stupid and not technically savvy will get caught because they won't know how to use tools in the online world that would conceal the harm they're causing and those who are tech savvy will escape.[69]

2.59 The AFP said they needed operational flexibility as would be provided by the three-year offence threshold. They said:

> There are offences even at the three-year level that we believe would be of potential relevance, including the offence of associating with a terrorist organisation, which is a three-year offence.[70]

2.60 The HRLC recommended the Bill be amended to increase the maximum term of imprisonment specified in the definition of 'relevant offence'. HRLC said this would ensure the warrants were only available where their use would be proportionate to the severity of the alleged offence. [71] The HRLC said the Bill would apply to a range of offences which were 'wholly unrelated to the purpose of the Bill stated in the Explanatory Memorandum'.[72] QCCL said they did not accept the warrants should be applied to the existing definition of a 'serious commonwealth offence'.[73]

2.61 After many submissions presented the general argument that three year offences could be lesser or less serious offences Home Affairs said it was a subjective test to determine whether an offence was serious:

> Objectively, parliament has set that threshold at three years, and, in our view, there must be some correlation to the seriousness of those offences.[74]

---

68 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 49.

69 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, Canberra, 10 March 2021, p. 16.

70 Mr Ian McCartney, Deputy Commissioner (Investigations), AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 49.

71 HRLC, *Submission 15*, p. 6.

72 HRLC, *Submission 15*, p. 8.

73 QCCL et al, *Submission 4*, p. 4.

74 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 49.

2.62 Home Affairs provided context for the definition of relevant offence, noting:

> Each power has been designed to align with the legislative framework in which it sits, and, as much as possible, to align with other powers that agencies are likely to use in conjunction with these new warrants.[75]

2.63 The Uniting Church said they would be concerned if the definition of relevant offence was raised to a higher minimum term of imprisonment. They provided the example of tax evasion and wage theft through 'phoenixing' that could have a massive impact on individuals. They said a person dealing with several million dollars' worth of proceeds of crime has a three year penalty and would not be included if the definition was altered.[76]

2.64 The Uniting Church said if the threshold was increased then it could 'cut off' investigation into offences like the negligent laundering of any amount of proceeds of crime. They noted under the current Bill anyway the AFP and ACIC would not be able to apply for these powers for the offence of negligently laundering less than $50,000.[77]

2.65 The Uniting Church noted several offences were often linked and provided the example of a money laundering offence which may tie to other more serious human rights abuses. They said it was important to consider the context in which the offence operated.[78] The Carly Ryan Foundation said:

> Various different crimes are often linked. So where there may be child abuse involved, there may be other offences that are layered upon that child abuse. I think three years is adequate.[79]

2.66 The Uniting Church noted the United Nations Convention against Transnational Organised Crime defined serious crime as any offence of four years and above.[80]

2.67 The Uniting Church said:

---

75 Department of Home Affairs, *Submission 9.1*, p. 6.

76 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, Canberra, 10 March 2021, p. 16.

77 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Submission 13.1*, p. 3.

78 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, Canberra, 10 March 2021, p. 16.

79 Ms Sonya Ryan, CEO, Carly Ryan Foundation, *Committee Hansard*, Canberra, 10 March 2021, p. 16.

80 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, Canberra, 10 March 2021, p. 15.

> If the Committee recommends an increase in the threshold it could cut off the ability of the warrants to be used in cases to investigate abuse of public office.[81]

2.68 The Uniting Church said:

> The Synod remains of the view that the warrants in the Bill should be available for offences that carry a maximum term of imprisonment of three years or more, in order to allow the AFP and ACIC flexibility in the pursuit of serious criminal activity. It is reasonable for the Committee to trust the AFP and ACIC will use the powers in the Bill to target serious crime, and not for lesser crimes that are unrelated to serious criminal conduct. Even if the AFP or ACIC attempted, on a rare occasion, to obtain a warrant for a lesser criminal matter there are still the safeguards in the Bill that the authorising judge, AAT member or magistrate (depending on the warrant) would need to be satisfied that the application met all the criteria outlined in the Bill.[82]

Assistance orders

2.69 The Committee considered assistance orders as part of this inquiry. These are orders issued to an entity or person to assist in the execution of the warrants proposed under this Bill and were a significant part of the Committee's previous inquiry into the TOLA Act. These assistance orders can be directed at the subject of the warrant, or a person that can assist with gaining access to the account.

2.70 Home Affairs said assistance orders already exist in relation to computer access warrants. Home Affairs said the assistance order mechanism under this Bill was not intended to allow law enforcement to compel assistance from the technology industry but rather from a person with relevant knowledge of a particular online account (such as a person who uses an online account). Home Affairs said:

> Orders requiring assistance already exist in relation to computer access warrants. This mechanism is not intended to allow law enforcement to compel assistance from the technology industry, but rather from a person with relevant knowledge of a particular computer or computer system, or online account in the case of account takeover warrants, to the investigation or operation (such as a person who uses a computer or online account).[83]

---

81 Uniting Church, *Submission 13.1*, p. 3.

82 Uniting Church, *Submission 13.1*, p. 2.

83 Department of Home Affairs, *Submission 9*, p. 23.

2.71 While near-universal across the three powers, this following section will briefly identify where assistance orders are found in the various proposed powers under the Bill before turning to general commentary across the proposed powers.

Data Disruption Warrants

2.72 Proposed section 64B will allow a law enforcement officer of the AFP or the ACIC to apply to an eligible Judge or nominated AAT member for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to access and disrupt data held in a computer subject to a data disruption warrant.

Network Activity Warrant

2.73 Proposed subsection 64(6A) sets out the matters to which an eligible Judge or nominated AAT member must be satisfied of in order to grant an assistance order in relation to a network activity warrant. The Judge or AAT member must be satisfied that there are reasonable grounds for suspecting that access to data held in the computer will substantially assist in the collection of intelligence in relation to criminal networks of individuals. The issuing authority must also be satisfied that there are reasonable grounds for suspecting that access to data held in the computer will substantially assist in the collection of intelligence that is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

2.74 The Explanatory Memorandum states:

> Although the SD Act provides for the issuing of warrants permitting covert activity, there may be circumstances in the course of an operation where a person who is not the suspect or target of the warrant will have knowledge of a computer system and be able to provide access to relevant data, without compromising the covert nature of the operation. Alternatively, there may be a point in the operation where the benefits of compelling information from a person in order to enable access to data outweigh the disadvantages of maintaining the secrecy of the operation.[84]

Account Takeover Warrants

2.75 Proposed section 3ZZVG provides that if an account takeover warrant or emergency authorisation is in force, a law enforcement officer may apply to a magistrate for an assistance order requiring a specified person to provide

---

84 Explanatory Memorandum, p. 56.

any information or assistance that is reasonable and necessary to allow the law enforcement officer to take control of an online account that is the subject of the warrant or authorisation.

2.76 Existing section 3LA of the Crimes Act allows a constable to make an application to a magistrate for an order requiring certain persons (such as owners or users of a device) to provide any information or assistance to allow law enforcement to access data held in, or accessible from, a computer that has been seized, moved or found in the course of a section 3E search warrant. For example, a section 3LA order may be used to compel a person to provide their password to assist law enforcement in obtaining access to data held in a computer found or seized under a search warrant.

2.77 Proposed new subsection 3LA(7) provides for the additional use of information or assistance provided as a result of an order made under section 3LA. Information or assistance provided under section 3LA for an investigation into an alleged offence under a search warrant may be used in the execution of an account takeover warrant that relates to that same investigation. The EM states:

> The inclusion of this provision overrides the principle that information obtained under a power conferred by statute can only be used or disclosed for the purpose for which it was obtained. In the case of a section 3LA assistance order, this would be for the purposes of executing a search warrant under section 3E. The intent of this amendment is to ensure that information obtained under a section 3LA assistance order can be used in the execution of an account takeover warrant. Account takeover warrants are designed to complement the use of other investigatory powers, including search warrants, to authorise the taking control of a person's online account in the investigation of serious offences.[85]

General comment on assistance orders

2.78 The Law Council recommended including in the issuing criteria the requirement to consider whether the person is, or has been, the subject of any previous mandatory assistance orders under multiple regimes.[86] This was, according to the Law Council, likely to prevent 'forum-shopping'.

2.79 The Law Council noted the existence of similar powers and said existing powers to obtain mandatory assistance orders in respect of computer access

---

85 Explanatory Memorandum, p. 137.

86 Law Council of Australia, *Submission 21*, p. 26.

warrants can require third parties render assistance in gaining access to data and making it available to law enforcement agencies. They said existing technical assistance requests or technical assistance notices can require the provision of technical assistance or capability.[87]

2.80 The Law Council recommended including an explicit requirement for all mandatory assistance orders to specify material particulars, including the date or time period over which the assistance must be rendered and the nature of the relevant assistance. The Law Council was concerned at the potential breadth of assistance orders as the Bill was currently drafted. [88]

2.81 In response to this point Home Affairs said assistance orders were not standalone orders but could be given in support of an underlying warrant. They said the period for which assistance could be compelled under an assistance order could not extend beyond the scope of the underlying warrant.[89]

2.82 Home Affairs said a key safeguard in the Bill as it related to assistance orders was the requirement for the assistance to be reasonable and necessary which would preclude the use of an assistant order to compel a person to give assistance on an ongoing or repetitive basis.[90]

2.83 QCCL and others said the proposed section 3ZZVG assistance orders were similar to the Technical Assistance Requests (TARs) contained in the TOLA Act and questioned why additional powers would be required.[91]

2.84 QCCL and others said there were no provisions for situations where the provision of assistance would constitute a beach of confidence or the relevant omission which underlies the offence arises as a consequence of a warrant that is inadequately or unclearly drafted. The QCCL and others recommended assistance orders be removed from the Bill.[92]

2.85 Communications Alliance (CA) said a conflict could arise where assistance orders were directed at an individual employee or officers rather than the business user or the platform corporation. CA said the conflict could be

---

87 Law Council of Australia, *Submission 21*, pp. 142-143.

88 Law Council of Australia, *Submission 21*, p. 26.

89 Department of Home Affairs, *Submission 9.1*, p. 24.

90 Department of Home Affairs, *Submission 9.1*, p. 24.

91 QCCL et al., *Submission 4*, p. 5.

92 QCCL et al., *Submission 4*, p. 8.

between the order and the employee's work responsibilities or terms of employment. CA recommended the Bill address these issues by requiring that the technology provider organisation be the target of assistance orders and where an individual is compelled to provide assistance providing and paying for independent legal advice.[93]

2.86 DIGI said there was no reference in the EM on the impact of the Bill on service providers. DIGI said they understood the intention of the powers to be that warrants and assistance orders did not apply at the service provider level but because of the broad drafting of the Bill it was likely to directly impact service providers.[94]

Good faith immunity provisions

2.87 The AIIA recommended the Bill be amended to introduce immunity from prosecution for both assisting entities and those employees or officers of assisting entities who are acting in good faith with an assistance order. The AIIA noted the government introduced section 30BE in the critical infrastructure reform process and a similar provision should be introduced into this Bill. [95] The critical infrastructure provision was cited by the AIIA to be:

> 1 An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith […]
>
> 2 An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1).[96]

2.88 AIIA said the imposition of 600 penalty units of 10 years' imprisonment was disproportionate, especially in the absence of appropriate good faith immunity provisions.[97]

Cost recovery, processes and damages

2.89 The AIIA recommended introducing provisions in the proposed legislation for cost recovery for private entities in relation to the costs they incur in

---

93 Communications Alliance, *Submission 12*, p. 4.

94 DIGI, *Submission 20,* p. 3.

95 AIIA, *Submission 17*, p. 2.

96 AIIA, *Submission 17*, p. 2.

97 AIIA, *Submission 17*, p. 4.

implementing assistance orders. They recommended the provision be enlivened where there is a:

> significant loss or extraordinary cost to the assisting entity, whether in repairing vulnerability, restoring service, addressing a human resources burden, or intensive technical impact incurred by the company in complying with an assistance order.[98]

2.90 Fastmail recommended the inclusion of a requirement in the Bill that incidental harm or loss be avoided or fully compensated, and/or an express right of compensation for all losses (not just property and personal injury) from the warrants. Fastmail said this would ensure companies knew the impact of their compliance could be recognised.[99]

Conflict with international laws

2.91 Twitter said compliance by service providers with assistance orders would directly conflict with obligations under laws of other countries where they operate. Twitter provided the example of the United States *Stored Communications Act* which prohibited service providers providing information absent appropriate *Electronic Communications Privacy Act* legal process. [100]

2.92 AWS said they were concerned employees might be ordered to do an act under an assistance order which may breach foreign law. AWS said it would be appropriate to make clear in the Bill that any such requirement would be unreasonable or provide a defence for an individual who refuses to do the act. Amazon Web Services recommended an appropriate defence would involve the introduction of a modified version of proposed section 317ZB(5) of the TIA Act in respect to the laws of foreign countries.[101]

Technical feasibility considerations of assistance orders

2.93 Several submissions called for mandatory consultation with industry as part of the assistance order regime (in addition to separate calls for mandatory consultation with industry for the powers themselves). The arguments in favour of technical consultation for assistance orders and warrant execution itself were often similar and sometimes blended.

---

98 AIIA, *Submission 17*, p. 2.

99 Fastmail, *Submission 10*, p. 2.

100 Twitter, *Submission 11*, p. 8.

101 Amazon Web Services, *Submission 8*, p. 4.

2.94 Amazon Web Services recommended considerations be introduced into the Bill for determining whether assistance notices from industry were reasonable and proportionate. AWS said this would be similar to that provided in the TOLA Act. AWS recommended these considerations include technical feasibility considerations so as not to allow 'technical fishing expeditions that put at risk third parties'.[102]

2.95 Amazon Web Services recommended the Bill be amended to include a specific prohibition against ATWs being executed in a manner that would require a person to implement or build a systemic weakness into a form of electronic protection or prevent a person from rectifying a systemic weakness in a form of electronic protection.[103]

2.96 The AIIA recommended the government include listed factors that decision-makers have to consider in determining whether industry assistance notices were reasonable and proportionate, including the security of relevant systems and technical feasibility. The AIIA recommended this occur at, for example, proposed section 3ZZUP of the Bill. They recommended an amendment to include factors informed by a holistic awareness of the systems involved, including the security of the relevant systems and technical feasibility. The AIIA said in 2018, due to industry concern, the government included in the TOLA Act provisions that listed certain factors decision-makers had to consider in determining whether the industry assistance notice were reasonable and proportionate. [104]

2.97 Amazon Web Services said the Bill did not provide sufficient protection for individual employees of technology providers and created an assistance regime different from the TOLA Act. AWS recommended the Bill be amended to make clear that where assistance is sought from an individual the assistance request should be both reasonable and proportionate using the criteria specified in the TOLA Act.[105]

2.98 Twitter said they did not store credentials in plaintext form which could make adherence to assistance orders not technically feasible.[106]

---

102 Amazon Web Services, *Submission 8,* pp. 2-3.

103 Amazon Web Services, *Submission 8*, p. 3.

104 AIIA, *Submission 17*, p. 2.

105 Amazon Web Services, *Submission 8*, p. 3.

106 Twitter, *Submission 11*, p. 8.

Clarification of 'specified person' and their duties

2.99 The AIIA recommended the Government clarify the term 'specified person' in SD Act proposed sections 64A and 64B(1) (for NAWs and DDWs) and Crimes Act proposed section 3ZZVG (for ATWs). The AIIA queried how these proposed sections would impact the ability for law enforcement to compel 'specified persons' to provide reasonable information and assistance to help them carry out a warrant. The AIIA requested additional clarification of the roles and responsibilities of a 'specified person' and specifically what 'provid[ing] any information or assistance that is reasonable and necessary' could constitute in the context of what law enforcement could compel a 'specified person' to do.[107]

2.100 The HRLC said the assistance order powers accompanying the ATWs would require the 'specified person' assist law enforcement. They said this could be the person suspected of committing the offence or a person who is, or was, a system administrator for the system including the computer or the electronic service to which the account relates (among others). The HRLC said the ability for law enforcement to compel individuals to answer questions or provide assistance that could expose them to legal ramifications would contradict the right to freedom from self-incrimination. The HRLC said there was a significant divergence from the EM to the Bill itself in this regard.[108]

2.101 The HRLC said it was possible the assistance orders could compel an individual to assist law enforcement to obtain evidence which was against their legal interest. The HRLC recommended the Bill be amended to ensure adequate safeguards for the freedom against self-incrimination.[109] The HRLC recommended a more narrowly worded provision to limit the assistance order to 'only information or assistance that is strictly necessary for the execution of the underlying warrant'.[110]

2.102 Twitter said it was unclear from the Bill and EM whether the Bill would require service providers and their relevant employees to comply with assistance orders. Twitter said this was due to the definition of 'specified person' under proposed section 3ZZVG, subsections (b)(vi) and (c).[111]

---

107 AIIA, *Submission 17*, p. 3.

108 HRLC, *Submission 15*, pp. 12-13.

109 HRLC, *Submission 15*, p. 6.

110 HRLC, *Submission 15*, p. 13.

111 Twitter, *Submission 11*, p. 8.

2.103 DIGI said there were issues with the scope of assistance orders. They said the pool of 'specified persons' for the purposes of these assistance orders was 'extremely broad' and could include service providers and their employees. DIGI said there was no reference in the EM to these orders being designed or intended for application to service providers or their employees and recommended this be clarified in the Bill.[112] Mr Paul Templeton said there were no legal provisions or pathway for a person compelled to provide assistance under the assistance order.[113]

Oversight

2.104 Oversight of these powers diverges in some respects but in others is universal. This section of the report addresses evidence received by the Committee that is universal, or near-universal, to the powers. Specific oversight commentary on particular powers will be addressed in later chapters.

2.105 The Bill provides that the IGIS and the Commonwealth Ombudsman (the Ombudsman) will be able to share information where it is relevant to exercising powers, or performing functions or duties, as an IGIS or Ombudsman official. This ensures that where a matter may arise during an inspection that would more appropriately be dealt with by the other oversight body, a framework is in place for the transfer of network activity warrant information, allowing efficient and comprehensive oversight to occur.

Data Disruption Warrants

2.106 Information obtained under DDWs will be 'protected information' under the SD Act and be subject to strict limits for use and disclosure. Consistent with existing warrants in the SD Act, compliance with the DDW regime will be overseen by the Commonwealth Ombudsman.

Network Activity Warrants

2.107 The IGIS will have oversight responsibility for NAWs given their nature as an intelligence collection tool. This approach departs from the traditional model of oversight by the Commonwealth Ombudsman of the use of electronic surveillance powers by the AFP and the ACIC. However, the

112 DIGI, *Submission 20,* p. 3.

113 Mr Paul Templeton, *Submission 1*, p. 1.

approach is consistent with the oversight arrangements for intelligence collection powers available to other agencies, including the Australian Security Intelligence Organisation (ASIO) and the Australian Signals Directorate (ASD).

2.108 The SD Act currently requires the chief officers of ACIC and AFP to make a report to the Minister as soon as practicable after a warrant issued under the Act ceases to be in force. Section 50 of the SD Act also contains requirements for certain information to be included in ACIC's and AFP's annual reports, including the number of applications made for warrants under the Act, the number of warrants issued or refused and the number of extensions applied for and granted and refused. These existing reporting requirements would extend to network activity warrants.

2.109 The IGIS said:

> the Bill proposes specific reporting requirements in relation to network activity warrants. Proposed subsection 49(2E) provides that reports to Ministers must contain specific information about a warrant including, but not limited to, the name (if known) of any person whose data was accessed, the extent to which the execution of the warrant assisted the agency in carrying out its functions and details of the compliance with the conditions (if any) stipulated in the warrant.
>
> The Bill also contains record keeping requirements, including provisions governing the destruction of records obtained by accessing data under a network activity warrant. Proposed section 46AA specifies that the chief officers of ACIC and AFP must ensure that every record or report relating to network activity warrant information is kept in a secure place, and destroyed within specified timeframes.22 Consistent with its current practice in reviewing other intelligence warrants, IGIS would inspect these records on a regular basis.[114]

Account Takeover Warrants

2.110 Oversight for ATWs is provided at proposed Division 7 (Inspections) and Division 6 (Reporting and record keeping). For ATWs this is in the form of the Commonwealth Ombudsman exclusively and not the Inspector General of Intelligence and Security (IGIS).

2.111 The Bill provides for Chief Officers' 6 monthly reports to the Minister and the Ombudsman at proposed section 3ZZVL. This requires the chief officer

---

114 IGIS, *Submission 18*, p. 8.

of the AFP or ACIC to set out the number of ATW applications made during the previous six months, the number of ATWs issued during the previous six months, the number of ATW variations issued during the previous six months, and the number of emergency authorisations of ATWs issued during the previous six months, amongst other things. The Bill also provides for Chief Officers' annual reports to the Minister at proposed section 3ZZVM.

2.112 The Bill provides for oversight by the Commonwealth Ombudsman at proposed Division 7. The Ombudsman said the Bill proposed extending the Ombudsman's oversight role within the Crimes Act to include the ATWs.[115] The AFP said Ombudsman oversight of ATWs was consistent with existing reporting requirements.[116]

2.113 The Ombudsman said the Bill imposed six-monthly inspection and six-monthly reporting obligations to the Ombudsman. The Ombudsman said this did not align with the requirements for other Crimes Act regimes they oversee. The Ombudsman recommended the inspection and reporting requirements for the ATW regime is aligned with the 12-monthly inspection and reporting obligations of the controlled operations regime in Part IAB of the Crimes Act. The Ombudsman said this would better reflect the likely operational intersection between ATWs and controlled operations, and provide the Ombudsman with more flexibility and discretion in managing their oversight functions.[117]

2.114 The IGIS said while the Ombudsman would have oversight of ATWs, the Ombudsman could communicate information obtained in the course of its oversight of these powers to IGIS officials for the purposes of IGIS officials exercising powers, or performing functions or duties as such.[118]

2.115 The Law Council recommended extending the reporting and record-keeping requirements to mandatory assistance orders under proposed section 3ZZVG.[119]

2.116 The Law Council recommended requiring the AFP and ACIC notify the Ombudsman if they cause loss or damage to a third-party, either in

---

115 Commonwealth Ombudsman, *Submission 5*, p. 3.

116 AFP, *Submission 6*, p. 18.

117 Commonwealth Ombudsman, *Submission 5*, p. 5.

118 IGIS, *Submission 18*, p. 6.

119 Law Council of Australia, *Submission 21*, p. 150.

contravention of the limits of the authority of the warrant or pursuant to proposed section 3ZZUR(8)(a) of the Bill.[120]

2.117 Home Affairs said additional notification to the Ombudsman of loss or damage was unnecessary.[121]

General comment on oversight

2.118 The IGIS said the Australian Signals Directorate (ASD) may have a role in providing technical assistance to the ACIC and AFP under the DDW and ATW frameworks, and this assistance would fall under ASD's existing functions and would not be an expansion of ASD's legislated powers. The IGIS said they would oversee conduct undertaken by ASD in rendering technical assistance to ACIC and AFP in the execution of a warrant under the Bill.[122]

2.119 The Law Council recommended increasing funding for the Ombudsman to enable the effective oversight of the new powers. The Law Council said this funding would be intended to enable the Ombudsman to have an appropriate number of security-cleared staff to perform inspection, investigatory and complaints handlings functions; have appropriate security infrastructure for the highest national security classification that is likely to be generated under the new powers; and access independent technical expertise to enable effective oversight of the powers.[123]

2.120 The Law Council recommended expanding the Ombudsman's inspection functions. The Law Council said this expansion should be similar to section 8 of the IGIS Act and cover: agencies' compliance with applicable policies and procedures, as well as legislation; the propriety of agencies' actions, practices and policies under the new powers; and the compatibility of agencies' actions with Australia's international human rights obligations.[124]

2.121 The Law Council recommended conferring a broader inspection function on the Ombudsman to consider the propriety, as well as legal compliance, of

120 Law Council of Australia, *Submission 21*, p. 150.

121 Home Affairs, *Submission 9.1*, p. 31.

122 IGIS, *Submission 18*, p. 6.

123 Law Council of Australia, *Submission 21*, p. 19.

124 Law Council of Australia, *Submission 21*, p. 19.

the activities of the AFP and ACIC under those warrants to be equivalent to the IGIS.[125]

2.122 The Carly Ryan Foundation said they believed the Bill included appropriate oversight and accountability of the powers.[126] The CSCRC said the safeguards were sufficient.[127] Fastmail however said there was a requirement for increased oversight and accountability.[128] The NSWCCL said 'Inspector-Generals and Ombudsman offices are not empowered to be a real counter-weight to law enforcement. The abuse of power this Bill enables will happen, as it already has under other laws NSWCCL has opposed'.[129]

INSLM and PJCIS

2.123 The Law Council said neither the INSLM nor Parliamentary Joint Committee on Intelligence and Security (PJCIS) would have comprehensive oversight of the new powers and recommended amending the *Independent National Security Legislation Monitor Act 2010* (the INSLM Act) and *Intelligence Services Act* (the IS Act) to make provision for full oversight by both the INSLM and PJCIS of all three new warrant regimes in the Bill.[130]

2.124 Home Affairs said neither the Committee nor the INSLM should be specifically empowered to oversee the new warrants proposed by this Bill in an operational sense.[131]

2.125 These issues were discussed at greater detail in the submissions received by the Committee for the Review of the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 (the IM Bill).

