Australian Human Rights Commission

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill exposure draft 2018

Australian Human Rights Commission

Submission to the Department of Home Affairs

10 September 2018

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
Complaints info line 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

Contents

1 Executive summary 3
2 Background 4
(a) Summary of the human rights impacts of the draft Bill 6
3 Human rights and digital law enforcement 8
3.1 Right to privacy 10
3.2 Right to freedom of expression 11
3.3 Permissible limitations on human rights 12
(a) Legitimate aims 12
(b) Necessity 13
(c) Proportionality 13
4 The draft Bill 14
4.1 Provider assistance framework (Schedule 1) 14
4.2 Warrant powers (Schedules 2–5) 19
5 Key human rights concerns: assistance requests and notices 19
5.1 Scope of assistance scheme 21
(a) 'Acts or things' 21
(b) 'Relevant objectives' 23
(c) 'Decision-making criteria' 25
5.2 Boundaries of systemic and non-systemic effects 28
5.3 Interaction with warrants 31
5.4 Voluntary nature of requests 33
5.5 Secrecy provision 35
5.6 Safeguards, oversight and reporting of assistance scheme 39
6 Key human rights concerns: warrant powers 44
6.1 Computer access warrants 44
(a) Access to third party computers, communications and premises 46
6.2 Concealment of access provisions 49
6.3 Ancillary interception powers 51
6.4 Assistance orders 54
(a) Disproportionality of increased penalty provisions 56
(b) Privilege against self-incrimination 57
7 List of recommendations 60

1 Executive summary

1. The Australian Human Right Commission (the Commission) makes this submission to the Department of Home Affairs (the Department), in response to the exposure draft of the Telecommunications and other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (the draft Bill).

2. The stated purpose of the draft Bill is to provide national security and law enforcement agencies with powers to respond to the challenges posed by the use of encrypted communications and devices.[1] To this end, the draft Bill creates a new scheme that compels communications providers to assist national security and law enforcement agencies, introduces a new covert computer access warrant, and strengthens existing search and seizure powers under warrant.

3. The Commission welcomes the opportunity for public consultation on the exposure draft, and commends the detailed explanatory document provided by the Department to facilitate public comment.[2]

4. In light of the short timeframe for the preparation of submissions in this consultation process, and the length and complexity of the draft Bill, this submission is not exhaustive. Rather, it draws attention to the key human rights concerns identified by the Commission to date. The submission is based on the Commission's understanding of the impacts of the draft Bill, noting that the Commission's technological expertise is limited.

5. The Commission acknowledges the critical importance of law enforcement and national security agencies having appropriate powers to carry out their functions. Such powers can be used to protect human rights, including the right to life,[3] and help fulfil Australia's international law obligations.[4]

6. However, the proposed access and assistance measures also authorise intrusive and covert law enforcement powers that can significantly limit an individual's rights to privacy and freedom of expression, among other rights.

7. Given the interdependent and globalised nature of digital technologies, the reforms not only impact the human rights of potential law enforcement targets, but also the human rights of the Australian public at large.

8. Legislation such as this must enable appropriate cyber intelligence capabilities for government, while at the same time preserving the ability

of individuals to lead their lives freely and privately. This is a complex challenge, and can involve an often delicate balancing process.

9. International human rights law provides a framework to assess whether this balance has been appropriately struck. It provides significant scope for governments to provide security and law enforcement agencies with extensive powers, even where they impinge on individual rights and freedoms. However, to be permissible, any limitation on human rights must be clearly expressed, unambiguous in its terms, and a necessary and proportionate response to a legitimate objective.
10. The Commission holds serious concerns that numerous provisions of the draft Bill do not meet this test. Of particular concern are the proposed breadth of the powers, the ambiguity of certain provisions and the inadequacy of effective safeguards.
11. This submission contains 39 recommendations made by the Commission to ameliorate the significant human rights concerns it has identified so far. The Commission's recommendations are set out throughout the body of the submission, as well as in a complete list at Pt 7.
12. The Commission considers that the draft Bill should be reconsidered and redrafted in a way that strengthens the relevant human rights protections.
13. Given the complexity of the draft Bill, the Commission urges the Department to allow a further opportunity for public comment. It stresses the importance of further and adequate time being provided for revision of the proposed framework in response to public submissions that identify human rights concerns.
14. The Commission would welcome the opportunity to provide further input into the development of the legal framework contemplated by the draft Bill.

2 Background

15. The evolution of digital technology has offered individuals unprecedented connection, convenience and choice in their everyday lives.
16. In particular, information communication technologies have revolutionised our common modes of interaction. For example, messaging applications on smartphones allow users to exchange texts, photos, and other data instantaneously, forming 'the backbone of digital life for tens of millions of individuals, [and] providing a popular means of communication and access to information'.[5]

17. As well as playing an important and valuable role in the lives of Australians, information communication technologies can be a means of realising the right to privacy and freedom of expression protected under articles 17 and 19 of the *International Covenant on Civil and Political Rights* (ICCPR).[6]

18. Information communication technologies collect, store, use and analyse a vast amount of data, including personal information. Now more than ever, our communications, financial information, health and biometric data are digitally created and held. Other private and sensitive online data can include information about a person's political beliefs, sexual orientation and geographic location and movements.