Judicial and merits review

2.126 QCCL and others said the Bill expressly precluded judicial or merits review of the decision to issue warrants at paragraph 44 of the Explanatory

---

125 Law Council of Australia, *Submission 21*, p. 150.

126 Carly Ryan Foundation, *Submission 2*, p. 2.

127 CSCRC, *Submission 14*, p. 8.

128 Fastmail, *Submission 10*, p. 1.

129 NSWCCL, *Submission 3*, p. 4.

130 Law Council of Australia, *Submission 21*, p. 158.

131 Department of Home Affairs, *Submission 9.1*, p. 33.

Memorandum to the Bill.[132] Home Affairs said this was an error in the EM and these decisions would be subject to judicial (but not merits) review.[133]

2.127 Twitter said the Bill was unclear regarding the standards of review and means of appeal available to service providers.[134] DIGI said there should be an opportunity for service providers to challenge the issuance of both the warrants and the assistance orders. DIGI said this would be for situations where the service provider objected to the warrant or particular elements of it. DIGI recommended the Bill be amended in this regard to provide additional guidance on:

> 1 The grounds on which a provider can object to the issuance of a warrant or an assistance (e.g. conflict of laws or technical inability);
>
> 2 To whom a provider should address an objection;
>
> 3 The body that would be charged with independently reviewing the objection;
>
> 4 The timeframe for objections;
>
> 5 The legal status of providers after an objection has been lodged;
>
> 6 An indication of the assessment criteria for how such objections will be approved or denied.[135]

Parliamentary privilege

2.128 For each warrant the Bill provides that it does not affect the law relating to the powers, privileges and immunities of any of the following:

- (a) each House of the Parliament;
- (b) the members of each House of the Parliament;
- (c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.[136]

---

132 QCCL et al, *Submission 4*, p. 3.

133 Department of Home Affairs, *Submission 9*, p. 23.

134 Twitter, *Submission 11*, p. 7.

135 DIGI, *Submission 20*, p. 6.

136 The Bill, proposed section 27KJ and 27KT amending the SDA and proposed section 3ZZUW amending the Crimes Act.

3. Data Disruption Warrants

3.1 As described in Chapter One data disruption warrants (DDW) will allow the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to disrupt criminal activity that is being facilitated or conducted online by using computer access techniques.

3.2 Following the setting out of some general comment this chapter will set out in more detail the following:

- Applications for DDW
  - Who may apply for a DDW
  - Determining the application
  - What an application must contain
- What a data disruption warrant authorises
- Extension, variation and revocation of a data disruption warrant
- Revocation and discontinuance of access and disruption under warrant
- Emergency authorisation
- Extraterritoriality

General comment on data disruption warrants

3.3 The Department of Home Affairs (Home Affairs) characterised the data disruption power as follows:

> The power to disrupt data under a data disruption warrant will allow the AFP and the ACIC to prevent the continuation of serious criminal activity and minimise harm to victims. These warrants could be used to disrupt or deny access to a computer that is being used for illegal purposes, or to illegal content. For example, removing content or altering access to content (such as child abuse material) could prevent the continuation of serious criminal activity, minimise harm to potential victims and be the safest and quickest option where offenders are in unknown locations or obfuscating their identity.

> Data disruption warrants will assist when the use of anonymising technologies or the dark web has constrained the ability of the AFP or the ACIC to respond to the criminal activity. For example, where the use of anonymising technologies has meant that offenders are too numerous, well-hidden or inaccessible for law enforcement to successfully use existing powers. The purpose of this warrant is to offer an alternative pathway for law enforcement to respond to serious crime online and minimise harm to victims, particularly where it is not feasible to pursue the traditional methods of investigation and prosecution.[1]

3.4 Whilst acknowledging the DDW as 'unique for Commonwealth law enforcement' the AFP said that the DDW was a:

> logical extension of the AFP's existing, extensive disruption activity. The AFP already seeks to delay, divert or otherwise complicate the commission of criminal activity, or the operations of a criminal entity, to prevent or reduce crime-related harm in Australia. Enforcement, disruption and prevention are closely interrelated and complementary in fulfilling the AFP's objectives of protecting the community and causing maximum damage to the criminal environment.[2]

3.5 The AFP said DDWs would be highly beneficial for child exploitation investigations as they could target services distributing child abuse material. The AFP provided an example of an online service utilised by over 600,000 persons that facilitates the sharing of child abuse material and the server hosts were suspected to be in Australia. The AFP said currently the removal of the content would require cooperation of the suspect, but with a DDW they could disable offenders' ability to utilise the site for criminal activity.[3]

3.6 The AFP said DDWs would be highly beneficial for cyber crime investigations by protecting the Australian community from the harmful effects of malware such as Remote Access Trojans (RATs). The AFP said currently their warrant powers only permit evidence collection and nothing could be done in one situation to remove a RAT from victim devices. The AFP said a DDW would allow the AFP to gain access to servers used by criminals distributing malware, then they could modify data in the

---

1 Department of Home Affairs, *Submission 9*, p. 13.

2 Australian Federal Police (AFP), *Submission 6*, p. 9.

3 AFP, *Submission 6.1*, p. 9.

computer making changes to the RAT software which would cause the removal of the R AT from the victims' computers.[4]

3.7 The ACIC said serious and organised crime was transnational by its very nature which, in combination with the effect of anonymising and encrypted technologies, meant offenders were both often anonymous and outside the jurisdiction of Australia. They said disruptions that were either short of, or in addition to, prosecution were sometimes the most practical way to prevent harm and fight crime.[5]

3.8 The ACIC said disruption in a digital environment to disrupt serious criminals was comparatively limited to the physical domain where Australian agencies could already lawful disrupt serious criminal activity through activities like interdicting drug shipments, freezing assets, confiscating proceeds of crime or restricting travel.[6]

3.9 The ACIC said data disruption powers such as would be provided by DDWs would allow the ACIC or AFP to halt the distribution of child exploitation material immediately when observed. They said DDWs could be used to block payments before rather than after the collection of evidence which could prevent additional offending occurring.[7]

3.10 The ACIC provided detailed examples of how DDWs would enable the ACIC to interfere with the data held on online criminal networks or devices in order to frustrate the commissioning of serious criminal offences. They said this would be 'particularly powerful' in the context of criminal activity that was largely conducted online such as the distribution of child exploitation material.[8]

3.11 The ACIC contextualised DDWs within the broader Bill and provided a hypothetical example whereby intelligence gathered from a network activity warrant (NAW) was used to inform a DDW application. This DDW could then be used to make it difficult for offenders to continue using encrypted handsets for example. They said this could include changing passwords to prevent users' access to the platform, introducing malware onto the devices connecting to the platform, and denial of service attacks to prevent the

---

4 AFP, *Submission 6.1*, p. 11.

5 ACIC, *Submission 23*, p. 4.

6 ACIC, *Submission 23*, p. 4.

7 ACIC, *Submission 23*, p. 4.

8 ACIC, *Submission 23*, p. 4.

server hosting the platform from operating. The ACIC said data disruption powers could also allow the ACIC to remove details of where to deposit money for those seeking to buy drugs or re-directing funds transfers. [9]

3.12 The ACIC said DDWs could enable evidence to be obtained and information gathered by virtue of disruption could be used in both the prosecution of offenders or to support further investigations under subsequent evidence gathering powers.[10]

3.13 The Uniting Church in Australia, Synod of Victoria and Tasmania (the Uniting Church) specifically supported the DDW and pointed to the:

> Lack of co-operation by many technology corporations with law enforcement agencies and their lack of pro-active efforts to ensure their services are not being used to facilitate serious human rights abuses or crimes.[11]

3.14 In supporting this argument the Uniting Church quoted a survivor of child sexual abuse as follows:

> From infancy until I was 15, I was trafficked and used in child sexual abuse material which continues to be shared widely across the internet. I spent hours every day searching for my own content, reporting thousands of accounts and posts sharing CSAM. When platforms don't actively look for or prevent this content from being uploaded, the burden falls to me to have these images removed. Each time one account gets taken down, five more like it take its place. It's like a hydra, a monster that I can never defeat. I'm not strong enough to take it down myself. It's costing me my well-being, safety and maybe even my life. I'm tired. I shouldn't find photos of myself as a child being raped when I'm just scrolling through my feed.
>
> *Survivor of child sexual abuse*.[12]

3.15 The Queensland Council for Civil Liberties, Liberty Victoria and Electronic Frontiers Australia (QCCL et al) had two fundamental issues of concern in relation to DDWs. These are:

- It is a dangerous step to enable law enforcement to modify what would be evidence in a criminal proceeding; and,

---

9 ACIC, *Submission 23*, p. 4.

10 ACIC, *Submission 23*, p. 5.

11 Uniting Church, *Submission 13*, p. 13.

12 Uniting Church, *Submission 13*, p. 13.

- Law enforcement has a poor record of the consequence of modification or deletion of digital information.[13]

3.16 The Law Council provided a detailed history and discussion of the Richardson Review and suggestion that, rather than suggest the AFP be granted disruptive powers to combat cyber-enabled crime, the Review recommended:

> the AFP should obtain assistance from the Australian Signals Directorate (ASD) to improve its technical capabilities, which could be deployed in the exercise of the AFP's existing investigatory powers.[14]

3.17 At the public hearing Home Affairs agreed that the government did not support the particular recommendation by Mr Richardson and explained that the DDW powers had been drafted very narrowly so as to address some of the concerns raised by Mr Richardson. Home Affairs said:

> The government did disagree with that recommendation, but, in framing the actual breadth of the offence, you would have noted that Mr Richardson's report was quite critical of the ability to destroy or damage computers. I think the quote—and I don't have the Richardson report in front of me, sorry—was about 'zapping computers' and in effect being 'judge, jury and executioner'. I would say that that legislation, as framed, if we're talking particularly about the data disruption warrant, does not do that. It's quite limited in the damage that it can do, and it can't do any damage to physical property or cause a monetary loss. It can't damage, as I said, other property. It's focused narrowly on disrupting data, so there's been an effort made to actually really focus on what we are about here. I think the operational examples from the AFP and others, which I can go to, show that it really goes to that ability to target data and not do that substantial or major damage that Richardson was referring to.[15]

Applications for data disruption warrants

Who may apply for a data disruption warrant

3.18 Proposed section 27KA sets out that a law enforcement officer of the Australian Federal Police or the Australian Crime Commission (or another

---

13 Queensland Council for Civil Liberties, Liberty Victoria and Electronic Frontiers Australia, *Submission 4*, p. 5-6.

14 Law Council of Australia, *Submission 21*, p.

15 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 45.

person on the law enforcement officer's behalf) may apply for the issue of a DDW if the law enforcement officer suspects on reasonable grounds that:

- (a) one or more relevant offences of a particular kind have been, are being, are about to be, or are likely to be, committed; and
- (b) those offences involve, or are likely to involve, data held in a computer (the target computer); and
- (c) disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more relevant offences that:
  - (i) involve, or are likely to involve, data held in the target computer; and
  - (ii) are of the same kind as the relevant offences referred to in paragraph (a).

3.19 An application may be made to an eligible judge or nominated AAT member. The Bill contains provisions for unsworn applications and for remote applications.

3.20 Relevant offence is set out in the Definitions section (section 6) of the SD Act and 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
>
> (c) an offence against section 15 of the Financial Transaction Reports Act 1988; or
>
> (ca) an offence against section 53, 59, 139, 140 or 141 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006; or
>
> (d) an offence against section 100, 100A, 100B, 101, 101A or 101AA of the Fisheries Management Act 1991; or
>
> (da) an offence against section 46A, 46C, 46D, 49A or 51A of the Torres Strait Fisheries Act 1984; 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
>
> (e) an offence that is prescribed by the regulations.

3.21 Issues relating to the definition of relevant offences are discussed in Chapter 2 of this report.

3.22 Noting the broad authority given to apply for a DDW the Law Council, whilst accepting that the AFP and ACIC may adopt internal policies to limit the class of people who may apply for DDW, preferred that such matters should be dealt with in primary legislation and not reliant on executive discretion in the exercise of powers. The Law Council said:

> A more judicious and focused statutory authorisation of applicants, which is limited to AFP and ACIC members of who possess a prescribed level of seniority and expertise, will offer greater assurance in relation to the rigour and consistency of quality of applications for data disruption warrants.[16]

3.23 In response to this suggestion, as part of an argument against only allowing senior officers to apply for DDWs, Home Affairs, citing advice from the AFP, said:

> it is strongly preferable that warrant applications are not restricted to only 'senior' or commissioned officers. It is important to ensure that, in all circumstances, the most appropriate person is able to apply for a warrant. This will be the person who has the relevant detailed knowledge about the investigation or operation should the issuing authority have questions in the course of considering the application. This will not necessarily be an officer who holds a senior rank in his or her agency.[17]

3.24 In addition Home Affairs said:

> The AFP has mandatory training requirements to ensure all AFP members who are eligible to apply for warrants, or authorise the use of powers, are familiar with their legislative obligations. This training provides all information required for members to understand the powers available under legislation, their statutory obligations and threshold requirements, any reporting obligations and oversight, the importance of legislative compliance and adverse consequences for non-compliance, and how to find assistance and resources to meet their obligations. The AFP's training is regularly inspected by the Ombudsman.

---

16 Law Council of Australia, *Submission 21*, p. 37.

17 Department of Home Affairs, *Submission 9.1*, p. 5.

> The ACIC advises that to achieve the highest standard of compliance with reporting, accountability and oversight measures associated with the Surveillance Devices Act and the Telecommunications Interception and Access Act 1979 (TIA Act) (and any other legislation providing the ACIC with similar powers), the agency has an Excellence in Compliance Strategy and training scheme. This consists of mandatory annual training and assessment requirements for staff who will be applicants for warrants and who need to access any information captured by a surveillance device or a telecommunications intercept or authorisation.[18]

3.25 Of note, the issue of internal application processes was addressed in part in other chapters of this report relating to the other powers. Substantively the arguments have much in common.

Determining the application

3.26 Proposed section 27KC provides that an eligible Judge or a nominated AAT member may issue a DDW if satisfied:

- (a) that there are reasonable grounds for the suspicion founding the application for the warrant; and
- (b) the disruption of data authorised by the warrant is justifiable and proportionate, having regard to the offences referred to in paragraph 27KA(1)(c); and
- (c) in the case of an unsworn application—that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and
- (d) in the case of a remote application—that it would have been impracticable for the application to have been made in person.

3.27 In determining whether a DDW should be issued, the eligible Judge or nominated AAT member must have regard to:

- (a) the nature and gravity of the conduct constituting the offences referred to in paragraph 27KA(1)(c); and
- (b) the likelihood that the disruption of data authorised by the warrant will frustrate the commission of the offences referred to in paragraph 27KA(1)(c); and
- (c) the existence of any alternative means of frustrating the commission of the offences referred to in paragraph 27KA(1)(c); and

[18] Department of Home Affairs, *Submission 9.1*, pp. 5-6. .

- (d) any previous warrant sought or issued under this Division in 1 relation to the alleged relevant offences referred to in 2 paragraph 27KA(1)(c).

3.28 The Law Council, after referring to the Richardson Review's characterisation of data disruption as different from electronic surveillances as it involves 'active intervention to frustrate the commission of an offence', cautioned against using consistency with the SDA as an argument for the proposed issuing authorities for a DDW and recommended:

> the Bill should be amended to provide that the issuing authority for a data disruption warrant is a judge of a superior court of record (specifically, a judge of a State or Territory Supreme Court or the Federal Court of Australia) who is appointed by the Attorney-General in their personal capacity.[19]

3.29 The Law Council pointed out that the third Independent National Security Legislation Monitor (INSLM) made recommendations in the of issuing authorities for the mandatory industry assistance orders under Part 15 of the *Telecommunications Act 1997* that there be independent issuing, by a new Investigatory Powers Division of the AAT, headed by a retired judge, comprising senior and experienced members with access to independent technical expertise.[20]

3.30 The Law Council said that consideration should be given to expanding this kind of regime to:

> all warrant-based powers conferred on investigative and intelligence agencies, subject to one matter of qualification. As with some current and previous AAT appointments, the members of any new Investigatory Powers Division should only be superior court judges, who are appointed to that Division in their personal capacities. This would be the Law Council's preference for the composition of a specialist division of the AAT for the issuance of warrants authorising coercive and intrusive powers.[21]

3.31 The Law Council submitted that determining data disruption warrants are 'likely to require complex judgments of fact and law' and recommended:

> a regime of public interest advocates to act as contradictors in all applications for data disruption warrants should be established.[22]

---

19 Law Council of Australia, *Submission 21*, p. 56.

20 Law Council of Australia, *Submission 21*, p. 54.

21 Law Council of Australia, Submission 21, p. 54.

22 Law Council of Australia, *Submission 21*, p. 56.

3.32 In relation to this the Uniting Church said:

> if you suddenly introduce a public interest monitor—as far as I can tell, the purpose there would be to only consider the right of privacy—then who advocates for the victims of human rights abuses such as the potential of being murdered, raped, tortured, subjected to sexual abuse? Do we have a victim's advocate who appears as well, who puts forward the case as to why the warrant is needed to prevent these other very serious human rights abuses from taking place?[23]

3.33 In addition Home Affairs referred to the Ministerial response to the Parliamentary Joint Committee on Human Rights and said:

> the warrants in the Bill are supported by a range of safeguards, stringent thresholds and oversight arrangements to protect the rights of an affected person and provide for independent scrutiny and review of decisions relating to the warrants. These measures will mitigate any need for public interest advocates to act as contradictors for all warrants.[24]

What an application must contain

3.34 A DDW must state the eligible Judge or nominated AAT member issuing the warrant is satisfied of the matters referred to in subsection 27KC(1) and has had regard to the matters referred to in subsection 27KC(2); and specify: a number of things including information on applicant, the relevant offence and a number of details around the target computer and any premises the computer is on.

3.35 A warrant may only be issued for a period of no more than 90 days.

What a data disruption warrant authorises

3.36 Proposed section 27KE sets out the doing of specified things (subject to any restrictions or conditions specified in the warrant) in relation to the relevant target computer.

3.37 The things that may be specified include any of the following that the eligible Judge or nominated AAT member considers appropriate:

- (a) entering specified premises for the purposes of doing the things mentioned in this subsection;

---

23 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, Canberra, 10 March 2021, p. 19.

24 Department of Home Affairs, *Submission 9.1*, p. 9.

- (b) entering any premises for the purposes of gaining entry to, or exiting, the specified premises;
- (c) using:
  - (i) the target computer; or
  - (ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
  - (iii) any other electronic equipment; or
  - (iv) a data storage device;
  - for the following purposes:
  - (v) obtaining access to data (the relevant data) that is held in the target computer at any time while the warrant is in force, in order to determine whether the relevant data is covered by the warrant;
  - (vi) disrupting the relevant data at any time while the 1 warrant is in force, if doing so is likely to assist in frustrating the commission of one or more relevant offences covered by the warrant;

3.38 In addition to the above the warrant may authorise a number of actions to achieve the purpose mentioned in subparagraph (c)(v) or (vi) such as adding, copying or altering other data in the target computer.

3.39 The warrant may also authorise a number of specified activities to obtain access to data held in a target computer.

3.40 Proposed sub-section 27KE(7) sets out a number of acts that are not authorised by a DDW as follows:

- Subsection (2) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to: 20
- (a) materially interfere with, interrupt or obstruct:
  - (i) a communication in transit; or
  - (ii) the lawful use by other persons of a computer;
- unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or
- (b) cause any other material loss or damage to other persons lawfully using a computer, unless the loss or damage is justified and proportionate, having regard to the offences covered by the warrant.

3.41 Equivalent to existing provisions of the computer access warrant regimes in the SD Act and ASIO Act proposed paragraph 27KE(8)(a) provides that all data disruption warrants must authorise the use of force against persons and things, where such force is reasonably necessary to do any act or thing authorised under the warrant.

3.42 The Law Council made a number of detailed argument in relation to its concerns around the following:

- Meaning of 'disruption' of data and 'frustration' of offences;
- Causation of material loss or damage to lawful computer users;
- Telecommunications interception;
- Use of force against persons and things; and,
- Temporary removals of computers and other things from premises.

Meaning of 'disruption' of data and 'frustration' of offences

3.43 The Law Council gave a detailed argument around its concerns about the lack of a statutory definition for 'disruption' of data and 'frustration' of the commission of an offence. The Law Council recommended that these terms be statutorily defined or, in alternative (non) preferred option, recommended:

> Proposed paragraph 27KA(3)(b) (item 13 of Schedule 1) should be amended to provide that the statement of facts and grounds accompanying all applications for data disruption warrants must specify the following matters:
>
> - the acts or types of acts of data disruption that are proposed to be carried out under the warrant;
> - -the anticipated impacts of those specific acts or types of acts of disruption on the commission of the relevant offence (that is, how they are intended to frustrate that offence); and
> - the likelihood that the relevant acts or types of acts of disruption will achieve that objective.

3.44 In relation to 'disruption of data' Home Affairs disagreed with the Law Council's assessment and said the Bill:

> includes a definition of 'disrupting data' in subsection 6(1) of the Surveillance Devices Act (item 8 of Schedule 1 of the Bill). This definition provides that disrupting data means adding, copying, deleting or altering data held in a computer in relation to data disruption warrants and emergency authorisations for disruption of data. There are strong safeguards that expressly prohibit causing loss or damage to data that is not justifiable and proportionate or causing any permanent loss of money, digital currency or property other than data under a data disruption warrant or emergency authorisation.[25]

---

25 Home Affairs, *Submission 9.1*, p. 10.

3.45 In relation to the term 'frustrate' Home Affairs said the term takes on its ordinary meaning and the:

> deliberate decision was made not to define what 'frustrate' means beyond the ordinary meaning, which provides sufficient clarity while also providing the operational flexibility the AFP and ACIC require to make effective use of data disruption warrants. Data disruption action taken by the AFP or the ACIC may 'frustrate' criminal offending in more than one way, and it may not be possible to specify the particular nature of the frustration at the time of applying for the warrant. For example, the action of removing illegal material from a website may frustrate criminal offending by preventing a person from selling that material, preventing a person from accessing that material, reducing the risk of harm to victims of that material, damaging a criminal organisation's reputation for providing that material, eventually having an impact on the production of such material, or having other flow-on effects.[26]

Causation of material loss or damage to lawful computer users

3.46 Whilst proposed sub-section 27KE(7)(a) replicates equivalent provisions for computer access warrants under the SDA and ASIO Act the Law Council pointed out proposed sub-section 27KE(7)(b), in authorising 'the AFP or ACIC to do acts or things under a warrant that cause material loss or damage to persons lawfully using a computer', was a major departure from equivalent provisions under the computer access warrant regimes'.[27]

3.47 The Law Council set out a number of concerns with this power as follows:

- the necessity of the power has not been demonstrated;
- the thresholds for the exercise of the power are disproportionately low to the gravity of its impacts on individual rights and liberties;
- there is over breadth in the purposes for which the power may be exercised, in that the AFP and ACIC may cause material loss or damage for the purpose of carrying out any activity under the warrant, not only data disruption;
- the conferral of the power to cause material loss or damage to lawful computer users would, as the Richardson Review cautioned, place law enforcement officers in the role of 'judge, jury and executioner' in relation to decisions about whether to extinguish or significantly infringe the private property rights of non-suspects;

---

[26] Home Affairs, *Submission 9.1*, p. 10.

[27] Law Council, *Submission 21*, p. 56.