19. This digitisation of information increases the risk of unauthorised access, whether by deliberate hacking or other inadvertent data breaches. Recent high-profile hacking attacks and data breaches show the increasing difficulty of ensuring security online.[7]

20. Various cybersecurity measures have been developed in response to such risks, most notably the use of encryption.

21. 'Encryption' has been defined as:

> A technique that attempts to secure data transmitted over computer networks from the point of interception to ensure its confidentiality. Encryption transforms data by the use of cryptography (complex mathematical algorithms) to produce unintelligible (encrypted) data.[8]

22. Encryption works by, for example, 'scrambling' the 'plain text' of an original message into an unintelligible form of 'cipher text' during transmission, and 'unscrambling' the message back to readable plain text form once opened by the recipient. This technique aims to ensure that when a 'data packet' is sent by a sender to a recipient, whether it be a voice call, email, credit card number or other information, it is securely transmitted and accessed only by the person for whom receipt is intended.

23. Encryption is ubiquitous in our digital lives and has many common uses, including securing data and authenticating the identity of individuals in a wide range of fields. These fields include traditional and cloud computing, smart phones (including through device locking), banking transactions, web browsing, email traffic and virtual private networks. The use of encryption is likely to continue to grow through new technological advances such as block chain.

24. The United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has said that encryption and anonymity, and the security concepts behind them,

provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age.[9]

25. However, the prevalence of encryption has also led to concerns about private, anonymous and untraceable cybertechnologies being used to facilitate serious crime. Termed 'going dark', law enforcement bodies are particularly concerned about the technical inability of investigators to intercept and access communications that aid criminal activity in such circumstances, despite holding legal authority such as a warrant.[10] The explanatory document to the draft Bill states that 95% of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications.[11]

26. While encryption might hamper law enforcement agencies' access to some data, the digital era has also fundamentally transformed the ability of investigators to carry out their work. Unencrypted metadata and other such material are now increasingly available as actionable intelligence and evidence that can be used in legal proceedings. Such material can be contrasted with the content of certain communications, such as text messages, which might be encrypted.

27. Some experts suggest that, overall, evidence gathering is now more efficient and cost-effective for investigators.[12] This should be kept in mind when considering the appropriateness of particularly intrusive digital law enforcement powers.

(a) Summary of the human rights impacts of the draft Bill

28. The draft Bill seeks to provide national security and law enforcement agencies with powers to respond to the challenges posed by encrypted communications and devices through a range of measures.[13] Detailed consideration of the operation of the draft Bill is set out in Pt 4 below, and an analysis of the key human rights concerns identified in Pts 5 and 6.

29. The draft Bill would introduce a new computer access warrant regime in the *Surveillance Devices Act 2004* (Cth) (SD Act) that will allow law enforcement agencies to covertly access data on computers, sometimes remotely.

30. Another key reform is the implementation of an assistance and access framework, which empowers certain agencies, by way of request or compulsory notice, to have a designated communications provider provide them with technical assistance.[14]

31. An important legislative safeguard is that a compulsory notice cannot require a provider to implement or build a 'systemic weakness, or a systemic vulnerability, into a form of electronic protection'.[15]

32. The Commission endorses this principle, which recognises the inherent dangers of weakening technologies that are developed to secure electronic information, primarily encryption. That is, allowing third party access to encrypted data or services, even if designed for the use of law enforcement, risks weakening the security of an encryption measure across the board.

33. A prime example, which appears *not* to be permitted under the framework, is requiring a company to modify a messaging application to include an independent port for law enforcement access.[16] The creation of such a port, sometimes termed an 'encryption backdoor',[17] can greatly increase the susceptibility of hacking by a malicious actor.

34. If such a port is hacked, third parties could obtain a vast amount of personal information, possibly about every user of the application, not just the law enforcement target. The result could be an increase in levels of cyber and traditional crime, such as identity fraud, and large-scale interferences with the rights to privacy and freedom of expression.

35. Such scenarios highlight the highly interconnected nature of cybersecurity technologies, and potentially pervasive consequences of the Government requiring exceptional access.

36. However, the Commission is concerned that the proposed 'systemic weakness' provision is ambiguous and authorises certain exceptional access measures.[18] As a result, this important protection cannot be fully effective, because the draft Bill could still be used to enable the creation of certain systemic weaknesses.

37. A further overarching human rights issue raised by the draft Bill is the impact of enhanced surveillance powers on the way that individuals use technology to conduct their private lives.

38. Any improved ability of the Government to conduct digital surveillance, intercept digital communications and collect personal data in a manner that is disproportionate or unnecessary to a legitimate objective risks a 'chilling effect' on the enjoyment of human rights, in particular the rights to freedom of expression and privacy.

39. The Commission considers that further consideration and refinement of the draft Bill are required to ensure its compatibility with human rights.

Recommendation 1

The Australian Government ensure that further and adequate time is afforded for public consultation, review and reform of the draft Bill, to enhance human rights compatibility.

3 Human rights and digital law enforcement

40. As a party to the ICCPR and other international human rights treaties, Australia has undertaken to comply with their provisions in good faith and take necessary steps to give effect to those treaties under domestic law.