- the conferral of a broad power to cause material loss or damage to lawful computer users under data disruption warrants, and the prohibition on such activities under computer access warrants, may create propriety risks for the AFP and ACIC in selecting the particular type of warrant to be used in the investigation of cyber-enabled offences; and
- if the AFP or ACIC requested ASD to carry out a disruption activity under a data disruption warrant that has been issued to the AFP or ACIC, there may be a mismatch in the scope of multiple statutory immunities that would apply to ASD staff members in these circumstances. An ASD staff member may have a wider immunity in relation to acts done under data disruption warrants than they would if they had done the same acts for the purpose of performing ASD's own functions under paragraph 7(1)(c) of the Intelligence Services Act 2001 (Cth) (ISA) to prevent and disrupt cybercrime outside Australia, via electronic means.[28]

3.48 Home Affairs provided a detailed response to the concerns raised by the Law Council. They made an important point regarding the impossibility of guaranteeing no material loss or damage to persons who are not suspects saying that introducing:

> an absolute prohibition on causing material loss or damage to persons who are not suspects or persons of interest makes the situations above impractical to target with a data disruption warrant, and will encourage criminals to adapt their methodologies to respond to this gap in law enforcement's coverage. Due to the sophistication of modern computer systems and networks, it will be difficult if not impossible to make targeted changes that are guaranteed to impact only intended computers. For this reason, a proportionality requirement has been inserted into the Bill, in addition to the prohibition on causing damage to data unless that damage is justified and proportionate.[29]

3.49 In addition Home Affairs pointed out:

> an affected person has an avenue to challenge decisions made in regards to warrants through judicial review. Australian courts will retain their jurisdiction to review administrative decisions through the original jurisdiction of the High Court and in the Federal Court of Australia by operation of section 39B of the *Judiciary Act 1903*, or under the ADJR Act. In addition, where a person suffers loss of, or serious damage to, property or

---

28 Law Council, *Submission 21*, p. 62.

29 Home Affairs, *Submission 9.1*, p. 11.

personal injury as a result of the execution of a warrant (or emergency authorisation), the Commonwealth is liable to compensate that person.[30]

3.50 Home Affairs also responded in detail to other suggestions by the Law Council, which is found in Submission 9.1. In regard to consequential amendments to the Criminal Code and IS Act in relation to ASD, Home Affairs said ASD members could only avail themselves of limitation of liability provisions in Division 476 of the Criminal Code and section 14 of the IS Act to the extent that they were acting in proper performance of ASD's functions. They noted per section 7(1)(e) of the IS Act this was nothing more than what the AFP or ACIC have the power to do themselves.[31]

3.51 Home Affairs said in relation to the Law Council's recommendation relating to notifying the Ombudsman of any loss or damage caused the AFP and ACIC are required to notify the Ombudsman about the exercise of actions undertaken for the purposes of a DDW which would involve notice of actions undertaken that have caused loss.[32]

3.52 Home Affairs said additional annual reporting requirements was inconsistent with the policy intent of Ministerial reporting when combined with annual public reporting requirements for DDWs.[33]

3.53 In response to the Law Council's recommendation for raising the threshold for causing loss or damage, limiting actions and additional requirements for warrant applications, Home Affairs said consideration could be given to this matter. Home Affairs said this would be similar to the consideration for the issue of NAWs in proposed paragraph 27KM(2)(f). Home Affairs additionally noted in some cases it would be impracticable or impossible to make a distinction between what is data disruption activity and what is things authorised under the warrant necessary to enable the disruption. Home Affairs said for this reason it was important the ability to cause material loss or damage was not limited to the data disruption activities exclusively.[34]

---

30 Home Affairs, *Submission 9.1*, p. 11.

31 Home Affairs, *Submission 9.1*, p. 12.

32 Home Affairs, *Submission 9.1*, p. 12.

33 Home Affairs, *Submission 9.1*, p. 21.

34 Home Affairs, *Submission 9.1*, p. 11.

Telecommunications interception

3.54 Proposed paragraph 27KE(2)(h) of the Bill provides a disruption warrant authorises the interception of telecommunications, for the purpose of doing any act specified in the warrant. It replicates equivalent provisions for law enforcement and ASIO computer access warrants.

3.55 Whilst acknowledging that data disruption 'may require the incidental interception of telecommunications' the Law Council raised concerns that:

> once an interception power is authorised under a computer access warrant or data disruption warrant, it could be exercised, without any specific external authorisation or supervision, in a very broad range of circumstances during a warrant operation. For example, a warrant that authorised the interception of telecommunications, without any warrant-specific conditions or limitations being applied to further limit the purposes of interception, would permit an agency to:
>
> - intercept a person's voice or text-based communications for the purpose of determining whether they are, or will be, present at particular premises to which covert entry is sought under the warrant; or
> - disable or 'hijack' security systems at those premises which are connected to the internet, such as surveillance cameras or digital authentication points, for the purpose of covertly entering and exiting those premises under the warrant.[35]

3.56 In addition the Law Council raised concerns the intersection of the breadth of the telecommunications intercept power the power under the TIA to make subsequent use and disclosure of interception information obtained under a disruption warrant. [36]

3.57 The Law Council said:

> Any power to intercept telecommunications under a computer access warrant, data disruption warrant, network activity warrant or an account takeover warrant should be limited to a subset of specific activities authorised under the warrant. This should cover the specific purpose of gaining access to relevant data, and in the case of disruption warrants, performing a data disruption activity. As a minimum, there should be no power to intercept

---

35 Law Council, *Submission 21*, p. 71.

36 Law Council, *Submission 21*, pp. 71-72.

telecommunications for the purpose of gaining entry to, or exiting, premises under the warrant.[37]

3.58 The Department of Home Affairs made the reasonable and foundational point that:

> Computer access capabilities do not work in a vacuum and require some degree of knowledge and interaction with the telecommunications system before execution. As a result, it will often be necessary for law enforcement agencies to intercept communications to make access to or disruption of data practicable or technically possible, and to be able to maintain the necessary covert nature required to ensure these activities are both possible and effective.[38]

3.59 In addition Home Affairs said that

- data disruption warrants and network activity warrants cannot authorise the collection of evidence or intelligence by interception. If the AFP or the ACIC require interception to do anything more than facilitate execution of a data disruption or network activity warrant—for example, if the AFP or the ACIC want to gather evidence by interception—those agencies must seek a separate interception warrant from an eligible issuing authority under the TIA Act; and
- without the ability to intercept communications under a data disruption warrant or network activity warrant, it will be difficult to implement what is proposed under the warrant. In particular, interception must be available for the purpose of entering or existing premises, as it can prove essential in preventing the target of the warrant from being alerted through an electronic security system (such as, an alarm or camera) that they are under law enforcement surveillance. Interception could also be essential to alerting the AFP or the ACIC where a target could become aware of an investigation against them through, for example, an automated email being sent when an account or computer is accessed from a new or unknown IP address, or through any other automated notification when new or irregular activity occurs with an online account.[39]
-

37 Law Council, *Submission 21*, p. 72.

38 Department of Home Affairs, *Submission 9.1*, pp.12- 13.

39 Department of Home Affairs, *Submission 9.1*, p. 13.

Use of force against persons and things

3.60 Commenting on the drafting of proposed paragraph 27KE(8)(a) the Law Council said:

> If an issuing authority decides to issue a data disruption warrant, they will have no discretion in the authorisation of force.[40]

3.61 In response Home Affairs pointed out that force can only be used 'where necessary and reasonable to do the things specified in the warrant' and that the

> ability to use force under warrant is required due to the eventualities that officers may face while executing a warrant. For example, it may be necessary to use force against a door or a cabinet lock to access a thing on the premises or to use force to install or remove a computer from a premises. In the case of force against a person, its use is constrained on the face of the legislation to circumstances where force is required to execute the warrant—for example, if a person is in physically preventing an officer from accessing a computer or other thing that needs to be used for the purposes of obtaining access to the relevant data under warrant. Use of force may also be necessary to ensure the safety of AFP and ACIC officers in the event a person acts aggressively.[41]

Temporary removals of computers and other things from premises

3.62 Proposed paragraph 27KE(2)(f) and subsection 27KE(3) of the Bill authorise the temporary removal and return of a computer or any other thing from warrant premises, for the purpose of doing any act or thing specified in the warrant under subsection 27KE(2).

3.63 The Law Council, echoing concerns previously raised about equivalent temporary removal provisions under law enforcement and ASIO computer access warrants, had four main concerns around the temporary removal powers as follows:

- Importance of statutory time limits for removal;
- Need for a clear statutory obligation to return items after a warrant expires;
- Ambiguity and overbreadth in the meaning of 'other things' that may be removed; and,

---

40 Law Council, *Submission 21*, p. 73.

41 Department of Home Affairs, *Submission 9.1*, p. 13.

- Removal of computers or things that may cause interference or loss.[42]

3.64 In response to these concerns Home Affairs said the power to remove items from a premises was limited by things that are, in some way, needed to execute the warrant. Home Affairs said this could include data storage devices or a piece of paper with passwords, for example.[43]

Extension and variation of data disruption warrant

3.65 Proposed section 27KF allows for the extension and variation of a DDW.

> 1 A law enforcement officer to whom a data disruption warrant has been issued may apply, at any time before the expiry of the warrant:
>
> a. for an extension of the warrant for a period of no more than 90 days after the day the warrant would otherwise expire; or
>
> b. for a variation of any of the other terms of the warrant.

3.66 The Law Council recommended that:

> Proposed subsections 27KD(2) and 27KF(1) (item 13 of Schedule 1) should be amended to provide that the total maximum duration of a data disruption warrant is 90 days, inclusive of any extensions if the warrant is initially issued for a period of less than 90 days.
>
> - If the AFP or ACIC consider that there is a need to carry out further data disruption activities after the 90-day total maximum period of effect for a data disruption warrant, then they should be required to seek a new warrant.[44]

3.67 Home Affairs pointed out that the proposed section did not mean that all warrants would be issued for 90 days and noted that the extension power provided for the flexibility needed in the warrant process to account for 'extended investigations and unexpected circumstances.'[45]

3.68 In addition, Home Affairs pointed to the reporting and oversight mechanisms in relation to extensions stating that:

> The AFP and the ACIC are required to report to the Minister for Home Affairs on the number of extensions and variations made to a warrant along with the

---

42 Law Council, *Submission 21*, p. 73.

43 Department of Home Affairs, *Submission 9.1*, p. 14.

44 Law Council, *Submission 21*, pp. 80-81.

45 Department of Home Affairs, *Submission 9.1*, p. 15.

reasons for why they were granted. The Ombudsman is empowered to inspect the AFP and the ACIC's records to determine the extent of their compliance with requirements for data disruption warrants. This will necessarily involve inspecting records made in relation to extensions and variations of warrants.[46]

Revocation and discontinuance of access and disruption under warrant

3.69 Proposed section 27KG allows for revocation of a DDW and 27KH allows for discontinuance of access and disruption under a DDW. No specific concerns were raised about this proposed section.

Emergency authorisation

3.70 Proposed section 35B inserts the power for a Judge or nominated AAT member to approve giving of an emergency authorisation for disruption of data held in a computer.

3.71 This may be done in the following circumstances if the eligible Judge or nominated AAT member if satisfied that there were reasonable grounds to suspect that:

- (a) there was a risk of serious violence to a person or substantial damage to property; and
- (b) disruption of data held in the target computer mentioned in that subsection may have helped reduce the risk; and
- (c) it was not practicable in the circumstances to apply for a data disruption warrant.

3.72 The Law Council raised detailed and nuanced concerns with accompanying recommendations in relation to emergency authorisation for DDWs.

3.73 The Law Council's primary concern was in relation to the appropriateness of emergency authorisations for data disruption powers. They argued that DDWs were 'a materially different power to conducting electronic surveillance for investigatory purposes' and had the potential to cause harm to non-suspects and should, therefore, should not be subject to the regime of emergency authorisations.[47]

---

46 Department of Home Affairs, *Submission 9.1*, p. 15.

47 Law Council, *Submission 21*, p. 83-84.

3.74 In the even that emergency thresholds remained available in relation to DDWs the Law Council outlined further concerns as follows: Thresholds for emergency authorisations;

- Thresholds for emergency authorisations;
- Obligations if issuing authority does not retrospectively approve an authorisation; and,
- 'Appropriate authorising officers' for emergency data disruption powers.[48]

3.75 Home Affairs gave equally detailed responses to the Law Council's concerns. In relation to the primary recommendation that emergency authorisation not be available for DDWs Home Affairs stated that

> the ability to disrupt data, and the ability to take control of an account in emergency situations is important for ensuring that the AFP and the ACIC will be able to respond to rapidly evolving and serious threats in a timely and effective manner.[49]

3.76 Home Affairs set out this reasoning in more detail providing a string argument for the continuation of emergency authorisation being available in relation to a DDW:

> The modern criminal environment is fluid and fast-paced, and criminal plans can escalate rapidly in response to numerous external factors. The AFP advises that, due to criminals' use of anonymising technology and encryption, it could be that the AFP becomes aware of an escalation of criminal planning or intent with short notice—for example, in the counter-terrorism space, where there is significant risk to the community if offenders are not disrupted. In a situation where a code word is posted to alert criminal network members to commence criminal activities, an emergency authorisation for the disruption of data could be utilised to remove the code word, reduce its visibility to criminal network members, and disrupt the plot for criminal offending. Emergency authorisations will allow the AFP to more effectively react to changes that pose a significant risk to community safety.[50]

3.77 Home Affairs provided detailed responses to the Law Council's recommendations should the emergency authorisation power remain in relation to DDWs.[51]

---

48 Law Council, *Submission 21*, p. 84-87.

49 Department of Home Affairs, *Submission 9.1*, p. 16.

50 Department of Home Affairs, *Submission 9.1*, p. 16.

51 Department of Home Affairs, *Submission 9.1*, pp. 17-18.

Extraterritoriality

3.78 Proposed section 43C of the SDA provides for the extraterritorial execution of data disruption warrants, which are similar to existing provisions of the SD Act in relation to surveillance device warrants and computer access warrants.

3.79 The Law Council raised a concern that this could represent an overlap with ASD's function to prevent and disrupt cybercrime outside of Australia. They said that they were

> concerned that the duplication created by proposed section 43C of the SDA creates a risk of conflict or inconsistency in the offshore disruption activities undertaken by ASD, the AFP and ACIC, including as a result of significant differences in applicable authorisation thresholds and processes and oversight mechanisms.
>
> Any duplication of powers to disrupt cyber-enabled crime by persons or organisations outside Australia could also jeopardise the security and effectiveness of offshore disruption operations (for example, if de-confliction and coordination mechanisms are inadequate or ineffective). It may also lead to inefficiencies in the use of public resources by multiple agencies in conducting substantially similar disruption operations outside Australia.[52]

3.80 Home Affairs explained that the roles of the AFP and ACIC using DDWs to take action against offenders—who are in Australia or who are Australian was in contrast to that of ASD's role in preventing and disrupting, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia. They said that:

> Australian offenders regularly interact with data held offshore, and conversely, the Australian community can be harmed using data hosted offshore. Transnational serious and organised crime groups operate with complete disregard for borders, and are increasingly choosing to conduct their activities in countries that are not favourable for Australian law enforcement activity. Removing the ability to access or disrupt data offshore with the permission from the relevant foreign country (as is proposed in relation to data disruption warrants and network activity warrants) will significantly constrain the AFP and the ACIC's ability to investigate serious criminality and

[52] Law Council of Australia, Submission 21, p. 82.

access the information required to identify offenders or disrupt online criminal activity.[53]

[53] Department of Home Affairs, *Submission 9.1*, p. 16.

4. Network Activity Warrants

4.1 The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) (the Bill) provides for the insertion of Network Activity Warrants (NAWs) into the *Crimes Act 1914 (Cth)* (the Crimes Act) for use by the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC).[1]

4.2 Following the setting out of some general comment this chapter will set out in more detail the following:

- Applications for NAW
  - Who may apply for a NAW
  - Issuing authorities
  - Determining the application
  - What an application must contain
  - Relevant offences
  - Emergency authorisation
- What a data disruption warrant authorises
  - Extension, variation and revocation of a data disruption warrant
  - Revocation and discontinuance of access and disruption under warrant
- Oversight, review and privacy

4.3 The Committee notes that a number of concerns raised by submitters, particularly the Law Council of Australia, and responses given by the Department of Home Affairs are similar, if not identical to, issues canvassed in the previous chapter on Data Disruption Warrants.

---

[1] ACIC means the agency established by the *Australian Crime Commission Act 2002 (Cth)* and in legislation is referred to as the ACC.

The requirement for the proposed legislation and the purpose of the powers

4.4 As describe in Chapter One NAWs would allow the AFP and the ACIC to collect intelligence on criminal networks operating online by permitting access to the devices and networks used to facilitate criminal activity. The Department of Home Affairs said:

> The Bill introduces a network activity warrant to enable the AFP and ACIC to collect intelligence on criminal networks operating online. This will enable investigators to identify offenders and understand the scope of their activities to build a full picture of how criminal networks are operating online. The intelligence gained through this will inform investigations by enabling law enforcement to strategically target criminal networks of the biggest threat to maximise impact.[2]

4.5 The threat environment and requirement of the NAWs is common across the other warrant types and referenced in earlier chapters. This chapter focusses specifically on the Bill itself and the proposed provisions relating to NAWs. The AFP said:

> In the online environment, we're far more restricted in how we can track illegal activities in this way. We can assume an identity and interact with offenders. We can get targeted warrants to intercept their communications and access their data, and, with the TOLA industry assistance framework, we can get help to pen the front door. But we've still got one hand tied behind our back.[3]

4.6 The AFP said the purpose of NAWs was for intelligence, and specifically they would be used in advance of specific computer access warrants against individual devices. The AFP said a NAW would allow them to collect intelligence on a network of computers to best identify which devices to target under a subsequent, and separate, computer access warrant.

4.7 The AFP said the rapid development of anonymising and encrypted technology was changing the counter-terrorism environment and presenting new challenges for the AFP. They said it was incredibly challenging for law enforcement to positively identify persons of interest and NAWs would

---

2 Ms Cath Patterson, Deputy Secretary (Strategy and Law Enforcement), Department of Home Affairs, *Committee Hansard,* 10 March 2021, p. 46.

3 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, 10 March 2021, p. 48.

provide additional opportunities to reduce the threat to public safety by enabling earlier intelligence connection.[4]

4.8 The AFP said NAWs could be used to identify unknown individuals in contact with a known individual. The AFP said a computer access warrant could be sought for the known individual but the NAW would be used to allow the AFP to gather intelligence about the broader network of individuals in contact with the known individual, even as they move between different encrypted platforms.[5] The Department of Home Affairs said NAWs would be used as a first step to gather intelligence that allows the use of more targeted warrants.[6] In this sense the NAWs could be considered as often antecedent to computer access warrants.

4.9 The ACIC placed this Bill in the context of the TOLA Act and said:

> Traditionally, we may know who has done something or we might know what somebody has done. If we are lucky enough to know the who and the what, we use electronic surveillance that we currently have under TI, surveillance devices, search warrants under the Crimes Act and all sorts of other covert and overt investigative powers. But when we do not know the who or the what, we have a very significant gap. This is where we use components of the TOLA legislation to help us work with telecommunications companies et cetera to help discover the networks that are available. And now this piece of legislation will enable us to get on those networks.[7]

4.10 The ACIC said NAWs would 'immediately transform' the ACIC's ability to discover and understand serious criminal groups using the dark web and encrypted communication platforms to undertake facilitate serious crime. The ACIC said this would 'critical enhance' the ability of the ACIC to more accurately inform the national understanding of serious and organised crime.[8]

4.11 The ACIC said the requirement for an NAW was because while the ACIC might be able to detect criminal behaviour on a website or network, they could not identify all the individuals participating in criminal behaviour in the network. They said a NAW would provide the ability to target and

---

4 Australian Federal Police, *Submission 6.1*, p. 14.

5 AFP, *Submission 6.1*, p. 15.

6 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, 10 March 2021, p. 48.

7 Mr Michael Phelan, CEO, ACIC, *Committee Hansard*, 10 March 2021, p. 56.

8 ACIC, *Submission 23*, p. 3.

infiltrate the network, or class of computers, in which the crime is occurring so the members could be fully identified and the extent of the criminality be detected through intelligence collection.[9]

4.12 The Law Council of Australia said the necessity of these particular powers had not been demonstrated as:

> Intrinsic materials to the bill do not clearly or precisely identify a gap in existing investigative powers or the need for both the AFP and the ACIC to have dedicated intelligence collection powers.[10]

4.13 The ACIC said:

> At the moment, we have a very significant gap in law enforcement in tackling serious and organised crime due to encrypted networks. These criminal networks are currently operating, for example, in Australia on dedicated encrypted devices of which we estimate there may be just over 10,000 in this country…you do not have one of these devices unless you are a criminal.[11]

4.14 The ACIC said they were 'flying blind' with respect to these 10,000 devices.[12] Additionally the ACIC said:

> I note that these networks operated by criminal networks are something that is different to what we've been able to tackle in law enforcement in this country up until this time – right now, as a matter of fact, before the Bill.[13]

4.15 The Uniting Church discussed criminal networks in their submission, a particularly relevant concept given the importance of 'criminal network' in the proposed sections below. They said some criminal networks required a monthly subscription of providing a fresh image of a child being sexually abused, in order to maintain presence within the network.[14]

4.16 The Carly Ryan Foundation described the requirement for these powers and the evolution of criminal offending using online means:

---

9 ACIC, *Submission 23*, p. 3.

10 Dr Jacoba Brasch QC, President, Law Council of Australia, *Committee Hansard*, 10 March 2021, p. 2.

11 Mr Michael Phelan, CEO, ACIC, *Committee Hansard*, 10 March 2021, p. 56.

12 Mr Michael Phelan, CEO, ACIC, *Committee Hansard*, 10 March 2021, p. 56.

13 Mr Michael Phelan, CEO, ACIC, *Committee Hansard*, 10 March 2021, p. 56.

14 Dr Mark Zirnsak, Senior Social Justice Advocate Uniting Church in Australia (Synod of Victoria and Tasmania) (Uniting Church), *Committee Hansard*, 10 March 2021, p. 14.

> For me, the power for law enforcement agencies to be able to have data disruption warrants, network activity warrants and account takeover warrants is something that needs to happen. Crimes have changed. We have seen criminals hiding behind the anonymity of the internet and hiding behind privacy. When we put privacy ahead of protecting children I think we have a real societal issue.[15]

4.17 The CRF said they were observing a huge network of offending happening online.[16] To illustrate the scale or size of these networks, the Uniting Church noted the existence of an 18,000 person network who was involved in a site that was just dealing with sexual abuse of infants and toddlers in 2019.[17] They said the networks were of a very large scale and the AFP were overwhelmed with the 'sheer scale and size' of the number of people engaged in these online abuse activities.[18]

4.18 The ACIC noted the possible relationship between NAWs and disruption:

> When we have got hold of the network we may need the tools to be able to disrupt them that we currently don't have. We may want to do something to those networks similar to what they did in the United Kingdom, France and other countries.[19]

Applications for network activity warrants

4.19 The Committee considered the application process for NAWs including the requirements for application, requirements for granting, emergency applications, applicable offences and the issuing authority.

Threshold and application requirements

4.20 The Bill provides for details for applications for NAWs at proposed section 27KK. They include, but are not limited to, the following requirements:

1 A group of individuals is a criminal network of individuals; and

---

15 Ms Sonya Ryan, CEO, Carly Ryan Foundation, *Committee Hansard*, 10 March 2021, p. 15.

16 Ms Sonya Ryan, CEO, Carly Ryan Foundation, *Committee Hansard*, 10 March 2021, p. 17.

17 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, 10 March 2021, p. 17.

18 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, 10 March 2021, p. 17.

19 Mr Michael Phelan, CEO, ACIC, *Committee Hansard*, 10 March 2021, p. 57.

2 Access to data held in a computer (the target computer) that is, from time to time, used, or likely to be used, by any of the individuals in the group will substantially assist in the collection of intelligence that:

a. Relates to the group or to any of the individuals in the group; and

b. Is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

4.21 Specifically this proposed section provides that it is immaterial if the identities of the individuals in the group are unascertained, the target computer can be identified or the location of the target computer can be identified. It is furthermore not material that the composition of the group changes from time to time. The effect of these proposed provisions would be to broaden the scope of applicable entity to which these proposed powers would apply.

4.22 These applications can be made by written document. The Bill provides for remote applications at proposed section 27KL of the Bill. The Department of Home Affairs said:

> The network activity warrant has been lifted up to a more senior level because of the intelligence collection nature. That was determined appropriate, given the limited number as well.[20]

4.23 The Bill provides for what information these applications must contain at proposed section 27KN of the Bill. This includes the kinds of relevant offences in respect to which the warrant is issued and the criminal network.

Criminal network

4.24 One of the most significant issues identified with the NAW framework, and most common topic in submissions, related to the definition of 'criminal network of individuals' in the Bill. Whilst slightly hyperbolic, the oft-repeated argument was that a NAW could be used to gather intelligence on every user of WhatsApp, technically. The Law Council of Australia recommended amending the definition of 'criminal network of individuals'. The Human Rights Law Centre (HRLC) said:

> The definitions provided by the network activity warrants are so expansive as to be practically unlimited in scope.[21]

---

[20] Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, 10 March 2021, p. 59.