41. Articles 17 and 19 of the ICCPR enumerate Australia's obligations to protect, respect and fulfil the right to privacy and the right to freedom of expression. These rights are related and mutually reinforcing—an individual's privacy facilitates their freedom of expression.[19]

42. The draft Bill would create broad new powers enabling government agencies to gain access to information that would otherwise remain private—for example, by virtue of encryption.[20]

43. The UN Office of the High Commissioner for Human Rights (OHCHR) has highlighted the fundamental importance, universal recognition and enduring relevance of the right to privacy, and the importance of ensuring proper safeguards in both law and practice.[21]

44. The right to freedom of expression and freedom of opinion have been described by the UN Human Rights Committee (HR Committee) as 'indispensable conditions for the full development of the person', 'essential for any society' and a 'foundation stone for every free and democratic society'.[22]

45. These rights are also an essential precondition for the proper protection of *all* human rights,[23] as well as the robust and representative nature of Australian democracy.

46. By allowing individuals to monitor, discuss and expose the human rights abuses of governments and other actors, the right to freedom of expression is integral to 'the realisation of the principles of transparency and accountability'.[24] It is also necessary for the effective exercise of the right to vote.[25]

47. With the advent of digital law enforcement, the rights to privacy and freedom of expression are newly resonant.

48. Most relevantly, the increasing ability of governments and others to conduct surveillance, intercept and decrypt the online activities of individuals can significantly limit these and other human rights. The

proposed access and assistance powers in the draft Bill facilitate digital surveillance and interception by law enforcement agencies, thereby engaging and limiting the same human rights.

49. In Resolution 68/167 adopted in 2013, the United Nations General Assembly (UNGA) expressed deep concern at the negative impact that government surveillance and the interception of communications may have on the exercise and enjoyment of human rights.[26]

50. The UNGA called on all States to respect and protect the right to privacy in digital communication, and affirmed that human rights must be protected online.[27] It called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, and emphasised the need to fulfil their obligations under international human rights law.[28]

51. The OHCHR has stated that electronic surveillance, of both content and metadata, will amount to a *prima facie* interference with privacy:

> [A]ny capture of communications data is potentially an interference with privacy and, further … the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.[29]

52. The 'chilling effect' of government surveillance on civil liberties has been described as the self-adjustment of behaviour by the community, even if their actions were not wrongful, in the knowledge that one's interactions and communications may be recorded and judged by unknown others.[30]

53. Other human rights may also be inappropriately limited by the unnecessary or disproportionate exercise of digital surveillance and interception by law enforcement agencies. These include a person's enjoyment of their rights to freedom of religion, a fair hearing and equality.[31]

54. For example, there is a risk of digital surveillance powers being used to monitor persons inappropriately on the basis of their race, religion or political opinions. Also concerning is the potential for targeting of journalists, whistle-blowers, opposition politicians, human rights defenders[32] and persons exercising lawful public dissent. Children's rights may also be affected by the use of the proposed coercive powers on underage providers, or to compel a minor to give access to a device. Such human rights impacts are not addressed in the present submission, but merit further consideration.[33]

55. Given the potentially significant and far-reaching consequences of the draft Bill on human rights, it is crucial to ensure that any rights limitations are necessary and proportionate. Part of achieving human rights compatibility is the provision of effective safeguards and oversight mechanisms.

3.1 Right to privacy

56. Article 17 of the ICCPR enumerates the right to privacy as follows:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

57. The right to privacy protects communications made in private, and is also applicable to the collection and use of personal information by government.

58. The right to privacy is especially important in the context of the draft Bill, given the narrow conception of privacy in Australian law and limited protection against invasion of privacy in our common law. Further, some intelligence agencies, including ASIO, are exempt from the operation of the *Privacy Act 1988* (Cth).

59. Under human rights law, any interference with the right to privacy must be lawful and non-arbitrary.

60. 'Lawful' means that limitations must be provided for by law in a precise and clear manner to allow individuals to regulate their conduct. The UN HR Committee has explained the requirements of lawfulness as follows:

> Relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by the authority designated under the law, and on a case-by-case basis.[34]

61. As stated by the OHCHR, 'non-arbitrary' means that any interference must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable—that is, proportionate and necessary to achieve a legitimate objective—in the particular circumstances.[35]

62. Further, for a limitation on the right to privacy to be compatible with human rights:

> The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for

the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.[36]

3.2 Right to freedom of expression

63. Article 19 of the ICCPR protects the right to freedom of expression:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

64. The right to freedom of expression protects all forms of communication, including 'political discourse, commentary on one's own and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching and religious discourse'.[37] It also protects the freedom to seek, receive and impart information and ideas of all kinds, free from unlawful interference.

65. However, free speech is not an absolute right and can be limited, as indicated in article 19(3). Any limitation must be lawful, necessary and proportionate to achieve a legitimate objective within the scope of article 19(3). This includes limitations for the protection of national security or to protect the rights of others, meaning human rights under international human rights law, including the ICCPR.[38]

66. As set out by the UN Economic and Social Council in the *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (Siracusa Principles)*, the term 'national security' relates to matters which threaten the existence of the State, its territorial

integrity or political independence.[39] This is a high threshold and not every law criminalising conduct can properly be described as protecting national security.