4.25 The Law Council of Australia said under the present definition it could be that a single person is suspected of an offence, but the power would allow application to a whole group. They said it could be that the group is not a criminal network, but a network that happens to have a criminal within it. The Law Council of Australia suggested:

> There's no nexus between the criminal activity and the group. Building the nexus would be a way of tightening it up.[22]

4.26 Specifically the Law Council of Australia recommended amending the Bill to require reasonable suspicion of a nexus between the suspected conduct of an individual group member in committing an offence, or facilitating the commission of an offence (or having done so, or being likely to do so); and the actions or intentions of the group as a whole. Additionally, they recommended amending the Bill to require proof that access to data held in the target computer was likely to substantially assist in the collection of intelligence that: relates to the group, or the actions of one or more of its individual members in pursuit of a common criminal purpose of the group; and is relevant ot the prevention, detection or frustration of one or more kinds of relevant offences, which are committed or facilitated in pursuit of a common criminal purpose of the group.[23]

4.27 The Cyber Security Cooperative Research Centre (CSCRC) said while the definition appeared vague, it was necessarily so for the intelligence gathering purposes of the warrant. They said it was unlikely the AFP or ACIC would use the power against an unrealistically large group but recommended the network be defined in the warrant application itself. [24]

4.28 The Uniting Church noted the different types of offending which could occur within networks. They said there was debate about contact and non-contact offenders within child exploitation networks. They said there were networks composed of largely contact offenders, but also non-contact

---

21 Mr Kieran Pender, Senior Lawyer, Human Rights Law Centre, *Committee Hansard*, 10 March 2021, p. 1.

22 Mr Tim Game SC, Member (National Criminal Law Committee), Law Council of Australia, *Committee Hansard*, 10 March 2021, p. 8.

23 Law Council of Australia, *Submission 21*, p. 24.

24 Ms Racheal Falk, CEO, Cyber Security Cooperative Research Centre (CSCRC), *Committee Hansard*, 10 March 2021, p. 24.

offenders who purchase child exploitation images and don't engage in the contact offending themselves.[25]

4.29 The Department of Home Affairs said that the definition was drafted 'to ensure operational efficacy' and is

> designed to capture individuals who did not intentionally facilitate criminal activity, or who may be accessing the same electronic service as those who do have those intentions. It is necessary that these individuals fall within scope of the warrant because the devices they use may hold, or lead to, valuable intelligence about criminal activity. The breadth of this definition is balanced by the stringent criteria to obtain a network activity warrant and the limitations on the use of information obtained under the warrant for intelligence collection purposes only.

4.30 In addition the Department of Home Affairs made a number of points as follows:

- criminal networks targeted by network activity warrants will not always be operating for a common criminal purpose—they may have multiple purposes and goals of which only some members are a part and carry out a range of serious crimes of differing gravity; and,
- dedicated encrypted communication platforms, such as Phantom Secure or Encrochat, which are commonly used by organised crime groups. Such organisations are frequently involved in multiple different types of offending.[26]

4.31 Ultimately The Department of Home Affairs submitted that implementing the Law of Australia's recommendation could

> undermine the intended purpose of network activity warrants as an intelligence collection tool to identify unknown individuals and the scope of their offending. Only being able to target one criminal enterprise would be detrimental to law enforcement gaining a complete understanding of the group's criminal activities. It is the intelligence gathered under this warrant that may show the common criminal purpose as agencies may not have an accurate understanding of what criminal activity is being facilitated until they have access to devices used by the criminal network.[27]

---

25 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard*, 10 March 2021, p. 17.

26 Department of Home Affairs, *Submission 9.1*, p. 26.

27 Department of Home Affairs, *Submission 9.1*, p. 26.

Issuing authority

4.32 The issuing authority for NAWs is an eligible Judge or nominated AAT member as provided by proposed section 27KK(3). This is similar to the Data Disruption Warrant (DDW) framework but distinct to the Account Takeover Warrant (ATW) framework. The Law Council of Australia recommended amending the Bill so that only judges of a superior court could authorise these warrants.[28] These arguments and responses from the Department of Home Affairs are similar to those set out in the chapter on Data Disruption Warrants (DDW).

Determining network activity warrant applications

4.33 The Bill provides for the process for determining NAWs by the issuing authority at proposed section 27KM of the Bill. Specifically this provides that the issuing authority may issue the warrant if satisfied that there are reasonable grounds for the suspicion founding the application of the warrant. Furthermore the issuing authority must have regard to:

1 The nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant; and

2 The extent to which access to data under the warrant will assist in the collection of intelligence that:

a. Relates to the group referred to in paragraph 27KK(1)(a) or to any of the individuals in the group; and

b. Is relevant to the prevention, detection or frustration of one or more kinds of relevant offences; and

3 The likely intelligence value of any information sought to be obtained; and

4 Whether the things authorised by the warrant are proportionate to the likely intelligence value of any information sought ot be obtained; and

5 The existence of any alternative, or less intrusive, means of obtaining the information sought to be obtained; and

6 The extent to which the execution of the warrant is likely to result in access to dat a of persons who are lawfully using a computer; and

---

[28] Dr Jacoba Brasch QC, President, Law Council of Australia, *Committee Hansard*, 10 March 2021, p. 2.

7 Any previous warrant sought or issued under this Division in relation to the group referred to in paragraph 27KK(1)(a).

4.34 The Department of Home Affairs said it was these factors that de facto narrowed the scope of the power so as to avoid the risk of intelligence collection against all users of WhatsApp, for example.[29]

4.35 The Law Council of Australia however said there was a real risk that the mandatory considerations under proposed section 27KM would become 'proforma assertions in affidavits'. They said it was rare for an issuing authority to seek additional information on a particular topic.[30]

4.36 The Communications Alliance said they were concerned that NAWs could be damaging for the privacy of third parties and recommended a requirement in the Bill to take into account the privacy of third parties.[31]

4.37 The Inspector-General of Intelligence and Security (IGIS) said the absence of considerations with respect to privacy in the granting criteria was conspicuous in this section.[32] Specifically:

> Clarity on the extent to which the right to privacy is intended to guide the use of network activity warrants will assist IGIS in the exercise of its legality and human rights oversight functions.[33]

Relevant offences

4.38 The Bill provides the NAWs can be sought in relation to relevant offences which carries the same definition as DDWs, and materially the same definition as ATWs though the latter is a creature of the Crimes Act. This definition is drawn from the existing SD Act to which these powers are proposed to be inserted into, and is not a new definition. The new component, as was identified in the evidence to this Committee, was

---

29 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, 10 March 2021, p. 52.

30 Mr Tim Game SC, Member (National Criminal Law Committee), Law Council of Australia, *Committee Hansard*, 10 March 2021, p. 2.

31 Mrs Christiane Gillespie-Jones, Director, Communications Alliance, *Committee Hansard*, 10 March 2021, p. 35.

32 The Hon Dr Christopher Jessup QC, Inspector General of Intelligence and Security, *Committee Hansard*, 10 March 2021, p. 38.

33 The Hon Dr Christopher Jessup QC, Inspector General of Intelligence and Security, *Committee Hansard*, 10 March 2021, p. 43.

applying these new powers to the existing definition and the appropriateness of doing so. This issue has been addressed in detail in Chapter 2.

4.39 The AFP discussed the relevance and importance of context when considering the relevant offences these powers would apply to:

> Criminal networks that we see online now, they commit a number of different offences. Collectively, it equals serious and organised crime.[34]

4.40 The Department of Home Affairs said proposed section 27KM(2) was intended to ensure the issuing authority considered 'the nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant'.[35] The Department of Home Affairs said:

> All of that together makes it very difficult to envisage a circumstance where you could have an offence that is subjectively considered a not serious three-year offence and then still get something like this network activity warrant. There is a range of measures in place for the issuing authority to give consideration to make sure that that exactly can't happen and that he nature and the gravity of the conduct is forefront.[36]

4.41 The Department of Home Affairs said if the thresholds were changed then potentially you would not be able to get targeted warrants for offences and do the intelligence work that the AFP have said they need to identify the offending.[37]

Emergency authorisations

4.42 There are no provisions for emergency authorisations in the Bill for this power given its intrusiveness and intelligence function, the justification for use in life-threatening situations is absent.

---

34 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, 10 March 2021, p. 61.

35 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, 10 March 2021, p. 52.

36 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce, Department of Home Affairs, *Committee Hansard*, 10 March 2021, p. 52.

37 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce, Department of Home Affairs, *Committee Hansard*, 10 March 2021, p. 49.

Duration, extension, revocation and variation of the warrants

4.43 The Bill provides for the extension and variation of NAWs at proposed section 27KQ of the Bill. The effect of this proposed section is to allow for multiple 90 day extensions of the warrants.

4.44 The Bill provides the warrants may only be issued for a period of no more than 90 days at proposed section 27KN(2) of the Bill. This is common across the three warrant types.

4.45 The Bill provides for revocation processes at proposed section 27KR of the Bill.

What a network activity warrant authorises

4.46 The Bill provides for what NAWs authorise in proposed section 27KP of the Bill. While similar to a computer access warrant, NAWs are distinct and could be considered as broader. It is possible the intention of a computer access warrant is further along a spectrum of warranted powers for these agencies and a NAW is designed to collect intelligence before a computer access warrant was sought, including to scope probable suspects for subsequent warranted activity.

4.47 Concealment provisions and certain acts not authorised are provided at proposed sections 27KP(6) and (8) of the Bill.

Journalist information

4.48 The HRLC said the AFP could seek a NAW in relation to a journalist, and from that point access a WhatsApp group to which the journalist belonged which would give rise to press freedom concerns.[38]

Power to authorise the use of surveillance devices

4.49 The Law Council of Australia recommended amending the Bill to omit the power to use surveillance devices under a NAW. They additionally provided non-preferred recommendations to this proposed section too.[39] Arguments around the use of surveillance devices is covered in detail in Chapter 2.

---

38 Mr Kieran Pender, Senior Lawyer, HRLC, *Committee Hansard*, 10 March 2021, p. 9.

39 Law Council of Australia, *Submission 21*, p. 24.

Oversight, review and privacy

4.50 The Bill provides that oversight of these powers would be by the Inspector-General of Intelligence and Security. The Law Council of Australia recommended the Government increase funding to the IGIS to ensure they were able to adequately perform their oversight functions.[40]

4.51 Department of Home Affair said that:

> The power to authorise the use of surveillance devices under network activity warrants does not constitute a trend towards a 'single electronic surveillance framework', as suggested by the Law Council. Rather, this limited and incidental use of surveillances devices reflects the challenges agencies face in combating serious cyber-enabled crime occurring in the increasingly complex modern communications environment.[41]

40 Law Council of Australia, *Submission 21*, p. 25.

41 Department of Home Affairs, *Submission 9.1*, p. 26.

5. Account Takeover Warrants and Controlled Operations

5.1 The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill) provides for the insertion of account takeover warrants (ATWs) into the *Crimes Act 1914 (Cth)* (the Crimes Act) for use by the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC).[1]

5.2 This chapter will set out in more detail the following:

- The threat environment and requirements for the powers
  - Necessity and proportionality of the powers
- Applications for account takeover warrants
  - Who may apply
  - What an application must contain
  - The issuing officer and threshold for granting the warrant
  - The applicable offences to which the warrant applies
  - Emergency authorisations
- What an account takeover warrant authorises
  - The scope of activities authorised by the warrant
  - Online account restoration
  - Extension, variation and revocation of account takeover warrants
  - Compensation for damages
- Oversight and review
- Modifications to the Controlled Operations regime and other minor amendments not related to ATWs

[1] ACIC means the agency established by the *Australian Crime Commission Act 2002 (Cth)* and in legislation is referred to as the ACC.

The requirement for the proposed legislation and the purpose of the power

5.3 As described in Chapter One ATWs would allow the AFP and ACIC to take exclusive control of specified online accounts possibly for the purpose of gathering evidence, or intelligence, to further a criminal investigation. Of note and according to the evidence received by this committee, the ATW would only authorise the control of the account and any gathering of evidence would need to be supported by powers or warrants elsewhere.

5.4 The AFP said these powers could be used alongside search warrants and controlled operations as they were not intended for use by themselves.[2] It is possible the combination of controlled operations and account takeovers would involve AFP control and use of alleged offender online accounts to collect intelligence and evidence against other offenders. The AFP said ATWs would allow them to assume the identity of an offender to take down child abuse material, identify further offender networks and their victims which they could not currently do.[3]

5.5 The Explanatory Memorandum (EM) for the Bill said these powers were intended for use against serious crime types such as terrorism and child-exploitation. The threat environment and requirement for the ATWs is common across the other warrant types and is referenced in earlier chapters.

5.6 The AFP said there was an existing gap these warrants would remedy. They said they had previously conducted consensual account takeovers but if consent was not forthcoming then this would hamper law enforcement efforts to frustrate offending or collect information. The AFP said account takeovers were not intended to be exercised in isolation – they were intended for use in conjunction with existing law enforcement powers.[4] The Department of Home Affairs said the narrow drafting of ATWs was deliberately for these purposes, and would increase the proportionality of the powers.[5]

---

2 Australian Federal Police (AFP), *Submission 6*, p. 13.

3 AFP, *Submission 6.1*, p. 9.

4 AFP, *Submission 6*, p. 13.

5 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 49.

5.7 The AFP said it was critical for the AFP to promptly secure online accounts during search warrants to prevent content being deleted by an offender and preventing other perpetrators in the network being alerted to law enforcement interest.[6] The AFP said their current challenges for child protection, as it related to ATWs, included the inability to safeguard resolution when executing warrants, the inability to take down child abuse material without account details, and that account access could both be retracted at any time and it was dependent on the offender's willingness to negotiate.[7]

5.8 The AFP said ATWs would greatly benefit child protection investigations. They said ATWs would lessen the risk that offenders not provide consent to a takeover which would halt valuable avenues of investigation and evidence collection or delete key evidence and notify criminal associates. The AFP said a covert ATW could prove useful prior to resolution of a search warrant.[8]

5.9 The AFP said ATWs would provide alternative avenues to remove child abuse material from an offender's online, cloud-based accounts, or prevent others accessing that material if the AFP had a data disruption warrant (DDW).[9]

5.10 The ACIC said ATWs would allow both the AFP and ACIC to use the 'trusted relationships and networks' that already existed between criminals against those very criminals. They confirmed what several other submissions had already noted that they would be often used in conjunction with other powers.[10]

5.11 The ACIC said ATWs would be an efficient method to infiltrate online criminal networks and could play a 'crucial' role in uncovering the identities of otherwise anonymous criminals, while also gathering evidence.[11]

5.12 The ACIC said they could disrupt crime under an ATW by preventing access to a criminal network, influencing a criminal network to support law

---

6 Australian Federal Police, *Submission 6.1*, p. 6.

7 AFP, *Submission 6.1*, p. 7.

8 AFP, *Submission 6.1*, p. 7.

9 AFP, *Submission 6.1*, p. 7.

10 ACIC, *Submission 23*, p. 5.

11 ACIC, *Submission 23*, p. 5.

enforcement operations, or collecting evidence.[12] The ACIC said the ability to exploit existing relationships within criminal networks would be more effective than infiltrating the networks via other means.[13]

5.13 The ACIC said these powers could additionally be used to preserve evidence where technology enables quick destruction of material on devices.[14]

5.14 The Law Council disagreed with the government-provided arguments of necessity and recommended ATWs not proceed unless and until a detailed justification of the perceived necessity was provided publicly which should include specific reasons for the perceived necessity of the power.[15]

5.15 The Law Council said the EM did not identify the precise objective underlying the power to lock someone out of an online account in addition to covertly monitoring the person's activities using that account. The Law Council queried whether the objective was to prevent destruction of evidence by a target, or to frustrate the commission of a relevant offence using that account.[16]

5.16 The Department of Home Affairs described the process and purpose of account takeover, saying:

> To take control of an online account involves law enforcement taking steps that result in law enforcement's exclusive access to the account. In most cases, taking control of an online account will involve depriving the account holder or a user of their access to the account. This may facilitate the preservation of evidence, by ensuring that offenders cannot remove evidence of their criminality, but this is not the primary purpose. By enabling law enforcement to obtain exclusive control of an account, offenders are not able to alert other offenders of potential law enforcement activity.[17]

5.17 The Law Council said the EM noted law enforcement agencies can presently only takeover a person's account with that person's consent and this power was intended to address this gap. The Law Council said this did not explain why these powers were necessary in light of several existing investigative powers. They said existing electronic surveillance powers existed which

---

12 ACIC, *Submission 23*, p. 5.

13 ACIC, *Submission 23*, p. 5.

14 ACIC, *Submission 23*, p. 5.

15 Law Council of Australia, *Submission 21*, p. 26.

16 Law Council of Australia, *Submission 21*, p. 143.

17 Department of Home Affairs, *Submission 9.1*, p. 28.

would authorise access (under computer access warrants, and surveillance device warrants authorising the use of data surveillance devices) to monitor a person's online activities using an account, for the purpose of obtaining evidence of a suspected relevant offence.[18]

5.18 As discussed above and based on evidence provided by the AFP it may be that ATWs are intended more towards collecting information against other suspects (subject to appropriate approvals) rather than collecting information against the person whose account is being taken over.

5.19 The Queensland Council for Civil Liberties and others in a joint submission said they did not accept that ATWs should be introduced into Australian law.[19] The Human Rights Law Centre (HLRC) said there was a lack of evidence justifying the need for the warrants.[20] In contrast, the Police Federation of Australia (PFA) and Uniting Church in Australia (Synod of Victoria and Tasmania) (the Uniting Church) said they supported the Bill and thought it should be introduced into Australian law.[21]

5.20 The HLRC said ATWs would enable the AFP and ACIC to undertake significant invasions of privacy in the investigation of suspected criminal activity.[22]

5.21 The Cyber Security Cooperative Research Centre (CSCRC) said if passed the Bill, including this power, would play a key role in countering serious cyber-enabled crime committed domestically and offshore. The CSCRC said authorities would no longer be required to ask serious criminals for permission to access online accounts as is the case currently.[23]

5.22 The NSWCCL described ATWs as 'crime prevention tools' and a new warrant type for law enforcement as their intention was not evidence gathering.[24] Amazon Web Services said ATWs were 'formulated for fundamentally different objectives for law enforcement' as they were not for

---

18 Law Council of Australia, *Submission 21*, pp. 142-143.

19 Queensland Council for Civil Liberties, Liberty Victoria, Electronic Frontiers Australia and the Australian Privacy Foundation (QCCL et al.), *Submission 4*, p. 6.

20 Human Rights Legal Centre (HRLC), *Submission 15*, p. 4.

21 Police Federation of Australia (PFA), *Submission 7*, p. 1. and The Uniting Church, *Submission 13*, p. 1.

22 HRLC, *Submission 15*, p. 7.

23 Cyber Security Cooperative Research Centre (CSCRC), *Submission 14*, p. 3.

24 NSWCCL, *Submission 3*, p. 5.

gathering evidence per se but to allow law enforcement agents to effectively stand in the online shoes of persons suspected of engaging in potential criminal activity. Amazon Web Services said these warrants would represent a significant departure from existing warrants and would elevate the risk to liberty and privacy of individuals which should be commensurate with an elevation of checks and balances. [25] In a broader discussion relevant to all of the powers the Law Council said:

> This is a big, further step and, hence, the need for the level of protections. If those steps are taken, the level of protections needs to be, correspondingly, much higher.[26]

5.23 The AFP disagreed with this characterisation and said:

> I want to emphasise that disrupting crime is a core business for the AFP. There is a misconception that disrupting crimes means that an investigation will never proceed to prosecution. This is simply not true. Many of our disruption efforts still result in the prosecution of offenders.[27]

Applications for account takeover warrants

5.24 The Committee considered the application process for ATWs including the requirements for application, requirements for granting the application, emergency applications, applicable offences and the issuing authority.

Threshold requirements and who may apply internally

5.25 The Bill provides details for applications for ATWs at proposed section 3ZZUN. They are:

1 A law enforcement officer may apply to a magistrate for the issue of an account takeover warrant if the law enforcement officer suspects on reasonable grounds that:

a. One of more relevant offences have been, are being, are about to be, or are likely to be, committed; and

b. An investigation into those offences is being, will be, or is likely to be, conducted; and

---

25 Amazon Web Services, *Submission 8*, p. 2.

26 Dr David Neal SC, Co-Chair (National Criminal Law Committee), Law Council of Australia, *Committee Hansard*, Canberra, 10 March 2021, p. 5.

27 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 47.

c. Taking control of one or more online accounts (the target accounts) is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of the commission of those offences.

5.26 These applications can be made by written document or in an emergency by other means of communication. If the latter occurs, the proposed section provides for several requirements to occur. The proposed section allows the magistrate to require the applicant provide additional information as is necessary for the proper consideration of the application.

5.27 The Law Council recommended limiting the 'law enforcement officers' who can apply for ATWs to staff members of a minimum classification who have been specifically authorised by the AFP Commissioner or ACIC CEO (as applicable) rather than authorising all staff of the AFP and ACIC as default.[28] The Department of Home Affairs said this proposed provision was to maintain consistency with other powers in the Act.[29]

5.28 The AFP said they had internal approval mechanisms to limit warrant and control warrant applications, saying:

> It has to be adjudicated. We have internal processes that go to a rank officer to make those calls. One is, you can't go to that issuing authority or issuing officer without going through that process. It has to be adjudicated. The resources have to be allocated. There are the costings of what this investigation or matter is going to apply and the specialist resources required. There's a lot that goes in before you make this application.[30]

5.29 When questioned about junior officers and whether these sections could or should be modified (in relation to both ATWs and DDWs) the AFP said:

> You may open up a can of worms in the sense that you may have a sergeant who's less experienced than a senior constable or constable. You might have a 25-year veteran who's a detective constable and never wants to go anywhere from a rank point of view. You could classify them as a junior officer but they're probably more experienced than the sergeant. We don't just have rank and the junior bit attached to that.[31]

---

28 Law Council of Australia, *Submission 21*, p. 26.

29 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 59.

30 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 60.

31 Mr Reece Kershaw, Commissioner, AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 59.

5.30 ACIC said they had existing training and oversight mechanisms in place regarding applications for warrants. ACIC noted their 'Excellence in Compliance' strategy relating to this topic.[32]

5.31 The Law Council recommended amending the definition of 'online account' per proposed section 3ZZUK to cover a more limited sub-set of online accounts, such as social media, email, and data or voice messaging accounts. The Law Council said if there was no intention to limit the definition of 'online account' in this way, they recommended the issuing criteria should apply specific exclusions or limitations in relation to online accounts that are used to provide essential services to a person such as banking and governmental services. [33]

5.32 The Law Council recommended reducing the scope of the proposed definition of 'online account' to accounts connected with electronic communications services in a way similar to the definition of 'designated communications provider' for the proposed Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) (the IPO Bill).[34]

5.33 The Law Council noted the definition of 'online account' was increasingly broad and encompassed most online activity. They said this, in combination with the definition of 'relevant offence', gave rise to issues of proportionality overall for the Bill. The Law Council said the EM did not provide insight into the key types of online accounts that the powers are directed towards.[35]

5.34 Home Affairs said the definition of online account per proposed section 3ZZUK of the Bill was 'deliberately broad and technologically neutral'. They said the type of accounts that may need to be taken over to enable evidence to be obtained varied immensely contingent upon the unique circumstances of each investigation.[36]

5.35 Home Affairs said it was important the definition of online account encompassed bank accounts and government services accounts. They said access to these accounts could be critical in revealing illicit financial flows,

---

32 ACIC, *Submission 23*, p. 6.

33 Law Council of Australia, *Submission 21*, p. 27.

34 Law Council of Australia, *Submission 21*, p. 144.

35 Law Council of Australia, *Submission 21*, p. 144.

36 Department of Home Affairs, *Submission 9.1*, p. 28.

suspicious transactions or additional criminal actors, directly relevant to the crime being investigated.[37]

5.36 Home Affairs said government accounts such as Centrelink and Medicare can form part of investigations into fraud, identity theft and the transfer of the proceeds of crime. They said it was important therefore that the ACIC and AFP were able to conduct account takeovers of these account types.[38]

What information account takeover warrant applications require

5.37 The Bill provides for what information is required in an ATW application at proposed section 3ZZUQ. This includes, but is not limited to, the applicant, the alleged offence, the target account (including the holder when known) and an outline of the investigation. This provision indicates that the subject of the warrant would be a target account rather than a named individual necessarily.