67. Relevantly, the *Siracusa Principles* state that:

> 29. National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force.
>
> 30. National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order.
>
> 31. National security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse.[40]

68. Consistently with these principles, the UN High Commissioner for Human Rights has stated that whistle-blowers who disclose human rights violations should be protected.[41]

3.3 Permissible limitations on human rights

69. Some human rights cannot legitimately be subject to any limitation—such as the freedom from torture and other cruel, inhuman or degrading treatment or punishment.[42] However, most human rights, including the rights to privacy and freedom of expression, may be limited where the limitation is: expressed in clear and unambiguous terms; directed towards a legitimate aim; necessary to achieve that aim; and is proportionate. A measure which limits a human right must not be arbitrary or jeopardise the essence of the right.

70. There is some overlap between a number of these criteria.[43] In particular, the concept of 'arbitrariness' in human rights law includes notions of 'inappropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity and proportionality'.[44]

71. Any assessment as to the necessity of a limitation is to be made on objective considerations. The burden of justifying a limitation of a human right lies with the State.[45]

(a) Legitimate aims

72. Human rights may be limited where the limitation is necessary and proportionate to achieving a legitimate aim. The Commission has long accepted that protecting the human rights of individuals endangered by serious criminal activity, such as the general public, is a legitimate aim.

73. The OHCHR has stated that surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a measure that serves a 'legitimate aim', but the degree of interference must be assessed against the necessity of the measure to achieve that aim, and the actual benefit it yields towards such a purpose.[46]

(b) Necessity

74. A measure which restricts human rights cannot be justified unless it is necessary. This is a vital consideration in the law enforcement context, given that there may be numerous methods of gathering evidence.

75. To be 'necessary', a measure must be based on one of the grounds justifying limitation that: are recognised in the ICCPR; respond to a pressing public or social need; pursue a legitimate aim; and are proportionate to that aim.[47]

76. A measure is not necessary if the aim of that measure could be achieved through less rights-intrusive means. Similarly, a restrictive measure cannot be said to be necessary if it essentially duplicates existing measures.

77. There is a real risk that law enforcement powers will limit human rights to a greater degree than is necessary through 'legislative creep'. That is, intrusive and previously extraordinary law enforcement powers can quickly become normalised through successive legislation and practice, and used as a precedent to justify even more invasive future measures.[48]

78. To establish necessity, the proposed reforms in the draft Bill must be closely scrutinised to determine whether they go beyond what is potentially useful to law enforcement.

(c) Proportionality

79. Assessing whether limitations on human rights are proportionate to the pursuit of a legitimate objective requires an assessment of the nature and extent of each limitation, the urgency of the objective, and the degree to which the rights-limiting measure is likely to achieve the objective.

80. The UN HR Committee has provided the following guidance on proportionality:

> Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected. The principle of proportionality has to be respected not only in the law that

frames the restrictions, but also by the administrative and judicial authorities in applying the law.[49]

81. The UN Economic and Social Council has said that, even during a public emergency that threatens the life of a nation, derogation from a State's ICCPR obligations must be strictly necessary to deal with the threat, and proportionate to the nature and extent of the threat.[50]

82. A fully informed assessment of these issues may, in some circumstances, depend on the consideration of classified security material. Therefore, relevant decision makers empowered to give notices or to obtain warrants under the draft Bill are uniquely placed to assess proportionality. In the Commission's view, it is accordingly crucial that human rights protections are built into the decision-making process, to ensure proper consideration of human rights by decision makers in all the relevant circumstances.

4 The draft Bill

83. The key changes introduced by the draft Bill are:

- enhanced obligations of designated communications providers, including both onshore and offshore providers, to assist national security and law enforcement agencies
- introduction of a new computer access warrant that will enable covert gathering of evidence directly from a device
- the strengthened ability of law enforcement and national security authorities to access data overtly through existing search and seizure warrants.

4.1 Provider assistance framework (Schedule 1)

84. The draft Bill proposes a new Pt 15 of the *Telecommunications Act 1997* (Cth), which establishes an 'industry assistance framework'.[51] The framework empowers certain law enforcement and national security agencies to request or compel 'designated communications providers' to do a range of 'acts or things' to provide technical assistance to prescribed agencies in prescribed circumstances.[52]

85. The explanatory document states that the purpose of the framework is to facilitate agencies' *access* to services or systems, without changing the existing mechanisms that agencies must use to lawfully access telecommunications content and data for investigations.[53] The assistance powers under proposed new Pt 15 of the *Telecommunications Act 1997*

(Cth) will not in themselves require or authorise the interception or retention of data, which will remain subject to existing warrants regimes.[54]

86. However, as will be discussed below, the breadth of the proposed powers under the industry assistance framework, and how it interacts with established warrants processes, is unclear, making it uncertain as to what exact actions can lawfully be required of providers.