5.38 The Ombudsman said the Bill required ATW applications to provide 'sufficient information' to enable the magistrate to make a determination. The Ombudsman recommended that an ATW application require an affidavit setting out the grounds of an application consistent with delayed notification search warrants (the Crimes Act), surveillance device warrants and retrieval warrants (the *Surveillance Devices Act 2004* (Cth) (the SD Act), computer access warrants (the SD Act), telecommunications interception warrants ((*Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act)), proposed data disruption warrants, and proposed network activity warrants.[39]

5.39 The Law Council also recommended the inclusion of an affidavit requirement setting out the facts and grounds on which the warrant application was based.[40] The Law Council said this was anomalous given that ATWs have been designed to operate in tandem with other warrants that required affidavits (such as computer access warrants). The Law Council said the requirement for affidavits was an important form of assurance in relation to the rigour, precision and internal approval requirements for warrant applications.[41]

---

37 Department of Home Affairs, *Submission 9.1*, p. 28.

38 Department of Home Affairs, *Submission 9.1*, p. 29.

39 Commonwealth Ombudsman, *Submission 5*, p. 3-4.

40 Law Council of Australia, *Submission 21*, p. 27.

41 Law Council of Australia, *Submission 21*, p. 145.

5.40 Home Affairs said ATW applications must provide sufficient information to enable the magistrate whether or not to issue the ATW. They said other existing warrants do not explicitly require the production of an affidavit such as search warrants.[42]

5.41 The QCCL and others said the warrants should include the statutory requirement the issuing authority must consider the human rights (including specifically the right to privacy) implications of issuing the warrants.[43]

Issuing authority

5.42 Account takeover warrants are issued by a magistrate per proposed section 3ZZUJ of the Bill. In this sense the ATW regime differs substantially from the network activity warrant (NAW) and data disruption warrant (DDW) regimes discussed earlier. The applicant for an ATW must suspect on reasonable grounds that:

1 One or more relevant offences have been, are being, are about to be, or are likely to be, committed; and

2 An investigation into those offences is being, will be, or is likely to be, conducted; and

3 Taking control of the online accounts is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of the commission of those offences.

5.43 The AFP and Home Affairs said the issuing of ATWs by a magistrate was consistent with existing powers in the Crimes Act.[44] Home Affairs discussed this point and said:

> We looked closely at the nature of the power and, in determining the nature of the power, determined that it was government determined and it was probably best placed in the Crimes Act, and those warrants are generally issued by magistrates.[45]

5.44 However the Ombudsman recommended eligible judges and nominated Administrative Appeals Tribunal (AAT) members would be more

---

42 Department of Home Affairs, *Submission 9.1*, p. 29.

43 QCCL et al., *Submission 4*, p. 5.

44 AFP, *Submission 6*, p. 18.

45 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 51.

appropriate issuing authorities for ATWs. This would have the practical effect of matching the issuing authority for ATWs to the other two warrants being considered under this Bill. Several submissions took this recommendation further and argued only superior court judges should be authorising officers for these powers, removing the role of AAT members and magistrates all together.[46]

5.45 The Ombudsman said raising the issuing authority would be more consistent with covert regimes for delayed notification search warrants (Crimes Act), surveillance device warrants and retrieval warrants (the SD Act)), computer access warrants (the SD Act), telecommunication interception warrants (the TIA Act), proposed data disruption warrants, and proposed network activity warrants. The Ombudsman said having a magistrate issue ATWs was more consistent with overt powers than covert powers.[47]

5.46 The Commonwealth Ombudsman said while the provisions of the Bill were consistent with other warrants in the Crimes Act:

> We see an important distinction here in relation to the covert nature of these powers and suggest that it would be preferable for eligible judges and nominated AAT members to be the issuers of account takeover warrants and emergency authorisations, because of a consistency with the existing covert regimes for things such as delayed notification search warrants, surveillance device warrants and retrieval warrants, computer access warrants, and telecommunication interception warrants. With respect to all of those, it is judges and members of the AAT, as I understand it, who issue those covert warrants, and it seems to us sensible and consistent with those arrangements to approach it in that way.[48]

5.47 The Commonwealth Ombudsman said judges and AAT members were more accustomed, and had background in, covert powers.[49] The Law Council recommended amending the issuing authority to be a superior court judge, and not even a nominated AAT member.[50] The Law Council said any

---

46 Commonwealth Ombudsman, *Submission 5*, p. 3.

47 Commonwealth Ombudsman, *Submission 5*, p. 3.

48 Mr Michael Manthorpe PSM, Commonwealth Ombudsman, *Committee Hansard*, Canberra, 10 March 2021, p. 39.

49 Mr Michael Manthorpe PSM, Commonwealth Ombudsman, *Committee Hansard*, Canberra, 10 March 2021, p. 39.

50 Law Council of Australia, *Submission 21*, p. 26.

operational issues with having a superior court authorise these warrants would be an issue of court resourcing and would depend on the volume of applications.[51] In terms of whether altering the issuing authority would present an operational issue the AFP said:

> I don't want to overegg the pudding and say this would be disastrous in terms of operational impact, but, as Andrew [Warnes] said, it's very consistent in terms of the powers that we currently have in place.[52]

5.48 Twitter said the use of 'lower-level magistrates' to issue ATWs was inconsistent with other electronic surveillance warrants. Twitter said the Committee had previously recommended serious search warrants be issued only by senior judges. [53]

5.49 The NSWCCL recommended the power to issue ATWs be limited to judges. NSWCCL said magistrates were not tenured and often did not have the background needed to properly examine requests under pressure and be prepared to reject the requests. NSWCCL said in *Smethurst v Commissioner of Police* a magistrate misstated the offence and used language so vague it provided no real limit on the nature of the search.[54]

Determining account takeover warrant applications

5.50 The Bill provides for the determination of ATWs at proposed section 3ZZUP:

1 A magistrate may issue an account takeover warrant if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant.

2 In determining whether an account takeover warrant should be issued, the magistrate must have regard to:

a. The nature and gravity of the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought; and

b. The existence of any alternative means of obtaining the evidence sought to be obtained; and

---

51 Dr David Neal SC, Co-Chair (National Criminal Law Committee), Law Council of Australia, *Committee Hansard*, Canberra, 10 March 2021, p. 2.

52 Mr Ian McCartney, Deputy Commissioner (Investigations), AFP, *Committee Hansard*, Canberra, 10 March 2021, p. 50.

53 Twitter, *Submission 11*, p. 6.

54 NSWCCL, *Submission 3*, p. 6. citing *Smethurst v Commissioner of Police* [2020] HCA 14.

c. The extent to which the privacy of any person is likely to be affected; and

d. The likely evidentiary value of any evidence sought to be obtained; and

e. Any previous warrant sought or issued under this Division in connection with the same online account; and

f. Any previous warrant sought or issued under this Division in connection with the same alleged relevant offence or the same alleged relevant offences.

5.51 Home Affairs said the determining characteristics assisted in narrowing the applicable relevant offences and ensuring proportionality for the powers. Specifically they noted the requirements, for example, in proposed section 27KM(2).[55]

5.52 The QCCL and others said the threshold requirement of 'reasonable suspicion' was 'inappropriately low'.[56] The QCCL and others recommended the threshold for issuing ATWs be raised to 'reasonable belief informed by probative evidence'.[57] The AIIA said they supported the QCCL recommendation that the threshold for granting the warrants should be raised from 'reasonably suspecting' to 'reasonably believing on the grounds of probative evidence'.[58]

5.53 The OAIC recommended the Bill or EM be expanded to identify some of the 'objective circumstances that should be considered in determining whether there are 'reasonable grounds' to support the seeking and issuing of a warrant'. The OAIC said this would assist in ensuring consistency in decision making as it relates to 'reasonable grounds'.[59]

5.54 The Law Council recommended introducing specific protections for privileged and journalistic information as part of the issuing criteria and process for the powers. The Law Council noted the PJCIS press freedoms

---

55 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 61.

56 QCCL et al., *Submission 4*, p. 4.

57 QCCL et al., *Submission 4*, p. 7.

58 AIIA, *Submission 17*, p. 3.

59 OAIC, *Submission 19,* p. 5.

inquiry and the recommendations made as part of that inquiry relating to this topic.[60]

5.55 The Law Council recommended requiring the applicant specifically declare whether they believed on reasonable grounds that the data access sought would include information subject, or likely to be subject, to client legal privilege. If it was expected, then the following issues should be addressed by the issuing authority: access to privileged information is necessary to execute the warrant; the public interest in accessing the information outweighs the interest in protecting it; and adequate procedures have been implemented to protect information subject to a claim or likely claim of client legal privilege.[61]

5.56 Home Affairs said the existing proposed provisions in section 3ZZUP supported magistrates giving consideration to third party impacts that included, but were not limited to, privacy.[62]

Public interest monitor, advocate or contradicter

5.57 The Law Council recommended the inclusion of a Public Interest Monitor (PIM) as part of the warrant authorisation process. The Law Council said this person would test the propositions being put by the applicant to the issuing authority.[63] The Law Council recommended a role for public interest advocates in all warrant applications that related to journalistic information and noted the PJCIS press freedoms inquiry recommendations. They recommended at least warrants sought in relation to journalists should be approved by a superior court judge.[64]

5.58 The NSWCCL and QCCL et al. recommended the creation of PIM to protect the public interest regarding applications by law enforcement agencies for various warrants.[65] NSWCCL said a similar role existed to some extent in Queensland, Victoria and New South Wales. NSWCCL said the Independent National Security Legislation Monitor (INSLM) did not fulfil this function.

---

60 Law Council of Australia, *Submission 21*, p. 29.

61 Law Council of Australia, *Submission 21*, p. 153.

62 Department of Home Affairs, *Submission 9.1*, p. 30.

63 Dr David Neal SC, Co-Chair (National Criminal Law Committee), Law Council of Australia, *Committee Hansard*, Canberra, 10 March 2021, p. 2.

64 Law Council of Australia, *Submission 21*, p. 153.

65 QCCL et al., *Submission 4*, p. 8.

NSWCCL recommended a PIM be able to contest warrant and be informed of warrants before they are issued.[66] The QCCL et al. said the warrants should be subject to a PIM to ensure that 'these intrusive powers remain in the public interest and do not scope creep without oversight and a modicum of transparency'.[67]

5.59 The Uniting Church in response to the recommendation for public interest advocates or monitors said:

> If you suddenly introduce a public interest monitor – as far as I can tell, the purpose there would be to only consider the right of privacy – then who advocates for the victims of human rights abuses such as the potential of being murdered, raped, tortured, subjected to sexual abuse? Do we have a victim's advocate who appears as well?[68]

5.60 No Commonwealth precedent for a public interest advocate or monitor (in existence) was provided to the Committee.

Regard to technical considerations

5.61 The Communications Alliance recommended the judicial authorisation process be informed by independent technical advice on the intended method of disruption, and potential risks to networks, third parties or other 'collateral damage'.[69]

5.62 The AIIA recommended the government stand up an independent board or approved list of communications and technology technical experts that are able to be consulted before applications for warrants are made. Of note, these recommendations were often common across the three warrant types and may be more relevant for the disruption powers considered elsewhere in this Bill. The AIIA said this board would have regard to security, integrity and technical feasibility considerations of government intervention in systems and networks and could provide advice to both government and industry in facilitating the disruption of crime in a reasonable, proportionate and technically feasible fashion.[70]

---

66 NSWCCL, *Submission 3*, p. 6.

67 QCCL et al., *Submission 4*, p. 5.

68 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church, *Committee Hansard,* Canberra, 10 March 2021, p. 20.

69 Communications Alliance, *Submission 12*, p. 2.

70 AIIA, *Submission 17*, p. 3.

Regard to privacy (including third parties)

5.63 The Law Council recommended amending the Bill to require the issuing authority have specific regard to adverse impacts on third parties and several other factors. The Law Council said this should include specific requirements to assess likely: impacts on personal privacy; financial impacts on individuals and businesses; impacts on a person's ability to conduct their business and personal affairs; and impacts on a person's ability to have contact with family members, or provide or receive care.[71]

5.64 The HRLC recommended amending the Bill so that in circumstances where an alternative means exist of preventing the offence or obtaining the evidence sought, the decision-maker should be obliged to deny the application unless reasonably satisfied that the alternative means would be more intrusive on the targeted individual's privacy, or materially less effective in frustrating the offence or obtaining the evidence sought.[72] The HRLC said the issuing authority must have regard to the existence of any alternative means of frustrating the offence or obtaining the evidence sought, however a warrant may be issued regardless of any such means.[73]

5.65 DIGI said the requirement in the Bill for the issuing authority to have regard to the impact on privacy was 'not sufficient' as it was limited and vague. DIGI said 'to have regard to privacy', as was currently in the Bill, was highly general and not replicable. DIGI recommended stronger protections for privacy across all the powers, which should include whether these warrants are proportionate and necessary.[74] The OAIC said the provisions in the ATWs required a magistrate to have regard to the extent to which the privacy of any person was likely to be effective. The OAIC however said they considered this to be a privacy protective measure that would help to ensure that ATWs were only issued in circumstances that were 'reasonable, necessary, and proportionate to do so following consideration of the privacy impacts'.[75]

5.66 DIGI recommended law enforcement write a 'Privacy Impact Assessment' for every warrant under the Bill. DIGI said while the EM alludes to such

---

71 Law Council of Australia, *Submission 21*, p. 27.

72 HRLC, *Submission 15*, p. 6.

73 HRLC, *Submission 15*, p. 11.

74 DIGI, *Submission 20,* p. 5.

75 OAIC, *Submission 19,* p. 3.

considerations they were not in the Bill itself. DIGI said this assessment would be in line with consumer expectations of their data privacy, provide necessary reassurances to the service provider on the due diligence undertaken, and ensure the Bill provides for the expected protections for privacy to assist Australia to be a qualifying power under the CLOUD Act. DIGI said these assessments should consider:

1. The necessity of the information being requested, and the need to minimise the collection of personal information to what is strictly necessary.
2. Whether the proposed method of accessing the information is the least privacy-infringing method available.
3. Whether the infringement on privacy is proportionate to the harm that will be averted by granting law enforcement access to the information.
4. An explicit requirement that agencies must show that they have attempted all other means of information access that would have a lesser privacy impact on individuals, and provide an explanation of why these alternate means are insufficient.
5. Requirements to minimise the retention of the data accessed during the investigation to a limited, specified period of time.[76]

Regard to human rights

5.67 The QCCL recommended the decision making criteria for the ATWs (and assistance orders) explicitly include consideration of the potential impact of the human rights of the subject and any other, directly or indirectly, affected person(s).[77]

Emergency authorisations

Application

5.68 The Bill provides for emergency authorisations by an appropriate authorising officer at proposed section 3ZZUJ of the Bill. This process is contained at proposed Division 3. This process allows for an official within the AFP or ACIC to issue the warrant, and it be subsequently authorised by a magistrate, having the practical effect of retrospective authorisation.

5.69 It does not allow the AFP or ACIC to authorise and issue their own ATWs. The application may be made orally, in writing or by telephone, fax, email or

---

[76] DIGI, *Submission 20*, p. 5.

[77] QCCL et al., *Submission 4*, p. 8.

any other means of communication. The appropriate authorising officer may give the emergency authorisation if satisfied that there are reasonable grounds for the suspicion founding the application.

5.70 The proposed section provides statutory conditions on this process, most prominently that an emergency authorisation must not be executed in a manner that results in damage to data unless the damage is justified and proportionate. Furthermore it must not cause a person to suffer a permanent loss of money, digital currency or property (other than data). The Law Council said:

> More fundamentally, we don't agree with the internal process itself. These sorts of extraordinary powers should be done by warrant, should be done through a judge, a superior court judge, with a contradicter there. So, as a fundamental issue, we don't agree with the internal process.[78]

Authorising officer

5.71 The appropriate authorising officers for emergency applications are the same as provided at proposed section 3ZZUM. The effect of this proposed section is to enable the chief officer of the AFP and ACIC, or their appropriately selected delegate to be the authorising officer. The Bill provides for requirements of recording the emergency authorisations and their attributes at proposed sections 3ZZUY – 3ZZUZ.

5.72 The OAIC said 'more appropriate mechanisms to seek a warrant in these kinds of emergency circumstances should be considered' and said other sections of the Bill allowed for applications made by telephone, fax, email, or any other means of communication. The OAIC recommended the Bill be amended to exclude warrant approval by an 'appropriate authorised officer' and consider alternative external warrant approval mechanisms. [79]

Review and consideration by magistrate

5.73 The Bill provides at proposed section 3ZZVA that within 48 hours after giving an emergency authorisation to a law enforcement officer, the appropriate authorising officer who gave the authorisation (or another person on that appropriate authorising officer's behalf) must apply to a magistrate for approval of the giving of the emergency authorisation.

---

78 Dr Jacoba Brasch QC, President, Law Council of Australia, *Committee Hansard*, Canberra, 10 March 2021, p. 5.

79 OAIC, *Submission 19*, p. 7.

Furthermore they must provide sufficient information to enable the magistrate to decide whether or not to approve the giving of the emergency authorisation and be accompanied by a copy of the written record made under section 3ZZUY in relation to the emergency authorisation.

5.74 In considering the emergency application, the Bill provides at proposed section 3ZZVB several factors the magistrate must consider including: the nature of the risk of serious violence to a person or substantial damage to property; the extent to which issuing an ATW would have helped reduce or avoid the risk; other alternative methods of investigation that could have been used; and whether it was practicable in the circumstances to apply for the ATW.

5.75 The Bill then provides at proposed section 3ZZVC the magistrate's consideration process of this application. For approval, the magistrate must be satisfied that there were reasonable grounds to suspect there was a risk of serious violence to a person or substantial damage to property, and taking control of the online account may have reduced this risk, and it was not practicable to apply for the ATW. The result of this process is the magistrate can issue the ATW as if it were approval for the original application. This has the practical effect of retrospective authorisation.

5.76 The OAIC recommended the Bill be amended to require that law enforcement agencies destroy any information collected under an emergency authorisation that was subsequently denied.[80] Home Affairs said for instances where an emergency authorisation was given by the agency but then not issued by the issuing authority any information obtained would be quarantined for oversight (e.g. Ombudsman) review of that particular episode.[81]

5.77 The Law Council recommended the issuing authority have discretion to order remedial action as appropriate, saying:

> It's our view that, if that occurs, there should be a requirement on the AFP or ACIC to inform the issuing authority of any adverse or potentially adverse impacts on third parties, and if there are adverse impacts on third parties as a result of an internal authorisation that has already been executed, then the issuing authority should have discretion to order remedial action be taken –

---

80 OAIC, *Submission 19*, p. 7.

81 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 53.

> for example, possibilities around financial compensation to those that have suffered damage or loss.[82]

Duration, extension, revocation and variation of the warrants

5.78 The duration of the ATWs is provided at proposed section 3ZZUQ(3) as 90 days. The Bill provides for multiple 90 day extensions at proposed section 3ZZUS. The OAIC recommended the Bill be amended to limit the number of warrant extensions that could be sought in respect of the same or substantially similar circumstances. The OAIC recommended requiring the issuing authority to consider the privacy impact on any individual arising from the extension to the warrant to ensure that the potential law enforcement benefits are necessary and proportionate to this impact'.[83]

5.79 The Bill provides for how ATWs are revoked or varied at proposed sections 3ZZUS – 3ZZUT.

5.80 The Law Council recommended amending the Bill to provide that ATWs must be executed within seven days of their issuance, and automatically cease to be in force once the AFP or ACIC has gained exclusive control of the account, akin to search warrants. The Law Council recommended amending the Bill so that if the AFP or ACIC sought to re-gain exclusive control of the account (or access was lost) they should be required to obtain specific authorisation under a new application.[84]

5.81 Home Affairs said it was not 'operationally feasible' to require ATWs be executed within seven days of issuance and for those warrants to cease to be in force once the AFP or ACIC had gained exclusive control of the account. They said search warrants authorised discrete evidence gathering and could effectively cease to be in force once the evidence gathering exercise is complete. They said ATWs were intended to be executed in tandem with continuous methods of evidence collection, covert surveillance and controlled operations. They said:

> Ongoing access to the online account is required to allow the flexibility needed to effectively infiltrate online criminality…The AFP and ACIC cannot remain in control of an account without an account takeover warrant, and as such the

---

82 Dr Jacoba Brasch QC, President, Law Council of Australia, *Committee Hansard*, Canberra, 10 March 2021, p. 5.

83 OAIC, *Submission 19,* p. 4.

84 Law Council of Australia, *Submission 21*, p. 146.

account takeover warrant must remain in force long enough to support evidence-gathering activities to be carried out.[85]

5.82 Home Affairs said a seven day period of effect may be significantly limiting on the effectiveness of law enforcement action.[86]

5.83 Home Affairs said it was not operationally feasible for there to be a requirement that the AFP or ACIC maintain control over the full period the ATW is in place. They said access could be lost due to a password reset which could reveal the existence of the operation. They said the requirement to obtain a new warrant where control of the account was lost temporarily was 'unnecessary and disproportionate'.[87]

Applicable offences

5.84 The Committee considered the applicable offences ATWs could be used for. In doing so it reviewed the EM, the Bill, submissions and public hearings. The ATWs apply to a 'relevant offence' per proposed section 3ZZUJ. This is defined by proposed section 3ZZUK (Definitions) as:

1 A serious Commonwealth offence; or

2 A serious State offence that has a federal aspect.

5.85 These two concepts are explored in **Appendix C** (Relevant Offences). These terms are not new to this Bill and are defined in the Crimes Act for existing use in other pieces of legislation. For an extensive discussion on applicable offences please see earlier chapters.

5.86 Home Affairs said the intention regarding relevant offences was to ensure consistency with other warrants in the Crimes Act. Home Affairs said another reason was because ATWs were a very, very narrow warrant and they did not enable access to data. They said it was hard to imagine a situation whereby an ATW was used without some other concurrent parallel power or controlled operation. [88]

---

85 Department of Home Affairs, *Submission 9.1*, p. 29.

86 Department of Home Affairs, *Submission 9.1*, p. 29.

87 Department of Home Affairs, *Submission 9.1*, p. 29.

88 Mr Andrew Warnes, Acting First Assistant Secretary (Electronic Surveillance Reform Taskforce), Department of Home Affairs, *Committee Hansard*, Canberra, 10 March 2021, p. 49.

What an account takeover warrant authorises

5.87 The Committee next considered the account takeover warrants themselves, including what they authorised and the manner in which this could be conducted. The Bill provides for what an ATW authorises at proposed section 3ZZUR. It requires an ATW to authorise the doing of specified things in relation to each target account. The proposed section provides:

1 An account takeover warrant must authorise the doing of specified things (the subject to any restrictions or conditions specified in the warrant) in relation to each target account.

2 The things that may be specified are any of the following that the magistrate considers appropriate in the circumstances"

a. Taking control of the target account at any time while the warrant is in force, if doing so is necessary, in the course of the investigation to which the warrant relates, for the purpose of enabling evidence to be obtained of the commission of the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is issued;

b. Using:

i. A computer; or

ii. A telecommunications facility operated or provided by the Commonwealth or a carrier; or

iii. Any other electronic equipment; or

iv. A data storage device;
for the purpose of taking control of the target account as mentioned in paragraph (1);

c. If necessary for the purpose of taking control of the target account as mentioned in paragraph (a):

i. Accessing account-based data to which the target account relates; or

ii. Adding, copying, deleting or altering account credentials to which the target account relates; or

iii. Adding, copying, deleting or altering data in a computer;

d. If, having regard to other methods (if any) of taking control of the target account which are likely to be as effective, it is reasonable in all the circumstances to do so:

i. Using a communication in transit for the purpose of taking control of the target account as mentioned in paragraph (1); and

ii. If necessary to achieve that purpose – adding, copying, deleting or altering data in the communication in transit;

e. Copying any account-based data to which the target account relates, and that:

i. Appears to be relevant for the purposes of determining whether the account-based data is covered by the warrant; or

ii. Is covered by the warrant;

f. Copying any account credentials to which the target account relates;

g. Any other thing reasonably incidental to any of the above.

3 For the purposes of paragraph (2)(e), if:

a. Access has been obtained to account-based data; and

b. The account-based data is subject to a form of electronic protection;

When account-based data is covered by a warrant

4 For the purposes of this section, account-based data is covered by a warrant if access to the data is necessary, in the course of the investigation to which the warrant relates, for the purpose of enabling evidence to be obtained of the commission of the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is issued.