87. The draft Bill establishes three tiers of mechanisms to facilitate or compel 'industry assistance', with each tier providing progressively more onerous obligations as follows:

    - Technical assistance request (TAR): Under a TAR, the Director-General of Security,[55] the Director-General of the Australian Secret Intelligence Service (ASIS), the Director-General of the Australian Signals Directorate (ASD) or the chief officer of an 'interception agency' can request that a provider *voluntarily* assist ASIO, ASIS, the ASD and interception agencies.[56]
    - Technical assistance notice (TAN): Under a TAN, the Director-General of Security, or the head of an 'interception agency', can *require* a provider to give assistance that it is already capable of providing, if the relevant decision maker is satisfied that the requirements are 'reasonable and proportionate' and that compliance is 'practicable and technically feasible'.[57]
    - Technical capability notice (TCN): Under a TCN, the Attorney-General can *require* a provider to build a new capability that will enable them to give assistance to ASIO and 'interception agencies', where the Attorney-General is satisfied that the requirements are 'reasonable and proportionate' and that compliance is 'practicable and technically feasible'.[58]

88. Despite the name 'technical assistance *requests*', and the explanatory document stating that TARs are voluntary, the Commission considers that their voluntary nature is not made explicit enough in proposed s 317G. This issue is discussed further below at Pt 5.4.

89. 'Interception agencies' are defined as agencies with interception powers under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), being the Australian Federal Police, the Australian Commission for Law Enforcement Integrity, the Australian Criminal Intelligence Commission, state and territory police agencies and anti-corruption commissions.[59]

90. The definition of a 'designated communications provider' in proposed s 317C is broad and includes:

- a person that 'is a carrier or carriage service provider' or 'a carriage service intermediary'
- a person that 'provides an electronic service that has one or more end-users in Australia'
- a person that 'develops, supplies or updates software used, for use, or likely to be used, in connection a listed carriage or an electronic service …'
- a person that 'manufactures or supplies components for use … in the manufacture of a facility'
- a person that 'connects a facility to a telecommunications network in Australia'
- a person that 'manufactures or supplies customer equipment for use … in Australia'
- a 'constitutional corporation' who 'manufactures or supplies or installs or maintains data processing devices'
- a 'constitutional corporation' who 'develops or supplies or updates software that is capable of being installed on a computer, or other equipment that is or is likely to be connected to a telecommunications network in Australia'.

91. The explanatory document states that the choice to define a 'designated communications provider' so broadly is deliberate, to capture 'the full range of companies in the communications supply chain both within and outside Australia'.[60] Notably, proposed s 317C extends to offshore entities that have a role in the provision of communications and related services in Australia.

92. By way of example of the breadth of providers subject to the assistance framework, the obligations apply to the provider of an 'electronic service' as defined by proposed s 317D(1)–(2) of the draft Bill.[61] The explanatory document states that an 'electronic service' covers websites, chat fora, cloud and web hosting, peer-to-peer sharing platforms and email distribution lists.[62] The explanatory document further states that this definition is intended to capture 'a range of existing and future technologies, including hardware and software'.[63]

93. The Commission notes that the definition of 'designated communications provider' applies to organisations as well as natural persons. While it is easy to imagine a scenario where industry leaders such as Google or Facebook are asked to provide technical assistance to law enforcement, the framework extends to individuals—for example, programmers, app

developers and webmasters—who may have lower levels of corporate and legal sophistication. Additionally, such individuals may not have access to legal advice to inform their understanding of the framework proposed by the draft Bill.

94. Proposed s 317E sets out the forms of assistance that a provider can be requested or compelled to provide, defined as 'listed acts or things', including:

    - removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider
    - providing technical information
    - installing, maintaining, testing or using software or equipment
    - facilitating or assisting access to, among other things, a facility, customer equipment, data processing device or listed carriage service
    - assisting with the testing, modification, development or maintenance of a technology or capability
    - notifying changes affecting the activities of the provider
    - modifying a characteristic of a service
    - substituting a service for another service
    - concealing the fact that covert action has occurred.[64]

95. The explanatory document states that the assistance requested or compelled from providers can include: the decryption of a communication or device; the provision of design specifications including source code; the installation or deployment of software provided by an agency; the formatting of information obtained under a warrant; the facilitation of access to a device or service; helping agencies test their own systems; notifying agencies of major changes to services or systems; and the blocking of delivery of service to a target.[65]

96. A provider that fails to comply with a notice 'to the extent that the provider is capable of doing so', is liable to a civil penalty.[66] A body corporate, whether onshore or offshore, can be liable to a penalty of up to $10 million and an individual of up to $50,000.[67]

97. Proposed s 317ZG(1) prohibits TANs or TCNs from having the effect of either 'requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection' or 'preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection'.

98. This limitation includes a prohibition on requiring providers to build a new decryption capability in relation to a form of electronic protection, or to take action that would 'render systemic methods of authentication or encryption less effective'.[68] As discussed below in Pt 5.2 of the submission, the terms 'systemic weakness' or 'systemic vulnerability' are not defined in the draft Bill.