5.88 The Law Council said ATWs did not authorise the collection of evidence of the relevant offence, which would require authorisation under a separate warrant such as a computer access warrant. The Law Council said this suggested ATWs would be sought and executed as part of a suite of warrants.[89]

5.89 DIGI said there was a disconnect between the Government's intention with ATWs and the drafting of ATWs in the Bill. DIGI noted the EM set out that ATWs required separate warrants or authorisation for accessing data but this point was not made explicit in the Bill. DIGI said it was difficult to understand how someone could take control of an account without accessing data on that account.[90]

---

89 Law Council of Australia, *Submission 21*, p. 139.

90 DIGI, *Submission 20,* p. 4.

5.90 Twitter said the scope of ATWs were unclear. Twitter said there were differences between what was outlined in the EM and the Bill (proposed Schedule 3 paragraph 25). Twitter said while the EM focussed on the AFP/ACIC taking over an account for the purposes of gathering evidence of criminal activity, the Bill provided that 'any other activities, such as accessing data on the account, gathering evidence, or performing undercover activities such as taking on a false identity, must be performed under a separate warrant or authorisation'. Twitter said the scope of what activities were ultimately authorised under at ATW were unclear.[91]

5.91 The Law Council recommended if the objective of account takeover was to preserve evidence of a suspected relevant offence by preventing its destruction, this should be included explicitly in the issuing criteria.

5.92 The Law Council recommended amending proposed paragraph 3ZZUR(8)(a) to provide that the AFP and ACIC must not execute a warrant in a manner that results in loss of, or damage to, data. The Law Council said there should be no general exception for loss or damage that is considered to be 'justified and proportionate'.[92] The Law Council said if there was a compelling justification for authorising the AFP or ACIC to cause loss of, or damage to, data in the course of executing an ATW, this should be among the powers in proposed subsection 3ZZUR(2) that the issuing authority may individually authorise.[93]

5.93 Certain acts not authorised are provided for a proposed section 3ZZUR(5).

Concealment of access, covert execution and mandatory consultation with providers prior

5.94 Concealment of access is provided for a proposed section 3ZZUR(6). It has the effect of authorising anything reasonably necessary to conceal the fact that anything has been done under the warrant. The Law Council recommended amending the Bill to ensure the ability to engage in post-warrant concealment activities more than 28 days after an ATW has ceased to be in force to require independent authorisation.[94]

---

91 Twitter, *Submission 11*, p. 5.

92 Law Council of Australia, *Submission 21*, p. 28.

93 Law Council of Australia, *Submission 21*, p. 28.

94 Law Council of Australia, *Submission 21*, p. 26.

5.95 DIGI said the powers could be used covertly without the knowledge of the service provider and this represented a key difference to the TOLA Act legislation which included service provider notifications.[95] DIGI said the lack of service provider notifications were a significant issue with the Bill. DIGI said:

> It is essential that a service provider be notified before the issuance of an Account Takeover Warrant. A lack of service provider notification compromises the security of users on the service provider's service. Law enforcement "hacking" or otherwise manipulating a service in order to obtain access will threaten the security of other users of that service.[96]

5.96 DIGI said for law enforcement to unilaterally undertake an account takeover they would need to identify and exploit vulnerability in the digital service and there was nothing to prevent this vulnerability being exploited by bad actors which would cause other security risks to users of the service and possibly crimes.[97]

5.97 Communications Alliance (CA) recommended the Bill be amended to provide that the service provider who will be required to action a warrant, or assists with or facilitates its execution, ought to be consulted prior to a warrant being issued. CA said this would confirm that the most appropriate provider has been approached, provides a means to streamline the process and/or ensure the most effective means to disrupt the targeted activity can be applied.[98] Twitter recommended introducing a requirement in the Bill for disclosure of ATWs to service providers before they are issued (i.e. in the planning phase) so the service provider can best assist the requesting agency.[99]

5.98 Fastmail Pty Ltd recommended a consultation process be established where the target computer was not owned by the person suspected of the offence. Fastmail said this would allow the company to advise on the consequential damage that may result from the warrant and give guidance on more appropriate mechanisms to meet law enforcement's needs. Fastmail said without this there was nothing stopping law enforcement compelling a

---

95 DIGI, *Submission 20,* p. 1.

96 DIGI, *Submission 20*, p. 4.

97 DIGI, *Submission 20*, p. 4.

98 Communications Alliance, *Submission 12,* p. 2.

99 Twitter, *Submission 11*, p. 8.

company to shut down their servers when they only needed to target a single account.[100]

5.99 The AIIA recommended the inclusion of a provision in the Bill mandating the formal consultation with any relevant company, service provider or related entity that will have any relevant computer or account asset accessed or investigated by authorised officers under the legislation. The AIIA said this consultation would involve formal and confidential notification that a warrant was being applied for that would require assistance from the relevant entity or network and an outline of the reasons for that warrant being sought. The AIIA said this would allow the entity or network to be on notice and consider the technical feasibility and impacts of the operation, resulting in a smooth and anticipated process of cooperation between government and the service provider.[101]

Compensation for damages

5.100 The Bill provides for losses related to the execution of the ATWs at proposed section 3ZZWA. This section has the effect of inserting Commonwealth liability for loss of or serious damage to property or personal injury as a result of subsequent court action.

5.101 Amazon Web Services recommended the Bill be amended to introduce a new immunity for online account providers in relation to the execution of ATWs in good faith. AWS recommended this for proposed section 3ZZUR of the Bill. AWS said the execution of an ATW should not result in civil liability to a person. AWS recommended this immunity be extended to civil and criminal liability, or an action or other form of proceedings for damages, in relation to an act or omission done in good faith in purported compliance with, or in the furtherance of a requirement under an ATW. [102]

5.102 The Law Council recommended amending proposed section 3ZZWA to extend statutory compensation rights to persons who suffer either direct or indirect loss, damage or injury from the execution of an ATW.[103] The Law Council said this statutory compensation right appeared to be unduly narrow and did not extend to people who suffer loss as an direct result of

---

100 Fastmail, *Submission 10,* p. 2.

101 AIIA, *Submission 17*, p. 3.

102 Amazon Web Services, *Submission 8*, p. 4.

103 Law Council of Australia, *Submission 21*, p. 28.

the execution of an ATW, even if that loss was reasonably foreseeable to the AFP or ACIC in executing the warrant.[104]

5.103 Home Affairs said there were existing important safeguards against unjustified and disproportionate loss or damage to data at proposed section 3ZZUR(8)(a) of the Bill. They said it would not be operationally feasible to guarantee that there would be no loss of or damage to data in all circumstances.[105]

Control of an account

5.104 The Bill provides that a person takes control of an online account if the person takes one or more steps that result in the person having exclusive access to the account. The Bill provides at proposed section 3ZZUL several examples of these steps including using existing account credentials to alter one or more account credentials; removing a requirement for two-factor authentication; or altering the kinds of account credentials required to access the account.

5.105 The Law Council said there was no clear justification for the specific power of 'lockout' from online accounts for the purpose of collecting evidence of an offence on top of existing computer access and data surveillance powers which already enabled the covert monitoring of a person's activities using those accounts.[106]

Restoration of an online account

5.106 The Bill provides for restoration of an online account at proposed section 3ZZUV. The effect of this section is to allow the holder of a target account to possibly operate the account after an ATW ceases to be in force, where it is lawful to do so and they are unable to do so because of the ATW.

5.107 The Law Council recommended proposed section 3ZZUV be amended to require the AFP and ACIC to take all reasonable steps to restore the account holder's access after an ATW ceases to be in force. They recommended removing the requirement in proposed section 3ZZUV(b) for the AFP or ACIC to form a view on whether it was lawful for the account holder to operate the account and instead introduce the ability to apply to an issuing authority for an exemption to the restoration obligation. They additionally

---

104 Law Council of Australia, *Submission 21*, p. 148.

105 Department of Home Affairs, *Submission 9.1*, p. 30.

106 Law Council of Australia, *Submission 21*, p. 10.

recommended requiring the AFP exercise separate powers of investigation, arrest and charge in relation to any offences that may be committed as a result of the person holding or operating the account instead of the ability to prevent restoration based on the indication of criminality.[107]

5.108 Home Affairs said existing proposed section 3ZZUV already provided that the AFP and ACIC must take all reasonable steps to restore an account holder's ability to operate their account, if it were lawful to do so.[108]

5.109 Home Affairs said this proposed section was designed on similar powers for the physical world. They provided the example of a search warrant where the return of a person's property once the investigation was no longer ongoing depended on whether holding that property was lawful.[109]

Extraterritoriality, overseas application and relationship with international laws such as the CLOUD Act

5.110 In contrast to the clear extraterritoriality provisions for DDWs and NAWs[110] the ATWs regime does not have equivalent provisions relating to extraterritoriality. Submitters raised concerns as to the possible serving of these ATWs on persons outside of Australia, or companies outside of Australia in order to give effect to the warrant.

5.111 The QCCL and others said the powers would effectively extend the reach of Australian law enforcement outside the sovereign jurisdiction of Australia with significant extraterritorial impacts. The QCCL and others said this would have Australian authorities authorise extraterritorial law enforcement operations outside the scope of their lawful jurisdiction. They said there were also due process risks for suspects located outside Australia which could jeopardise prosecutions. They recommended the setting of clear limits for the extraterritorial exercise of Australian law enforcement powers. [111]

5.112 This point was juxtaposed against the data disruption and network activity warrant powers which submissions said did not have the same ambiguity as ATWs. The Communications Alliance elaborated on this point and said:

---

107 Law Council of Australia, *Submission 21*, p. 28.

108 Department of Home Affairs, *Submission 9.1*, p. 31.

109 Department of Home Affairs, *Submission 9.1*, p. 31.

110 Bill, proposed sections 43C and 43E.

111 QCCL et al., *Submission 4*, p. 8.

> It does not seem to see any consent is required from an official or the service provider that has to be sought. That stands in contrast to the data disruption or network activity warrants, which do require that access has been granted by an appropriate consenting official in the foreign country.[112]

5.113 Fastmail recommended clarity on how the powers could be used by foreign law enforcement entities. Fastmail said there was nothing in the *Mutual Assistance of Criminal Matters Act 1987* (the Mutual Assistance Act) and Telecommunications Legislation Amendment (International Production Orders) Bill (the IPO Bill) that would obviously preclude the usage of these warrants on behalf of a participating foreign country. Fastmail queried whether these powers could be used by foreign powers to circumvent stronger data privacy protections in their own country.[113]

5.114 DIGI said the Bill raises a number of conflicts of law issues for overseas service providers and particularly those located in the United States. DIGI said there was no express provision in the Bill for a service provider to refuse to comply with a warrant on the basis of overseas laws. DIGI said further consideration of these issues was required.[114]

5.115 Twitter said the ATWs were 'divorced from standard due process requirements' and 'antithetical to core legal principles enshrined in democratic law and procedural fairness'. Twitter said they were concerned the Bill allowed law enforcement direct access to data regardless of the location of the server, without the provider being aware, and absent the agreement of a consenting official of the relevant foreign country where the warrant would be enforced.[115] Twitter said:

> If the Account Takeover Warrant is to be used to access an online account regardless of the location of the server, and executed without the knowledge of a service provider, or foreign official, then all due process requirements and safeguards that typically surround warrant processes have essentially been removed.[116]

---

112 Mrs Christiane Gillespie-Jones, Director, Communications Alliance, *Committee Hansard*, Canberra, 10 March 2021, p. 32.

113 Fastmail, *Submission 10*, p. 3.

114 DIGI, *Submission 20,* p. 6.

115 Twitter, *Submission 11*, p. 7.

116 Twitter, *Submission 11*, p. 8.

5.116 DIGI said ATWs could be used to access an online account regardless of the location of the server and without the knowledge of relevant foreign officials.[117]

5.117 Home Affairs said ATWs could be used to take control of an online account regardless of where the account data is located but the power was only available if the AFP or ACIC were investigating a relevant offence within the AFP or ACIC's functions to investigate.[118] DIGI said there was a risk of Australian law diverging from the 'robust protections for privacy and civil liberties' required entering into a CLOUD Act agreement under US law.[119]

Notification to target of ATW

5.118 The Law Council recommended amending the Bill to require the AFP or ACIC notify an account holder that their account was the subject of an ATW. The Law Council recommended amending the Bill to allow the issuing authority to authorise an order, on the application of the AFP or ACIC, to either delay or dispense with the notification requirement if satisfied on reasonable grounds that giving notification to the account holder would frustrate an investigation, or jeopardise the life or safety of any person.[120] The effect of this recommendation by the Law Council would be to introduce a positive requirement to notify the subject of an ATW, rather than inverse.

5.119 The Law Council said the absence of any notification requirement meant that an account holder could be deprived of access to their account(s) for a prolonged period of time (up to 180 days) without any information about the reasons or an ability to challenge the legality of the warrant.[121]

---

117 DIGI, *Submission 20,* p. 2.

118 Home Affairs, *Submission 9*, p. 22.

119 DIGI, *Submission 20*, p. 7.

120 Law Council of Australia, *Submission 21*, p. 28.

121 Law Council of Australia, *Submission 21*, p. 149.

Review and privacy

Administrative and judicial review of decisions

5.120 QCCL recommended the issue of the ATWs be subject of merits and judicial review with the Federal Court of Australia.[122] The AIIA recommended merits review processes.[123]

Privacy concerns (including third parties)

5.121 Fastmail said Australia's global reputation was moving away from individual rights and towards state surveillance. Fastmail said Australia was moving further away from global norms, and from the expectations of privacy protection that consumers are now demanding.[124] CSCRC said an absolute right to privacy could never exist and there would be exceptions, such as provided by this Bill.[125]

5.122 The Communications Alliance said there were privacy issues of third parties that were not the subject of ATWs. CA recommended the Bill provide protections for information that is being accessed in the course of such action but is unrelated to the crime under investigation. CA said the issuing authority should have 'regard to the privacy of any individual affected by any of the new warrants under consideration'.[126] Twitter said the Bill did not contemplate processes to protect the rights of third party users who interacted with the account subject to an ATW.[127]

5.123 Twitter said the Bill included limited safeguards but did not consider the implications of law enforcement agencies accessing a service without the knowledge of the service provider. Twitter said they had concerns about the implications for Twitter's own obligations as well as the privacy implications for the users of Twitter.[128]

---

122 QCCL et al., *Submission 4*, p. 7.

123 AIIA, *Submission 17*, p. 4.

124 Fastmail, *Submission 10*, p. 1.

125 CSCRC, *Submission 14*, p. 8.

126 Communications Alliance, *Submission 12*, p. 4.

127 Twitter, *Submission 11,* p. 7.

128 Twitter, *Submission 11*, p. 6.

5.124 DIGI said the powers could compromise the privacy of users of the service provider's digital products and it was unclear how law enforcement would mitigate against the violation of users' privacy rights. DIGI said for ATWs in particular, law enforcement would have access to all content and data not just the content and data required to complete the investigation. DIGI said there was a requirement for rules to minimise the collection, retention, and use of data that is not relevant to the investigation.[129] Telstra recommended the legislation be amended to address the issue of confidential information of non-targets.[130]

5.125 Twitter said they noted specified account holders of requests for their account information unless they were prohibited or the request fell into one of the exceptions to their user policy.[131]

5.126 The Bill provides for offences of unauthorised disclosure of protected information at proposed section 3ZZVH of the Bill. Exceptions to this proposed provision are provided by proposed section 3ZZVH(3).

Protection of account takeover technologies and methods

5.127 The Bill provides at proposed section 3ZZVK that 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 account takeover technologies or methods. It provides that the person conducting the proceeding must take into account whether the information is necessary for the fair trial of the defendant or is in the public interest.

Miscellaneous other changes

Controlled operations

5.128 The Bill amends the Crimes Act in three instances. These amendments would have the effect of removing the requirement for guaranteeing that illicit goods would be held by Australian law enforcement at the conclusion of online controlled operations. This is achieved via negative in the below amendments.

---

129 DIGI, *Submission 20*, p. 5.

130 Telstra, *Submission 16*, p. 2.

131 Twitter, *Submission 11*, p. 3.

5.129 In paragraph 15GI(2)(d) Crimes Act, before 'that the operation', insert 'so far as the conduct involved in the controlled operation is not conducted online'.

5.130 In paragraph 15GQ(2)(d) Crimes Act, before 'that the operation', insert 'so far as the conduct involved in the controlled operation is not conducted online'.

5.131 In paragraph 15GV(2)(d) Crimes Act, before 'that the operation', insert 'so far as the conduct involved in the controlled operation is not conducted online'.

5.132 The Uniting Church said these Bill provisions were 'consistent with their ability to conduct controlled operations in the physical world offline'.[132] The Law Council however recommended omitting Schedule 4 from the Bill in recognition that the issues that have given rise to the perceived need for the amendments were, in fact, capable of being managed under the existing provisions governing the authorisation of controlled operations.

5.133 The Law Council said despite the suggestion in the EM the proposed amendments were minor, they appeared to have significant legal effect to the following matters:

- The authorisation of law enforcement officers and other covert operatives to engage in activities that would otherwise constitute offences or torts, or both; and
- The exercise of discretion by a court to exclude evidence on the basis that it has been unlawfully or improperly obtained.[133]

5.134 The Law Council said this created a 'fundamental tensions with the doctrine of the rule of law' and it was no small measure to authorise agents of the state to engage in otherwise unlawful conduct and to limit the usual discretion of courts to exclude evidence obtained through such conduct.[134]

5.135 The Law Council said the existing Act did not have an absolute requirement to ensure that law enforcement agencies must, invariably, have complete control over all illicit goods at the conclusion of a controlled operation. They said the requirement was the agency must take all reasonable steps to ensure that it would be a in a position to exercise control to the maximum extent possible. They said the existing authorisation, variation and extension

---

132 Uniting Church, *Submission 13*, p. 19.

133 Law Council of Australia, *Submission 21*, p. 160.

134 Law Council of Australia, *Submission 21*, p. 160.

provisions would be suitable and it would be dependent on the applications by the AFP or ACIC.[135]

5.136 The Law Council noted the Richardson Review and said the measures in Schedule 4 of the Bill were an example of the perceived problem not being a defect in the relevant provisions of the existing Act. They said the existing provisions were a carefully designed safeguard which already took into account the issues identified in the EM.[136]

5.137 The Law Council said there were two significant risks in 'granting a wholesale exemption for online controlled operations' from the requirements of sections 15GI, 15GQ and 15GV. These were the removal of statutory obligations even where it is possible to exercise control and unintended consequences. They said in situations where law enforcement could exercise a meaningful degree of control over illicit data the proposed amendments would have the effect of relieving the agency of the legal requirement to do so. The Law Council said they were concerned that the 'wholesale exclusion' would remove any statutory obligation, and potentially a strong incentive, to use existing capabilities and powers, or pro-actively seek out or develop new ones, to exercise control over harmful or illicit content that is accessed or disseminated as part of an online controlled operation. They said the effect of this would be to make the law governing the conduct of online controlled operations 'frozen in time' to reflect present technical limitations, or perceived limitations. [137]

5.138 The Law Council said controlled operations conducted online could authorise an extremely broad range of otherwise unlawful activities, including the dissemination of a computer virus. They recommended requiring the applicant satisfying the issuing authority that they would be able to control that virus at the conclusion of the controlled operation.[138]

5.139 The Law Council recommended amending section 15HC of the Crimes Act to provide expressly that a controlled operation cannot authorise, or confer criminal immunity or civil indemnity for, activities in respect of which a DDW, or NAW is required under the SD Act (or an emergency authorisation for these activities).[139] The Law Council said they were concerned that acts

---

135 Law Council of Australia, *Submission 21*, p. 161.

136 Law Council of Australia, *Submission 21*, p. 162.

137 Law Council of Australia, *Submission 21*, p. 163.

138 Law Council of Australia, *Submission 21*, p. 163.

139 Law Council of Australia, *Submission 21*, p. 30.

done under a DDW or NAW were not clearly covered by the exclusions list of section 15HC which provides that criminal immunities and civil indemnities under Part IAB do not apply to certain conduct.[140]

5.140 Home Affairs said the Schedule 4 amendments were important for the effective operation of controlled operations online.[141]

5.141 Home Affairs said the nature of material which is likely to be the subject of a controlled operation conduct online necessarily meant that it could be much more easily forwarded, coped or transferred than was possible with physical goods.[142] Home Affairs put this amendments in context and said:

> As an example, the AFP may conduct a controlled operation to gather evidence as part of an investigation into the sale of stolen Australian identity documents on a dark web forum. The AFP might purchase those illicit goods as part of the controlled operation, but law enforcement cannot guarantee that they have purchased the only copy or that they will have all copies in their possession at the end of the operation.[143]

Minor amendments

5.142 Several minor amendments are provided for in Schedule 5 of the Bill. These amend the SD Act and the TIA Act.

140 Law Council of Australia, *Submission 21*, p. 164.

141 Department of Home Affairs, *Submission 9.1*, p. 33.

142 Department of Home Affairs, *Submission 9.1*, p. 34.

143 Department of Home Affairs, *Submission 9.1*, p. 34.

6. Committee comment

6.1 The Committee accepts evidence the threat environment from serious cyber-enabled crime is severe and Australian authorities do not currently have the tools to address the threat. It is international, complex, and technologically advanced. The Committee accepts evidence there is a requirement for powers such as these due to the effects of anonymising technology and the dark web in particular. The Committee accepts evidence serious crime is being enabled by these technologies and the Australian Federal Police (AFP) and Australian Criminal Intelligence Commission (ACIC) are currently unable to prevent the harm. The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill) is world-leading and novel but it also needs to be subject to serious consideration and review. The Committee accepts it is one among many measures being considered to counter these threats.

6.2 The Committee supports these powers and the Bill conditional on the amendments as outlined below. As identified by many submissions to this inquiry, the key issues at the micro level are the articulation and definition of necessity and proportionality with these powers. While almost all submissions generally supported the intent of the Bill, many submissions thought the Bill was either poorly defined or differed substantially from the Explanatory Memorandum (EM). On this latter point, the Committee strongly recommends Government clearly articulate these key issues in the EM as if it had done so then it is likely the inquiry process would have occurred more smoothly as people's understanding of what the Bill is would have been likely stronger. This is particularly the case for the debate on relevant offences and issuing authorities which are the two key issues from a technical and legislative perspective.

Intelligence oversight and relationship with the Integrity Measures Bill

6.3 The key issue at the macro level relates not to these powers themselves but the broader framework for intelligence oversight in Australia to which this Bill relates quite strongly to. It is at this point the relevance of the Intelligence Oversight and Other Legislation (Integrity Measures) Bill 2020 (the IM Bill) becomes apparent. As noted in evidence to this Committee there is a strong relationship between the SLAID Bill and the IM Bill as evidenced in the co-design and redundant measures implemented in both.

6.4 Currently the Inspector General of Intelligence and Security (IGIS) does not have oversight of the AFP and ACIC. Between the complementary measures of this Bill and the IM Bill, IGIS oversight is proposed for the ACIC (but not AFP) but only as it relates to the ACIC's intelligence functions. IGIS oversight could apply to the AFP in so far as it relates to a network activity warrant (NAW).

6.5 Currently the PJCIS does not have oversight of the AFP or ACIC, except for the AFP as it relates to certain terrorism functions. This point will be addressed below. Between the complementary measures of this Bill and the IM Bill, PJCIS oversight is not proposed for either the ACIC or AFP, and in particular the intelligence functions of these organisations.

6.6 The Committee is strongly of the view, firstly, that parliamentary oversight of intelligence matters should mirror integrity body (e.g. IGIS) oversight of intelligence matters. As it stands, this Bill risks creating a divergence. Secondly, the Committee is of the view that intelligence matters should be overseen by the parliamentary committee for intelligence matters – regardless of whether it is by a traditional intelligence collector (as is the case in the National Intelligence Community (NIC)) or law enforcement bodies that perform intelligence functions.

6.7 The Committee notes the issue of defining and separating ideas of intelligence and law enforcement has received substantial attention in both the Independent Intelligence Review (IIR) and the Comprehensive Review by Dennis Richardson (the Richardson Review). The Committee notes the Richardson Review differed from the IIR on the topic of oversight and the Government has in part differed from both the IIR and the Richardson Review

6.8 The Committee accepts evidence there is substantial overlap between intelligence and law enforcement matters. You can have intelligence matters that have no bearing on law enforcement and law enforcement matters that have no bearing on intelligence, but for certain agencies and most notably the ACIC and AFP this is far less likely. For the ACIC in particular they have both law enforcement and intelligence in their very title. It is hard to imagine the intelligence functions being a minor part of a body that is titled an intelligence commission.

6.9 The Committee does not believe these areas of law enforcement and intelligence were ever mutually exclusive, but it is certainly the case that the grey area between the two concepts is rapidly growing as the overlapping nature of these concepts is increased. These powers go to that increasing overlap. This causes some structural oversight issues given there is the PJCIS for intelligence, and the Parliamentary Joint Committee on Law Enforcement (PJCLE) for law enforcement. Where the Richardson Review discussed at length the differences between foreign and domestic intelligence and related topics, the issue of law enforcement powers compared to law enforcement intelligence powers has received less attention. It is possible the definition of intelligence function applied elsewhere in the NIC could apply to law enforcement agencies.

6.10 This Bill is a perfect example of something belonging equally to both parliamentary oversight bodies. The Committee notes this Bill was sent to the PJCIS for review which would imply that out of the two bodies, the PJCIS was more suited for this particular query. The Committee agrees with this suggestion. The PJCIS can receive classified hearings, is well-versed in intelligence legislation, and reviews other related matters to this Bill in particular (for example the TOLA Act). This begs the question therefore of why the PJCIS is reviewing this Bill but not being given the oversight of the very bodies it is being asked to empower. It raises the distinct possibility the Committee could authorise these powers, subject to certain provisions, and then not have the capacity to review them once the Bill becomes an Act.

6.11 IGIS oversight is not proposed for the AFP under the IM Bill, but under the SLAID Bill it is proposed for network activity warrants (NAWs) as a specific warrant type. This would have the effect of the IGIS being able to review one particular warrant within the broader AFP intelligence structure, but nothing further. Evidence given to this Committee suggested NAWs would be used in tandem with broader investigative and intelligence powers. This very evidence strengthens the Committee's view that oversight fragmentation will occur if this Bill proceeds without amendment.

6.12 If the AFP use NAWs in tandem with multiple other warranted and non-warranted powers, then the IGIS could only review the NAW-component even if other clearly intelligence-focussed powers were in use. This appears to the Committee to be an error. This is still higher than the proposed PJCIS oversight of the AFP which is limited to existing restrictions around terrorism – not NAWs at all. This does not reflect either good oversight practice or the current reality of the PJCIS reviewing AFP matters and legislation. The very existence of this Bill inquiry goes to the PJCIS role in these issues.

6.13 The Committee notes that according to the Government the PJCLE has oversight of ACIC and this is sufficient and a reason not to involve the PJCIS. The Committee is not persuaded by this argument. Firstly, the SLAID Bill was deliberately selected for PJCIS review given its experience in reviewing national security intelligence legislation in Australia, not the PJCLE. Should the SLAID Bill have been referred to the PJCLE then the Committee deliberations may have been different. Secondly, the ability of the PJCIS to conduct classified hearings makes it a better oversight body for the ACIC as it relates to intelligence functions. Thirdly the SLAID Bill is a specific intelligence power, rather than general oversight of an agency.

6.14 Already, by virtue of these inquiries occurring, there has been a divergence between the PJCIS and PJCLE. It is the view of the Committee that the correct course of action would be to extend parliamentary oversight to the PJCIS. Even if it were the case that PJCLE oversight was sufficient, the cost to increasing oversight to incorporate the PJCIS is considered to be far lower than the numerous benefits that this would bring. The Committee believes overlapping oversight is far more advantageous than fragmented oversight. Additionally, not all oversight is equal in its scope or functions.

6.15 The Committee notes the IM Bill only proposes increasing PJCIS oversight of AUSTRAC but not the two bodies (the AFP and ACIC) that the Committee has been asked to review for these powers.

6.16 More broadly this highlights a risk of matters not being dealt with appropriately and is a substantial risk. In many ways this Bill is a good test case to determine the responsibilities of the PJCLE compared to the PJCIS. The Committee is strongly of the view that the most suitable thing to do would be to have mutual areas of overlapping jurisdiction rather than potential gaps. This would be in line with the broader recommendations from the Richardson Review in avoiding fragmentation. It could then be for the PJCLE and PJCIS to decide amongst themselves who reviewed certain

matters relating to the AFP and ACIC. There is a substantial risk of oversight fragmentation as a result of this Bill. Areas of concurrent jurisdiction are supported in favour of exclusionary models that make oversight gaps more likely.

6.17 Much of the evidence to this inquiry focussed on how the Commonwealth Ombudsman and IGIS would be able to co-oversee several of these bodies, and cited evidence from the Richardson Review in favour of increased oversight that overlapped slightly rather than gaps. The Committee notes this same logic applies to parliamentary oversight as it does to Ombudsman/IGIS oversight and the logical conclusion would be to have PJCLE and PJCIS oversight of the ACIC to avoid an oversight gap. As it stands this logic has been applied to the integrity bodies but not to parliamentary committees. The Committee is not satisfied with the current parliamentary oversight of the ACIC in particular. There is far more to be gained than lost from any such extension of oversight, and it would be expected to apply in the very situation that this inquiry finds itself, a Bill review of intelligence powers.

6.18 Of note the IGIS expansion of oversight on the ACIC and AUSTRAC only applies to the statutorily defined 'intelligence functions' of those agencies. This has been deliberately selected after the Richardson Review to encompass the relevant points. This same logic applies for parliamentary oversight as well and the Committee would propose it has oversight of these same agencies so far as it relates to the 'intelligence functions' of those agencies.

6.19 As the evidence to this Committee demonstrated, these are serious and extraordinary intelligence powers that do have a relationship to the National Intelligence Community (NIC) via the Australian Signals Directorate (ASD) as evidence to this Committee showed. It is the view of the Committee that the PJCIS is the most appropriate body for reviewing intelligence legislation and that should not be limited by the current definitions that are proposed.

6.20 In summary, the Committee strongly supports and recommends parliamentary oversight mirror integrity body oversight. As it stands, this Bill would create a divergence on this issue which in the Committee's view, is unacceptable.

Recommendation 1

6.21 The Committee recommends that, in line with the proposed expansion of the Inspector-General of Intelligence and Security's oversight role, the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 and, to the extent necessary, other legislation be amended to expand the oversight remit of the Parliamentary Joint Committee on Intelligence and Security to cover the intelligence functions of the ACIC (including, but not limited to, the use of network activity warrants by the ACIC).

6.22 A related point the Committee deliberated on was parliamentary oversight of the AFP. Where the IM Bill proposes changes for ACIC oversight it does not amend AFP oversight which currently does not include the IGIS and only includes the PJCIS to the extent that the matter is a certain terrorism function (this being the existing status rather than a proposed change).

6.23 The Committee finds it unpersuasive whereby PJCIS oversight of the AFP is not proposed, but the PJCIS is asked to review intelligence powers proposed for the AFP. A component argument, that the AFP does not have considerable intelligence powers is considered weak when viewed against the very powers proposed by this Bill. There is a contradiction and oversight quagmire presented by this approach. It is the view of the Committee that if the PJCIS is reviewing intelligence legislation for the AFP, which is appropriate given the role of this Committee, then it should be formalised and expanded to realistically account for the current PJCIS activities related to the AFP.

6.24 As above, the Committee finds the argument of existing PJCLE oversight as unsatisfactory. There is more to be gained than lost by PJCLE and PJCIS having overlapping oversight of the AFP, with particular relevance for the PJCIS on intelligence matters.

6.25 The Committee is strongly of the view that amendments to both this Bill and the IM Bill are required to allow for PJCIS oversight of the AFP beyond the certain terrorism functions the PJCIS currently has oversight over.

Recommendation 2

6.26 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020) and, to the extent necessary, other legislation be amended to expand the oversight remit of the Parliamentary Joint Committee on Intelligence and Security to cover the intelligence functions of the AFP (including, but not limited to, the use of network activity warrants by the AFP).

6.27 As it stands, the PJCIS has been asked by Government to review particular powers for the AFP and ACIC without being given commensurate increases in oversight of these agencies or the explicit ability to review these powers once they are enacted into law.

6.28 The Committee notes IGIS oversight of the AFP is limited to network activity warrants (NAWs) exclusively.

Recommendation 3

6.29 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020) and, to the extent necessary, other legislation be amended to extend the oversight remit of the Inspector-General of Intelligence and Security's oversight to include all intelligence functions of the AFP (including, but not limited to, not the use of just network activity warrants).

6.30 As this section of Committee Comment shows, the vexed issue of intelligence oversight in a law enforcement context remains unaddressed despite efforts by the IIR and the Richardson Review to solve this very issue. Differing standards across different agencies on different powers by different oversight bodies is hardly ideal and not supported by this Committee.

6.31 There are substantial differences between the IGIS, the Commonwealth Ombudsman, the Australian Commission for Law Enforcement Integrity (ACLEI) the Office of the Australian Information Commissioner (OAIC) and the Australian National Audit Office (ANAO). It does not do well to equate these bodies as they have vastly different powers and mandates. Additionally, quantity of oversight does not equate to quality of oversight, if indeed some of these agencies can be classified as oversight bodies.

6.32 From a Committee perspective there is no equivalent to the oversight powers afforded by the IGIS and as it stands IGIS does not have oversight of the AFP intelligence functions nor the intelligence functions of Home Affairs. For this particular inquiry, the Committee is limiting its criticism to the lack of inclusion of operational agencies where the intelligence function is clearly present compared to policy agencies such as Home Affairs.

6.33 The Committee notes this issue will be likely relevant for the proposed Electronic Surveillance Bill proposed by the Richardson Review to consolidate and normalise all electronic surveillance powers in Australia across intelligence and law enforcement. If not now, at the point this Bill is referred (likely to this very Committee) these issues discussed above will become even more relevant. It appears the Government is moving towards a uniform and centralised piece of legislation to guide electronic surveillance. The Committee supports that endeavour in principle. It should be the case that oversight mirrors this philosophy.

6.34 In relation to oversight, given these are extraordinary powers the Committee recommends Government consider deepening the level of Commonwealth Ombudsman oversight to explore issues of propriety that the IGIS currently considers for intelligence agencies. The Committee notes the significant differences between the Ombudsman and IGIS in this regard.

Recommendation 4

6.35 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 and, to the extent necessary, other legislation be amended to expand the inspection mandate and functions of the Commonwealth Ombudsman to cover – in explicit terms – the propriety of the AFP and ACIC's actions, practices, policies and activities under these new powers.

Technology companies

6.36 The Committee invited several technology companies to public hearings and for various reasons these invitations were rebuffed, ignored or refused. The Committee notes many of these large commercial entities provided written submissions outlining their intention to support the Committee and provide additional information, but when asked to provide additional evidence at a public hearing did not see fit to do so.

6.37 The Committee is disappointed in these technology companies and notes their lack of appearance meant that the evidence base was weaker as it did not comprehensively take into account the concerns of technology providers on these issues. The Committee strongly recommends these companies appear in the future, and not in the form of industry lobby groups. It is not good practice to criticise a Bill but then not turn up to a hearing to discuss said Bill.

Submissions

6.38 The Committee thanks all the submitters to this inquiry and those who appeared before the Committee. The level of detail in many submissions was comprehensive and addressed specifically the proposed sections of the Bill. The Committee particularly thanks those who addressed the Bill itself and the proposed sections within it.

6.39 The Committee notes the ACIC, while seeking these new and extraordinary powers and being one of only two bodies proposed to be receiving these powers, did not submit a standalone submission to this inquiry justifying their need of these powers until asked by the Committee to provide at a public hearing. Given the above comments regarding perceived lack of oversight of the ACIC, the ACIC then not initially providing a submission to the Committee only strengthened the Committee's view that oversight of the ACIC is substantially lacking. The Committee thanks the ACIC for its subsequent submission it made at the Committee's request.

6.40 The Committee acknowledges the ACIC position was incorporated within the Home Affairs portfolio submission but this is neither adequate nor persuasive. The Committee required justification for why particular agencies required particular powers. The AFP provided that justification clearly and persuasively – initially the ACIC did not and only provided such justification at the Committee's request.

6.41 The Committee recommends agencies that are seeking warranted powers provide their own submissions to this Committee. Doing so assist the Committee in providing justification for enabling the agency to receive said powers. This was particularly the case with the topic of disruption which was subject of substantial focus in the Richardson Review.

Recommendation 5

6.42 The Committee recommends that, where a Bill proposes to give operational or intelligence agencies specific new or expanded powers, those agencies should, in addition to providing input to any departmental submission, provide a separate unclassified submission to the Committee which should, at least, outline the necessity and proportionality of the proposed new or expanded powers. Such a submission should include, where appropriate, case studies on the current environment and how the use of any proposed new or expanded powers will assist the agency in the carrying out of its functions.

The Committee also recommends that the Department of Home Affairs not make any further submission to the Committee that purports to be authored by, or submitted on behalf of, the "Home Affairs Portfolio".

For the avoidance of doubt this recommendation should not preclude an agency providing a classified submission in addition to any unclassified submission.

Mandate for disruption

6.43 The Committee accepted evidence from the AFP and ACIC that articulated clearly their mandate for disruption and the relationship between disruption and prosecution. These powers have been clearly demonstrated in the offline world and this Bill enables these agencies to attempt to do the same in the online world.

6.44 As above, the disruption mandate lends itself to a stronger focus on intelligence powers which is clearly the domain of the PJCIS.

Issues related to all powers

6.45 Committee comment for this Bill is divided between issues universal (or near-universal) to all powers, and issues that are specific to the particular warrant types.

The proposed Electronic Surveillance Act

6.46 The Committee considered how this particular Bill would be placed within the broader recommendations recommended by the Richardson Review. In particular the Committee notes the proposal for a omnibus Electronic

Surveillance Act and evidence by Home Affairs that work is being undertaken to implement this proposal. The Committee is very supportive of any legislative attempt to increase consistency, accountability and transparency around the application of these types of intrusive powers and will take an ongoing interest in the Electronic Surveillance Act.

Additional reporting

6.47 The Committee noted concerns that while these powers were justified in terms of being used for particularly serious offences they could be used for lesser offences. It is of considerable importance to the Committee that powers are used for the purposes they are outlined for. To provide assurance the Committee is recommending a report be provided each year to Parliament and the Committee outlining the specific offences that these powers were used for. Such a report will greatly assist the Committee's consideration of whether or not to conduct a statutory review of the powers discussed below.

Recommendation 6

6.48 The Committee recommends that, in support the proposed expansion of the Parliamentary Joint Committee on Intelligence and Security's oversight remit (see Recommendations 1 and 2), the AFP and the ACIC provide an unclassified annual report to the Committee which sets out:

- **to the extent it is possible to do so in an unclassified report, similar information to what is required to be provided under section 3ZZVL of Schedule 3 of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (except that information should be provided in respect of all three of the new powers rather than just the account takeover warrants); and**

- **the offences in respect of which the warrants were sought or obtained.**

This new reporting requirement should be supplemented by classified briefings to the Committee outlining the use of the new powers and their relationship both to each other and other existing powers provided to the AFP and ACIC.

Review by the Independent National Security Legislation Monitor

6.49 The Committee accepts that the warrants outlined in the Bill will most liklely be used for law enforcement matters. However there is, equally, a national security element to the proposed use of the warrants. On this basis the the Committee recommends the Data Disruption, Network Activity and Account Takeover warrants be subject to review by the Independent National Security Legislation Monitor (INSLM) three years after the Bill gains assent. The Committee further recommends that a copy of the INSLM's report be provided to this Committee.

Recommendation 7

6.50 The Committee recommends the INSLM Act be amended to provide for INSLM review of the data disruption, network activity and account takeover warrants introduced by the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 within three years of the Bill receiving Royal Assent.

The Committee further recommends that the INSLM Act be amended to require the INSLM to provide a copy of his or her report to the Committee at the same time the report is provided to the Minister.

Statutory review

6.51 The Committee notes the powers are limited to certain agencies, the AFP and ACIC, and this provides the Committee with a high degree of assurance that they will be used appropriately and within a set scope.

6.52 However, it is the usual practice of the Committee to recommend that it undertake a statutory review into the operation, effectiveness and implications of recently legislated new powers.

6.53 Such a power of review provides the Parliament with additional assurance that the powers are being used as intended for relevant and serious offences the Committee is recommending the Committee be given the ability to elect to review this Bill at least three years after assent. The Committee is deliberately recommending that such a review be optional as the reporting by AFP, ACIC and the INSLM referred to above and any briefings the Committee may request may provide the Committee with the assurance that a formal statutory review is not needed.

6.54 In addition the Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that powers sunset five years from when the Bill receives Royal Assent.

Recommendation 8

6.55 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the Parliamentary Joint Committee on Intelligence and Security may conduct a review of the data disruption, network activity and account takeover warrants not less than four years from when the Bill receives Royal Assent to allow the Committee to take into account any report by the INSLM.

In addition the Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that each of the new powers sunset five years from the date on which the Bill receives Royal Assent.

Issuing authority

6.56 One of the major issues identified by submissions to this inquiry related to the issuing authority of the three powers and what would be appropriate. Generally this came in the form of submitters recommending raising the account takeover warrant (ATW) issuing authority to be in line with network activity warrants (NAWs) and data disruption warrants (DDWs) (at minimum), and recommending raising NAWs and DDWs further to superior court judges alone.

6.57 The Committee heard no compelling evidence, beyond administrative coherence with existing powers, for not raising the issuing authorities and as such is recommending that the Bill be amended so that the issuing authority for all three new powers, including emergency authorisations, is a superior court judge except for Account Takeover Warrants which may be granted by an Eligible Judge per *Section 12 of the Surveillance Devices Act 2004* (Cth). These are extraordinary powers and the issuing process should reflect this.

Recommendation 9

6.58 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the issuing authority for all of the new powers introduced by the Bill, including emergency authorisations, must be a superior court judge (either of the Federal Court

or a State or Territory Supreme Court), except for Account Takeover Warrants which may be granted by an Eligible Judge per *Section 12 of the Surveillance Devices Act 2004* (Cth).

Issuing criteria

6.59 The Committee accepted evidence from Home Affairs that the issuing authority criteria sufficiently narrowed the scope of these powers The Committee, after accepting evidence from several submissions, recommends that these criteria can be refined further to provide assurance that the powers will be used for appropriate offences.

Recommendation 10

6.60 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to provide additional requirements on the considerations of the issuing authority to ensure the offences are reasonably serious and proportionality is maintained. The effect of any changes should be to strengthen the issuing criteria and ensure the powers are being used for the most serious of offending.

- **This should include specific consideration as to whether the offending relates substantially to: offences against the security of the Commonwealth per Chapter 5 of the Criminal Code; offences against humanity including child exploitation and human trafficking per Chapter 8 of the Criminal Code; serious drug, weapons and criminal association offences per Chapter 9 of the Criminal Code; and money laundering and cybercrime offences per Chapter 10 of the Criminal Code. These examples are not exhaustive, but designed to reflect the intention of the Bill as seen through the Explanatory Memorandum and evidence to this Committee.**

- **This should include the nature of the offending and its relationship to other serious offences.**

Recommendation 11

6.61 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the issuing authority, to the extent known, must consider the following:

- **consideration to third parties specifically, including their privacy;**

- **specific consideration of privileged and journalistic information; and,**

- **specific consideration of privacy impacts, financial impacts, and the ability of individuals to provide or receive care.**

Relevant offences

6.62 The second major issue was the discussion around relevant and applicable offences for the three powers. This was an area of serious debate with many non-governmental organisations arguing that the scope of relevant offences meant that many 'non-serious' offences, or offences not mentioned in the EM, were included in the Bill. Government organisations argued the definition of relevant offence was already set by Parliament and this Bill simply sought to use it as a definition, as did many other warrants. The EM clearly articulated that these powers would be used for the most serious types of crime and it is important the Bill reflects that.

6.63 The Committee notes the nuanced relationship between offences and powers which evolve over time. New powers are introduced to address new and serious threats which by their very definition tend to be more significant and extraordinary. There is the risk of a lag if new powers are introduced with no substantial changes to the existing architecture of legislation to which they apply. It is for this reason the Committee is generally unpersuaded by arguments of legislative consistency or coherence when extraordinary powers are introduced. Increases in powers afforded to agencies like the ACIC and AFP should be matched by increases in accountability, oversight and other measures designed to constrain and restrict these powers towards their appropriate purpose.

6.64 The Committee explored alternatives and possible recommendations including raising the threshold or specifically listing offences. For various reasons, the Committee considers it unfeasible to recommend either of these options. It appears that the issue of 'relevant offence' is a broader issue than this particular Bill and likely not one that will be addressed via this inquiry. The Committee notes that this is an issue that will need to be addressed as it will become increasingly difficult to 'tack on' new and intrusive powers to old definitions. At some point the definitions themselves will require review and it is possible we are fast approaching that point.

6.65 While the EM itself said the powers would be used for the most serious of offences, it clearly became apparent at the hearing that the powers would also be used for 'lesser' offences. The most obvious example provided

related to outlaw motorcycle gangs and the possible intention to use these powers to degrade these networks by attacking their periphery. Some comparisons can possibly be drawn between this strategy and Al Capone being charged with tax evasion. The argument being that law enforcement would go after minor offending being done by serious criminals as a way to move upstream to the more serious offending. The Committee found this argument persuasive.

6.66 As a general point the Committee notes the argument of legislative consistency is supportive but not determinative of a particular outcome. The Committee considers that arguing for something simply because it is consistent with existing legislation is not entirely persuasive when new legislation or powers are being implemented or considered.

6.67 The Committee does recommend the Government clarify the EM as addressing this specific issue was clearly lacking in the EM as identified by many submissions. Whilst Government subsequently provided arguments to this Committee as to why the definition was appropriate, this could have been addressed at the EM stage of this Bill and in not doing so, likely delayed the progression of these powers. The EM clearly set out that these powers were being used for serious crime, but the evidence given to this Committee in Hansard indicated the powers would also be used to target minor offences that serious criminals were undertaking – a clear distinction from the EM itself. Additionally the EM contained an error regarding to human rights compatibility that was subsequently addressed by Home Affairs.

6.68 Importantly this Bill does not define relevant offence, it is a creature of existing legislation and as such it would be inappropriate for this Committee to address it as a substantial issue for recommendations to apply to. The Committee accepted evidence that a dynamic category was required to ensure operational efficacy of the Bill. However, the issues raised by submissions need to be addressed and as such the Committee recommends the Government undertake a broad review of offence classifications to address the concerns identified by these submissions. It may be that new categories are required to provide assurance to the public that extraordinary powers are not being used for ordinary offences.

6.69 The Committee recommends much greater attention be placed to justifying the 'relevant offences' for powers such as these in the future. Arguments of internal legislative coherence are not satisfactory for extraordinary powers such as these. The Committee is satisfied that the issuing authority criteria

suitably narrows the *de facto* 'relevant offences'. The Committee notes that rather than relying on issuing authorities judgement it is much more preferable that legislation is clear as to which offences are captured by proposed powers. For these reasons several recommendations are outlined below.

6.70 The Committee notes that it is probable the Government will address the issue of relevant offences and definitions with the creation of the proposed Electronic Surveillance Act.

Recommendation 12

6.71 The Committee recommends the Government commission a review of Commonwealth legislation to determine whether the concepts of "serious offence", "relevant offence" and other similar concepts:

- **should be made consistent across different Acts of Parliament (noting that, for example, the definition of "serious offence" in the Telecommunications (Interception and Access) Act 1979 is different to the definition of "relevant offence" in the *Surveillance Devices Act 2004*; and**

- **whether the threshold for the concept of "serious offence" in all Commonwealth legislation should be – at a minimum – an indictable offence punishable by a maximum penalty of seven years' imprisonment or more, with a limited number of exceptions.**

This body of work should inform the eventual electronic surveillance bill being considered by the Department of Home Affairs and other departments.

Emergency authorisations

6.72 The Committee considered the possible scenarios where emergency authorisations are not subsequently ratified by the issuing authority. In these situations the Committee recommends the issuing authority have discretion to order remedial action as appropriate.

Recommendation 13

6.73 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that, in order to provide an emergency authorisation for disruption of data held in a computer:

- **in addition to the matters set out in proposed section 28(1C) of the *Surveillance Devices Act 2004*, an authorising officer must be satisfied that that there are no alternative means available to prevent or minimise the imminent risk of serious violence to a person or substantial damage to property that are likely to be as effective as data disruption; and**

- **the authorising officer must consider the likely impacts of the proposed data disruption activity on third parties who are using, or are reliant on, the target computer and be satisfied that the likely impacts on third parties are proportionate to the objective of the emergency authorisation.**

In addition, the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 should be amended so that, where an issuing authority declines to retrospectively approve an emergency data disruption authorisation, the issuing authority may require the AFP or ACIC to take such remedial action as considered appropriate in the circumstances, including financial compensation.

Requesting officers and public interest advocates

6.74 The Committee noted evidence recommending amending the Bill so that only certain officers could apply for these warrants within the AFP and ACIC. The Committee disagrees with this suggestion and is content with the sub-legislative provisions and policies that ensure accountability for this process within both agencies.

6.75 The Committee noted evidence recommending the inclusion of a public interest advocate to act as contradictors in these warrant applications. The Committee does not support this recommendation for this Bill.