99. The explanatory document refers to a number of other safeguards and oversight mechanisms in the draft Bill, including:

- before giving or varying a TAN or TCN, the decision maker must be satisfied that the notice is reasonable and proportionate and that compliance is practicable and technically feasible[69]
- before giving a TCN, the Attorney-General must give the provider the opportunity to consult through making a submission, noting that this requirement does not apply where it is urgent or impracticable[70]
- revocation of a TAN or TCN must occur if a decision maker is satisfied that the requirements are not reasonable and proportionate or that compliance is not practicable and technically feasible[71]
- core data retention and interception capability obligations remain subject to existing legislative arrangements in the TIA Act[72]
- the reforms will not alter the need for agencies to seek a warrant or authorisation under the TIA Act or the SD Act to undertake activities permitted by those Acts; however, if a warrant is already issued, provider assistance can be directed towards facilitating execution of the warrant[73]
- the purposes for which a provider can be requested or compelled to assist an agency are limited to objectives deemed 'relevant objectives', including purposes related to criminal law enforcement, national security or the protection of public revenue[74]
- the requested or compelled assistance must be in connection with an 'eligible activity' of a provider and must relate to the performance of a function or exercise of a power conferred on a relevant agency, so far as it relates to a 'relevant objective'[75]
- the ability to issue notices is reserved to 'senior decision-makers', although delegation is possible in certain instances[76]
- judicial review is available to challenge a decision to issue a notice
- unauthorised disclosure of information obtained about or under a notice is an offence, punishable by five years imprisonment[77]

- the Minister is required to table a report every financial year setting out the number of TANs and TCNs given[78]
- arbitration is available to resolve disputes between the Government and providers regarding the terms and conditions of a notice.[79]

100. The Commission is concerned that some of these safeguards are either not fully embodied in the draft Bill, or are insufficient to ensure that human rights are not impermissibly limited. A discussion of the adequacy of certain of these proposed safeguards to protect human rights is provided below in Pts 5 and 6 of this submission.

4.2 Warrant powers (Schedules 2–5)

101. Key features of Schedules 2–5 of the draft Bill include:

- provisions that would insert a new 'computer access warrant' regime into the SD Act to allow law enforcement agencies to access data in computing devices covertly and, in some cases, remotely, in investigations relating to relevant offences, recovery orders, mutual assistance investigations, integrity operations and control orders
- provisions that would attach ancillary interception powers to computer access warrants issued under the new computer access warrant regime in the SD Act and also under the ASIO Act
- provisions that would increase the penalties for non-compliance with 'assistance orders' issued under the SD Act, the *Crimes Act 1914* (Cth) (Crimes Act), the *Customs Act 1901* (Cth) (Customs Act) and the ASIO Act.

102. Schedules 2–5 of the draft Bill propose to amend over 10 pieces of existing Commonwealth legislation to enhance existing warrant powers. Again, in light of the short timeframe provided for public consultation on the exposure draft, it is beyond the scope of the present submission to comprehensively address all of these changes. Rather, this submission focuses on a number of impacts that the draft Bill would have, primarily on the rights to privacy and the freedom of expression.

5 Key human rights concerns: assistance requests and notices

103. As an overarching comment, the Commission is concerned about the wide scope of operation of the proposed assistance scheme.

104. The Commission considers that certain provisions in Schedule 1 of the draft Bill limit human rights to a significant degree, without demonstrating that such limitations are necessary and proportionate.

105. The Commission is especially concerned about the following features of the assistance framework:

- it contains overbroad powers that are not appropriately limited to ensure that they are only available when necessary and proportionate
- certain powers can be broadened by the executive once the law is enacted
- the proposed safeguards, to mitigate unlawful interferences with human rights, are inadequate.

106. As law enforcement powers have the potential to be extremely rights-intrusive, they must be subject to close scrutiny. Compelling evidence will be required before the rights limitations can be demonstrated to be necessary and proportionate. Further, it is important that such laws are drafted with precision, to ensure that they impinge on human rights no more than is strictly necessary to achieve their purpose.

107. In the law enforcement and national security context, it is also particularly important to ensure that legislative authority for exercises of power is clearly articulated, to ensure their lawful exercise in often complex, difficult and time-critical circumstances where a balancing of competing considerations is required.

108. Additionally, relevant law enforcement officials are often the only persons with access to the full range of relevant intelligence and information to make a decision, and with the necessary expertise to assess the relevant risks and benefits of an exercise of power. It is therefore important that human rights protections are built into the decision-making process, to ensure adequate consideration and protection in all the circumstances.

109. Further, given the proposed secrecy provisions in the draft Bill, it is also important to ensure that the law sets out publicly accessible, precise and clear criteria for decision making, given that public scrutiny will be limited in practice.

110. In light of these concerns, the Commission draws attention to the following instances where the proposed powers have not been shown to be necessary and proportionate in accordance with human rights law.

5.1 Scope of assistance scheme

(a) 'Acts or things'

111. The assistance scheme empowers agencies to request or compel the provision of a wide range of assistance from a designated communications provider, under the 'listed acts or things' designated in proposed s 317E.[80]

112. The explanatory document appears to suggest that the primary purpose of the industry assistance provisions is to facilitate access to data, devices or systems that are already the subject of a warrant, where such material would otherwise be inaccessible or unintelligible.

113. However, the definition of 'acts or things' in the draft Bill is so vague as to potentially permit almost limitless forms of assistance to be requested or required, possibly including assistance that is unconnected to a warrant.

114. The Commission considers that the language used to define 'listed acts or things' is inappropriately ambiguous and overbroad. For example, proposed s 317E(c) allows an agency to require a provider to assist with 'using' 'software or equipment'. The Commission considers that it is unclear on the face of this provision exactly what may constitute 'use' of software. Further, 'equipment' is an extremely broad term that could encompass almost anything.

115. Further, in the case of TARs and TANs, the listed 'acts or things' in the definition in proposed s 317E are non-exhaustive.[81]

116. For TCNs, the list of 'acts or things' in the draft Bill is exhaustive, and excludes any act or things covered by proposed paragraph 317E(1)(a).[82] That is, a provider cannot be compelled by a TCN to remove electronic protection that was applied by or on behalf of a provider.

117. However, the Minister may, by way of legislative instrument, determine further 'acts or things' that can be compelled under a TCN.[83] It is not clear that the legislative safeguard that prevents the removal of electronic protection being requested of a provider under an initial TCN applies to this Ministerial determination power.

118. Before making such a determination, the Minister must consider the interests of law enforcement, national security, the objects of the Act, the likely impact of the determination on designated communications providers, and such other matters as the Minister considers relevant.[84] While the consideration of human rights impacts could fall under the last criterion, most relevantly how the right to privacy might be limited, this is not explicitly mandated.

119. The Commission considers that, rather than by way of Ministerial determination, it would be more appropriate for further acts and things only to be added by way of legislative amendment. This approach would allow for full parliamentary and public scrutiny, including of the necessity and proportionality of likely further significant human rights limitations.

120. Further, the Attorney-General's power to vary a TCN, once issued, appears to allow the inclusion of *any* listed act or thing, including the removal of electronic protection.[85] This power would make the listed acts and things *non-exhaustive* for varied TCNs, in contrast with the initial issue of a TCN.

121. This potential loophole raises concerns that providers could, in fact, be compelled to implement or build a capability that removes electronic protection by a TCN variation (noting that the proposed prohibition in s 317ZG on a notice requiring a provider to create a systemic weakness would still apply).[86] This is inconsistent with the intention expressed in the explanatory document, that 'agencies may not require providers to build a capability to remove electronic protection under a TCN'.[87]

122. It is possible that the broad drafting of proposed s 317E might be intended to 'future-proof' the scheme. However, the Commission considers that its breadth and ambiguity may not satisfy the requirements of necessity and proportionality. The explanatory document does not demonstrate that such a broad definition is required to achieve the objectives of the draft Bill.

123. Having such a large potential suite of 'assistance measures' also increases the risk of agencies choosing the most rights-intrusive form of assistance as a matter of convenience, when a less restrictive measure would suffice.

124. The Commission considers that, given the significant potential limitation on human rights, in particular the right to privacy, the draft Bill should be redrafted so that: the 'listed acts or things' in s 317E are as confined as possible; the definition of 'listed acts or things' is exhaustive in relation to all kinds of assistance requests and notices; and so that the definition of 'acts or things' cannot be expanded by legislative instrument.

125. The Commission recommends that:

Recommendation 2

Proposed s 317E of the *Telecommunications Act 1997* (Cth) be redrafted in narrower terms, to ensure that the 'acts or things' that can be requested or required under TARs, TANs and TCNs are restricted to those that are strictly necessary for law enforcement and national security agencies to carry out their functions.

Recommendation 3

Proposed ss 317G(6), 317L(3) and 317X(3) of the *Telecommunications Act 1997* (Cth) be amended so that the only 'acts or things' permissible under a TAR, TAN or TCN are those specified in s 317E (that is, the list of 'acts or things' in s 317E should be exhaustive in all cases).

Recommendation 4

Proposed s 317(X) of the *Telecommunications Act 1997* (Cth) be amended to make clear that a varied TCN cannot compel a provider to remove electronic protection, by excluding the applicability of s 317E(1)(a).

Recommendation 5

Proposed s 317T(5) of the *Telecommunications Act 1997* (Cth) be removed, to prevent the ability of the Minister to expand the definition of 'acts or things' for the purposes of a TCN by way of legislative instrument.

Recommendation 6

In the event that Recommendation 5 is not accepted, that the decision-making criteria in proposed s 317T(6) of the *Telecommunications Act 1997* (Cth) be amended to require the Minister to consider the right to privacy and other human rights before making a legislative instrument that will expand the definition of 'acts or things' for the purpose of a TCN, and only allow the exercise of power if the Minister is satisfied that the limitation of the right to privacy and other human rights is necessary and proportionate in all of the circumstances of a particular case.

Recommendation 7

In the event that Recommendation 5 is not accepted, proposed s 317T(5) of the *Telecommunications Act 1997* (Cth) be amended to make clear that a legislative instrument that expands the definition of 'acts or things' for the purpose of a TCN is a disallowable instrument.

(b) 'Relevant objectives'

126. The Commission is concerned that the relevant objectives that enliven the giving of requests or notices for assistance are overly broad.