Concealment powers

6.76 The Committee is of the view that concealment activities that cannot be completed within 28 days should require the approval of a superior court judge to undertake post-concealment activities at a later date.

Recommendation 14

6.77 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that any post-warrant concealment powers must be exercised within 28 days after the relevant warrant has expired unless the AFP or the ACIC (as applicable) has obtained the approval of a superior court judge to undertake post-concealment activities at a later date.

Consistent with the recommendation made by the INSLM, the superior court judge should be required to consider:

- **how the AFP or the ACIC (as applicable) is proposing to conceal access;**
- **the likely privacy implications at the time and in the place where the concealment activity is proposed to occur; and**
- **whether, in all the circumstances, the concealment activity is appropriate.**

In addition, and noting that the Committee did not receive evidence on concealment in relation to computer warrants, the Committee recommends that the Government consider whether the same amendment should be made in respect of computer access warrants in the *Surveillance Devices Act 2004* consistent with the recommendation made by the INSLM.

Loss or damage to a third-party

6.78 The Committee considered the fact that integrity body oversight of this Bill, would be by both the Inspector General of Intelligence and Security and the Commonwealth Ombudsman. The Committee is satisfied with the integrity body oversight arrangements of this Bill with only several minor recommendations, some of which have been addressed elsewhere.

Recommendation 15

6.79 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that:

- **for the purposes of proposed paragraphs 27KE(7)(b) and 27KE(12) (and any other relevant provision), a data disruption warrant may only authorise the AFP or ACIC to cause material loss or damage to other persons lawfully using a computer if the loss or damage is necessary to do one of the things specified in the warrant (i.e. it is not enough that the loss or damage is "justified and proportionate"); and**

- **the AFP and ACIC must notify the Commonwealth Ombudsman or IGIS (as appropriate) as soon as reasonably practicable if they cause any loss or damage to other persons lawfully using a computer.**

The notification to the Commonwealth Ombudsman or IGIS (as applicable) must include, among other things, details of the loss or damage caused by the disruption activity and an explanation of why the loss or damage was necessary to do one of the things specified in the warrant.

Recommendation 16

6.80 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the power to temporarily remove computers and other things from premises under a data disruption warrant or a network activity warrant must be returned to the warrant premises as soon as it is reasonably practicable to do so.

Reporting to the Ombudsman

6.81 The Committee notes that the Commonwealth Ombudsman recommended varying the reporting requirements from six-monthly to annually. The Committee recommends implementing this change.

Recommendation 17

6.82 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 should be amended to change the reporting requirements from the agencies to the Commonwealth Ombudsman from six-monthly to annually.

Press freedom

6.83 The Committee noted the previous recommendation it made in the Inquiry into Press Freedoms regarding expanding the role of the Public Interest Advocate for all warrant related provisions that could relate to journalists. The Committee continues to support these recommendations and notes the Government's current ongoing holistic analysis of all legislation that will implement these changes.

Recommendation 18

6.84 The Committee recommends that the Government introduce legislation to implement the Committee's recommendations in its report on press freedom as soon as possible.

In the meantime, the Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that the issuing criteria for each of the proposed new powers requires the applicant, and the issuing authority, to consider the following matters in respect of any warrant that relates to – or may affect – a person working in a professional capacity as a journalist or a media organisation:

- **the public interest in preserving the confidentiality of journalist sources; and**

- **the public interest in facilitating the exchange of information between journalists and members of the public to facilitate reporting of matters in the public interest.**

Recommendation 19

6.85 Consistent with Recommendation 2 of the Committee's report on press freedom, the Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to require that – with respect to an application for a data disruption warrant, a network activity warrant or an account takeover warrant that is being sought in relation to a journalist or media organisation – a "public interest advocate" be appointed.

Assistance orders

6.86 Several submissions discussed assistance orders for the powers. A general theme which was present was that the assistance order regime from the TOLA Act was more developed and comprehensive and this Bill would do well to reflect key definitions and concepts from that Bill.

6.87 Several submissions called for mandatory consultation with technology providers prior to warrants being issued, or executed, and for an independent technical advisory board as part of the issuing process. The Committee disagrees with both of these suggestions for this particular Bill. The Committee is supportive of greater technical considerations being placed into the issuing authorities' considerations but is not supportive of involving technology companies at this stage of the process.

6.88 The Committee accepted evidence from submissions in favour of the assistance order regime in the TOLA Act and accepted evidence that the assistance order regime under the Bill should be modelled, in so far as it is possible to do so, on the TOLA Act assistance order regime.

Recommendation 20

6.89 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to make clear the issuing criteria for an assistance orders also requires the issuing authority to be satisfied that:

- **the order for assistance – and not just the disruption of data – is:**
  - **reasonably necessary to frustrate the commission of the offences that are covered by the disruption warrant; and**

- **justifiable and proportionate, having regard to (i) the seriousness of the offences that are covered by the disruption warrant and (ii) the likely impacts of the data disruption activity on the person who is subject to the assistance order and any related parties (including, if relevant, the person's employer) and (iii) the likely impacts of the data disruption activity on other persons, including lawful computer users or clients of the person subject to the order; and**

- **compliance with the request is practicable and technically feasible (noting that these criteria are to be found in the industry assistance measures introduced by the Assistance and Access Act 2018).**

6.90 Some submissions discussed the possibility of 'forum shopping' for assistance orders under various other regimes. To avoid this, the Committee is recommending provisions be inserted into the Bill to prevent this from occurring.

Recommendation 21

6.91 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to require consideration by the issuing authority, to the extent that is possible, of whether a person is, or has been, subject to other mandatory assistance orders (including mandatory assistance orders made under other Commonwealth legislation).

Having regard to the covert nature of mandatory assistance orders, and the fact that it may not be possible for the issuing authority or applicant to have knowledge of previous (or even concurrent) orders, the Committee further recommends that the Government develop a mechanism to ensure that individuals and companies are not subject to multiple mandatory assistance orders unless specific consideration is given to whether, in all of the circumstances, it is reasonably necessary and proportionate.

6.92 There were substantial concerns raised by the submissions to this inquiry that the assistance order framework was unnecessarily large and it could compel assistance from anyone for any purpose. The Committee supports narrowing the scope to be in line with what Government intends with this Bill, in so far as it is reasonable to do so. The Committee is satisfied that the duration of the assistance is already limited by the duration of the

underlying warrant to which the assistance order relates to (i.e. assistance orders could not outlast the underlying warrants).

6.93 The Committee heard substantial evidence on the topic of assistance orders across the three new proposed powers. Some were concerned around the lack of perceived scope in these orders.

Recommendation 22

6.94 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to:

- **impose a maximum period during with a non-emergency mandatory assistance order may be served and executed (and if the order is not served and executed within that period, the order will lapse and a new order must be sought);**
- **require all applications for a non-emergency mandatory assistance order to be made in writing;**
- **require all applications for a non-emergency mandatory assistance order to include, to the extent known key particulars, including the nature of the mandated assistance;**
- **prohibit the AFP and the ACIC, unless absolutely necessary, from seeking a non-emergency mandatory assistance order in respect of an individual employee of a company (i.e. assistance should only ever be sought from the company or business);**
- **set out the process that must be followed in respect of the service of a non-emergency mandatory assistance order on the specified persons, and link the commencement of an order to the date and time of service; and**
- **require that an issuing authority consider whether a person is, or has been subject, to a non-emergency mandatory assistance orders (including mandatory assistance orders made under other Commonwealth legislation).**

Recommendation 23

6.95 The Committee recommends that the Government make clear that no mandatory assistance order, including those defined in the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, can ever be executed in a manner that amounts to the detention of a person.

6.96 Several submissions recommended good faith immunity provisions be included for persons assisting with assistance orders. The Committee supports this.

Recommendation 24

6.97 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to introduce good faith immunity provisions for both assisting entities and those employees or officers of assisting entities who are acting in good faith with an assistance order.

Judicial review

6.98 The Committee notes the evidence provided by Home Affairs that there was an error regarding judicial review of in the initial submission and this will be corrected.

Recommendation 25

6.99 The Committee recommends the Explanatory Memorandum to the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to make it clear that decisions under the proposed new powers are not excluded from judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act).

For the avoidance of doubt, the Committee believes that no decision made in relation to data disruption warrants, network activity warrants and account takeover warrants should be exempt from judicial review under the ADJR Act.

Data Disruption Warrants

6.100 The Committee considered the Law Council's submission that the terms 'disruption' of data and 'frustration' of the commission of an offence be

statutorily defined. Whilst the Committee accepts the arguments by Home Affairs against further defining these terms, it recommends increasing the considerations built into the authorisation process.

Recommendation 26

6.101 The Committee recommends proposed paragraph 27KA(3)(b) of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to provide that the statement of facts and grounds accompanying all applications for data disruption warrants must specify the following matters to the extent that is possible:

- **the acts or types of acts of data disruption that are proposed to be carried out under the warrant;**
- **the anticipated impacts of those specific acts or types of acts of disruption on the commission of the relevant offence (that is, how they are intended to frustrate that offence); and**
- **the likelihood that the relevant acts or types of acts of disruption will achieve that objective.**

6.102 In addition the Committee makes the following recommendations.

Recommendation 27

6.103 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that only individuals who satisfy the following requirements may apply for a data disruption warrant or an account takeover warrant:

- **the person is a law enforcement officer in relation to the AFP or ACIC (as applicable) within the meaning of section 6A of the *Surveillance Devices Act 2004*;**
- **the person has been individually approved, by written instrument made by the AFP Commissioner or ACIC CEO (as applicable) to apply for data disruption warrants; and**
- **the relevant agency head is satisfied that the person possesses the requisite skills, knowledge and experience to make warrant**

applications, and the person has completed all current internal training requirements for making such applications.

Recommendation 28

6.104 The Committee recommends that paragraph 27KC of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended so that, rather than a judge having to be satisfied, that a data disruption warrant would be "justifiable and proportionate", the judge must be satisfied, to the extent possible at the time an application is made, that a data disruption warrant is:

- **reasonably necessary to frustrate the commission of the offences referred to in the warrant application; and**
- **proportionate, having regard to:**
  - **the specific nature of the proposed disruption activities;**
  - **the proportionality of those activities to the suspected offending;**
  - **the potential adverse impacts of the disruption activities on non-suspects; and**
  - **the steps that are proposed to be taken to avoid or minimize those adverse impacts, and the prospects of those mitigating steps being successful.**

6.105 The Committee considered the involvement of Australian Signals Directorate (ASD) officers in these powers and, to ensure no gaps in oversight by the IGIS recommends that the IGIS Act be amended to provide that staff members of the Australian Signals Directorate are subject to IGIS oversight if they are seconded to the AFP or ACIC to execute a data disruption warrant for and on behalf of the AFP or ACIC.

Recommendation 29

6.106 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 and the IGIS Act be amended to make it clear that staff members of the Australian Signals Directorate are subject to IGIS oversight if they are seconded to the AFP or ACIC to execute a data disruption warrant for and on behalf of the AFP or ACIC.

Network Activity Warrants

6.107 A key issue was the definition of 'criminal network of individuals'. At the most extreme, some submissions argued it could apply to all users of WhatsApp.[1] The Government response, which this Committee agrees with, is that the issuing authority requirements make this increasingly unlikely. Furthermore, the efficacy of narrowly defining this term could lead to operational inefficiencies. However, there are likely some improvements which could be made to this definition.

6.108 The definition should include consideration of the actions or intentions of the group as a whole, and the possible offending being undertaken by the group as a whole as well as the severity of that offending. It is important that some nexus between the type of offending and the type of group is present to narrow the scope of these warrants while maintaining the intelligence function.

Recommendation 30

6.109 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to strengthen the issuing authority considerations for network activity warrants, including by amending the definition of a "criminal network of individuals" to require there to be a reasonable suspicion of a connection between:

- **the suspected conduct of the individual group member in committing an offence or facilitating the commission of an offence; and**
- **the actions or intentions of the group as a whole.**

6.110 The Committee agrees with the IGIS submission and evidence on clarifying the importance of privacy considerations in the issuing authority criteria for NAWs at proposed section 27KM.

Recommendation 31

6.111 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to clarify that a decision-

[1] Mr Kieran Pender, Human Rights Law Centre, *Committee Hansard*, 10 March 2021, p. 9.

maker, and the issuing authority, must consider the privacy implications to the extent they are known, of a proposed network activity warrant.

To be clear, the committee does not believe that privacy considerations should be determinative in their own right, just that they should be considered.

Account Takeover Warrants

6.112 The Committee considered several issues in relation to Account Takeover Warrants (ATWs). The Ombudsman recommended that affidavits support ATW applications. The Committee agrees with this recommendation.

Recommendation 32

6.113 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to require a sworn affidavit setting out the grounds of an application for an account takeover warrant (consistent with the delayed notification search warrants in the *Crimes Act*).

Recommendation 33

6.114 The Committee recommends that the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be amended to require an issuing authority to consider, to the extent that is possible at the time the application is made, whether a proposed account takeover warrant is likely to have an adverse impact on third parties, including a specific requirement to assess the likely:

- **impacts on personal privacy;**
- **financial impacts on individuals and businesses;**
- **impacts on a person's ability to conduct their business or personal affairs; and**
- **impacts on a person's ability to have contact with family members or provide or receive care.**

Recommendation 34

6.115 The Committee recommends the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 be passed, subject to the amendments outlined above.

Senator James Paterson
Chair

4 August 2021

A. Submissions

1 Mr Paul Templeton

2 Carly Ryan Foundation

- 2.1 Supplementary to submission 2

3 NSWCCL

4 Queensland Council for Civil Liberties, Liberty Victoria, Electronic Frontiers Australia, Australian Privacy Foundation

5 Commonwealth Ombudsman

- 5.1 Supplementary to submission 5

6 Australian Federal Police

- 6.1 Supplementary to submission 6

7 Police Federation of Australia

8 Amazon Web Services

9 Department Of Home Affairs

- 9.1 Supplementary to submission 9

10 Fastmail Pty Ltd

11 Twitter

12 Communications Alliance

- 12.1 Supplementary to submission 12

13 Uniting Church in Australia, Synod of Victoria and Tasmania

- 13.1 Supplementary to submission 13

14 Cyber Security Cooperative Research Centre

- 14.1 Supplementary to submission 14

15 Human Rights Law Centre

16 Telstra

17 Australian Information Industry Association

18 Inspector-General of Intelligence and Security

- 18.1 Supplementary to submission 18

19 Office of the Australian Information Commissioner

20 Digital Industry Group Inc.

21 Law Council of Australia

- 21.1 Supplementary to submission 21

22 *Name Withheld*

23 Australian Criminal Intelligence Commission

B. Witnesses appearing at the Public Hearing

Wednesday, 10 March 2021

Committee Room 2R1

Canberra

Law Council of Australia

- Dr Jacoba Brasch QC, President
- Dr David Neal SC, Co-Chair national Criminal Law Committee
- Mr Tim Game SC, Member National Criminal Law Committee (Via Teleconference)
- Dr Natasha Molt, Director of Policy, Policy Division

Human Rights Law Centre

- Mr Kieran Pender, Senior Lawyer

Uniting Church in Australia, Synod of Victoria and Tasmania

- Dr Mark Zirnsak, Senior Social Justice Advocate

Carly Ryan Foundation (Via Teleconference)

- Ms Sonya Ryan, CEO and Founder

Cyber Security Cooperative Research Centre

- Ms Rachael Falk, Chief Executive Officer
- Ms Anne-Louise Brown, Head of Corporate Affairs

Communications Alliance (Via Teleconference)

- Mr John Stanton, CEO
- Ms Christiane Gillespie-Jones, Director Program Management
- Mr Patrick Fair, Chair Communications Alliance Communications Security Reference Panel

Commonwealth Ombudsman

- Mr Michael Manthorpe PSM, Commonwealth Ombudsman
- Ms Penny McKay, Deputy Ombudsman
- Ms Emma Cotterill, Senior Assistant Ombudsman, Assurance Branch
- Ms Louise Cairns, Director

Inspector-General of Intelligence and Security

- The Hon Dr Christopher Jessup QC, Inspector-General of Intelligence and Security
- Ms Bronwyn Notzon-Glenn, Acting Deputy Inspector-General of Intelligence and Security
- Mr Sol Heredia, Assistant Director Legal

Department Of Home Affairs

- Ms Cath Patterson, Deputy Secretary Strategy & Law Enforcement
- Mr Andrew Warnes, A/g First Assistant Secretary Electronic Surveillance Reform Taskforce
- Ms Rebecca Vonthethoff, A/g Assistant Secretary National Security Policy Branch

Australian Federal Police

- Commissioner Reece Kershaw APM
- Deputy Commissioner Ian McCartney, Deputy Commissioner Investigations
- Commander Douglas Boudry, Commander Covert & Technical Operations
- Commander Christopher Goldsmid, Commander Cybercrime Operations
- Superintendent Robert Nelson, Superintendent Digital Surveillance Collection

Australian Criminal Intelligence Commission

- Mr Michael Phelan, Chief Executive Officer

Australian Signals Directorate

- Ms Rachel Noble PSM, Director-General
- Ms Abigail Bradshaw CSC, Head of the Australian Cyber Security Centre
- Mr Stephen McGlynn, First Assistant Director-General General Counsel
- Mr Karl Hanmore, First Assistant Director-General Cyber Security Services

C. Relevant offences

This section is provided to illustrate how relevant offences are considered within the Act. It is designed to assist illuminate the relevant offences to which the various proposed powers apply as it was a considerable source of debate throughout the inquiry process.

For the purposes of Network Activity and Data Disruption Warrants

Network activity warrants (NAWs) and data disruption warrants (DDWs) apply to relevant offences which are defined in the *Surveillance Devices Act* 2004 (the SD Act). This includes:

- An offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of three years or more or for life; or
- An offence against a law of a State that has a federal aspect and that is punishable by a maximum term of imprisonment of three years or more or for life; or
- An offence against section 15 of the *Financial Transaction Reports Act 1988*; or
- An offence against section 53, 59, 139, 140 or 141 of the *Anti-Money Laundering and Counter-Terrorirsm Financing Act 2006*; or
- An offence against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991*; or
- An offence against section 46A, 46C, 46D, 49A or 51A of the *Torres Strait Fisheries Act 1984*; or
- If a surveillance device 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

- An offence that is prescribed by the regulations.

The first two categories listed about are substantially the same as the definition provided below for account takeover warrant (ATW) applicable offences.

For the purposes of Account Takeover Warrants

This warrant applies to relevant offences which are serious Commonwealth offences or serious State offences that have a federal aspect.

A serious Commonwealth offence and serious State offence has the same meaning under the proposed Bill as Part IAB of the Crimes Act which relates specifically to controlled operations. This is further defined at section 15GE of Division 1 of Part IAB of the Crimes Act. Specifically section 15GE of the Crimes Act provides:

Meaning of serious Commonwealth offence

1 For the purposes of this Part, *serious Commonwealth offence* means a Commonwealth offence that:

a. Involves a matter mentioned in subsection (2); and

b. Is punishable on conviction by imprisonment for a period of 3 years or more.

2 The matters are as follows

a. Theft;

b. Fraud;

c. Tax evasion;

d. Currency violations;

e. Controlled substances;

f. Illegal gambling;

g. Obtaining financial benefit by vice engaged in by others;

h. Extortion;

i. Money laundering;

j. Perverting the course of justice;

k. Bribery or corruption of, or by, an officer of the Commonwealth, of a State or of a Territory;

l. Bankruptcy and company violations;

m. Harbouring of criminals;

n. Forgery (including forging of passports);

o. Armament dealings;

p. Illegal important or exportation of fauna into or out of Australia;

q. Espionage, sabotage or threats to national security;

r. Misuse of a computer or electronic communications;

s. People smuggling;

t. Slavery;

u. Piracy;

v. The organisation, financing or perpetration of sexual servitude or a sexual offence against a person who is under 18 outside Australia;

w. Dealings in child abuse material;

x. Importation of prohibited imports;

y. Exportation of prohibited exports;

z. Violence;

aa. Firearms;

bb. A matter that is of the same general nature as a matter mentioned in one of the preceding paragraphs;

cc. A matter that is prescribed by the regulations for the purposes of this paragraph.

3 Without limiting subsections (1) and (2), an offence against one of the following provisions of the *Criminal Code* is a *serious Commonwealth offence* for the purposes of this Part:

a. Part 5.3 (Terrorism);

b. Division 273A (Possession of child-like sex dolls etc.);

c. Subdivision B of Division 471 (Use of postal or similar service involving sexual activity with person under 16);

d. Subdivision D of Division 474 (Use of carriage service for child abuse material);

e. Subdivision F of Division 474 (Use of carriage service involving sexual activity with person under 16).

Meaning of serious State offence that has a federal aspect

4 For the purposes of this Part, *serious State offence that has a federal aspect* means a State offence that has a federal aspect and that would be a serious Commonwealth offence if it were a Commonwealth offence.

Federal aspect is defined at section 3AA of the Crimes Act. This includes section 3AA(1):

1 For the purposes of this Act, a State offence has a *federal aspect* if, and only if:

a. Both:

i. The State offence is an ancillary offence that relates to a particular primary offence; and

ii. Assuming that the provision creating the primary offence had been enacted by the Parliament of the Commonwealth instead of by the Parliament of the State – the provision would have been a valid law of the Commonwealth; or

b. Both:

i. The State offence is ancillary offence that relates to a particular primary offence; and

ii. Assuming that the provision creating the primary offence had been enacted by the Parliament of the Commonwealth instead of by the Parliament of the State – the provision would have been a valid law of the Commonwealth; or

c. Assuming that the Parliament of the Commonwealth had enacted a provision that created an offence penalising the specific acts or omissions involved in committing the State offence – that provision would have been a valid law of the Commonwealth; or

d. Both

i. The Australian Federal Police is investigating an offence against a law of the Commonwealth or a Territory; and

ii. If the Australian Federal Police is investigating, or were to investigate, the State offence – that investigation is, or would be, incidental to the investigation mentioned in subparagraph (i).

Additional Comments by Labor Members

Labor members support the Committee's report and its 34 recommendations.

We do, however, believe that Recommendation 10 can and should go further.

All members of the Committee have acknowledged that the powers in the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 are extraordinary.

The need for these extraordinary new powers has been justified by reference to the most serious types of offences. In the Explanatory Memorandum, for example, the Government has said that:

This Bill addresses gaps in the legislative framework to better enable the AFP and the ACIC to collect intelligence, conduct investigations, disrupt and prosecute **the most serious of crimes, including child abuse and exploitation, terrorism, the sale of illicit drugs, human trafficking, identity theft and fraud, assassinations, and the distribution of weapons.**

This statement deliberately mischaracterises the breadth of the new powers. As all members of the Committee have acknowledged, the new powers will enable the AFP and the ACIC to collect intelligence, conduct investigations, disrupt and prosecute all "relevant offences" (as defined in the *Surveillance Devices Act 2004*).

The definition of “relevant offence” includes all offences against the law of the Commonwealth that are punishable by a maximum term of imprisonment of 3 years or more. This includes the types of crimes listed in the Explanatory Memorandum – but it also includes tax offences, trade mark infringement and a range of other offences which do not fall within the categories of “child abuse and exploitation, terrorism, the sale of illicit drugs, human trafficking, identity theft and fraud, assassinations, and the distribution of weapons".

We are not suggesting that other types of offences are not serious. We are simply pointing out that the Government – and the agencies – have failed to make the case for why these extraordinary new powers are needed to “collect intelligence, conduct investigations, disrupt and prosecute” crimes that are not “child abuse and exploitation, terrorism, the sale of illicit drugs, human trafficking, identity theft and fraud, assassinations, and the distribution of weapons".

It is obviously much easier to justify the introduction of extraordinary powers by focusing only on the most serious crime types, especially crimes like child abuse and exploitation and terrorism. But it is incumbent on this Committee, and the Parliament, to require the Government and agencies to engage in the more difficult task of justifying the introduction of extraordinary powers by reference to how the powers could actually be used.

Labor members consider that Recommendation 10 and the other recommendations in the Committee’s report go a long way to ensuring that these new powers will only be used in relation to the most serious offending. However, in recognition of the extraordinary nature of these new powers and the way in which the Government and agencies sought to justify their introduction, Labor members think the Committee should have gone further by recommending that the references to “relevant offence” in the bill be replaced by a new concept of “serious offence”.

We note that there are a number of different definitions of “serious offence” in Commonwealth legislation. Our preference would be to adopt a definition that is broadly consistent with the definition of “serious offence” in the *Telecommunications (Interception and Access) Act 1979*.

Hon Anthony Byrne MP
Deputy Chair

Hon Mark Dreyfus QC MP

Senator Jenny McAllister

Senator the Hon Kristina Keneally

Dr Anne Aly MP