127. A decision maker can issue a voluntary TAR to ensure that a provider is capable of giving help or can help the relevant agency in relation to the performance of a function or exercise of a power conferred by or under law 'so far as the function or power relates to a relevant objective', or matters ancillary or incidental.[88]

128. Proposed s 317G(5) defines 'relevant objective' for TARs to mean:

(a) enforcing the criminal law and laws imposing pecuniary penalties; or

(b) assisting the enforcement of the criminal laws in force in a foreign country; or

(c) protecting the public revenue; or

(d) the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

129. Similarly, proposed s 317L(2)(c) provides that relevant objectives for TANs are:

(i) enforcing the criminal law and laws imposing pecuniary penalties; or

(ii) assisting the enforcement of the criminal laws in force in a foreign country; or

(iii) protecting the public revenue; or

(iv) safeguarding national security …

130. Proposed s 317T(3) defines 'relevant objective' for TCNs to mean:

(a) enforcing the criminal law and laws imposing pecuniary penalties; or

(b) assisting the enforcement of the criminal laws in force in a foreign country; or

(c) protecting the public revenue; or

(d) safeguarding national security.

131. The explanatory document highlights that the assistance powers will be used for national security and law enforcement purposes. However, the Commission notes that the relevant objectives for assistance requests cover a large range of contexts that do not appear to relate to serious crime, including 'the interests of Australia's national economic well-being'. Further, 'protecting the public revenue' is a relevant objective for TARs, TANs and TCNs. This term is not defined in the draft Bill. The explanatory document states that these objectives cover matters such as tax evasion, corporate misconduct and debt recovery actions.[89]

132. Restrictions on human rights are only permissible when they are proportionate to achieving a legitimate objective. While measures that significantly limit human rights may be permissible to protect national security, it is much more difficult to establish that they will be proportionate to achieving comparatively less important and pressing objectives such as debt recovery. The Commission considers that 'the interests of Australia's national economic well-being', and 'protecting the public revenue', are so broad that they could be said to include matters that are of less importance than the protection of basic human rights.

They have not been demonstrated to require the significant restrictions on human rights entailed by assistance request and notices.

133. Further, insufficient justification has been given for having a broader list of 'relevant objectives' that are applicable to TARs, as compared with compulsory notices.

134. The human rights impacts on those whose data is accessed, in particular the significant intrusions into their privacy, is the same regardless of whether an assistance measure is voluntary or mandatory as regards the entity that holds this data. In the Commission's view, it is appropriate for the same thresholds to be applicable to both requests and notices.

135. The Commission recommends that:

Recommendation 8

Proposed ss 317G(5)(a), 317L(2)(c)(i), 317T(3)(a) of the *Telecommunications Act 1997* (Cth) be amended to limit the relevant objectives that permit the giving or varying of a TAR, TAN or TCN to those related to serious crimes under Australian law.

Recommendation 9

Proposed s 317G(5) of the *Telecommunications Act 1997* (Cth) be amended to align the 'relevant objectives' applicable to TARs with those applicable to TANs and TCNs.

(c) 'Decision-making criteria'

136. Proposed ss 317P, 317Q(10), 317V and 317X(4) provide that, before giving or varying a TAN or TCN, a decision maker must be 'satisfied' that certain criteria are met as follows:

- the requirements imposed are reasonable and proportionate
- compliance is practicable and technically feasible.

137. The explanatory document states that relevant considerations under these criteria include:

> [That] the decision-maker must evaluate the individual circumstances of each notice. In deciding whether a notice is reasonable and proportionate, it is necessary for the decision-maker to consider both the interests of the agency and the interests of the provider. This includes the objectives of the agency, the availability of other means to reach those objectives, the likely benefits to an investigation and the likely business impact on the provider …
>
> The decision-maker must also consider wider public interests, such as any impact on privacy, cyber security and innocent third parties. In deciding whether compliance with the notice is practicable and technically feasible,

> the decision-maker must consider the systems utilised by a provider and provider expertise. To be satisfied, the decision-maker would need to consider material information given to the agency by the provider. It is expected that the agency would be engaged in a dialogue with the provider prior to issuing a notice. The decision-maker may also make inquiries with other persons who have relevant experience and technical knowledge.[90]

138. However, the draft Bill itself does not set out such considerations as part of the decision-making criteria, in particular the impacts on privacy and other human rights, cyber security and innocent third parties. Such factors are critical to ensuring appropriate consideration of human rights in decision-making, and should form part of the decision-making criteria that is required under the legislation rather than mere inclusion in explanatory material.

139. Legislative entrenchment of decision-making criteria is far more rights protective than its inclusion in extraneous guidance. Even assuming that the passages from the explanatory document set out above were to be reproduced in an explanatory memorandum, explanatory memoranda do not form part of the legislation. They are not binding, and indeed may only be referred to by courts interpreting legislation where the meaning of a particular provision is considered ambiguous.

140. Further, while the explanatory document states that safeguards will ensure that 'agency powers are utilised only where *necessary* for core law enforcement and security functions',[91] the *necessity* of a notice is not a specified mandatory consideration for the issue of that notice. As discussed above, a measure that limits human rights cannot be justified unless it is necessary.[92]

141. Inclusion of necessity in the decision-making criteria will substantially enhance the compliance of the scheme with Australia's international human rights law obligations, especially if combined with a complementary requirement to consider the impact on the human rights of affected persons, such as their right to privacy.

142. Another issue with the decision-making criteria is a potential gap in their interaction with the 'systemic weakness' limitation in proposed s 317ZG. As discussed above, this limitation provides that a notice cannot have the effect of requiring a provider to build or implement a systemic weakness or systemic vulnerability into a form of electronic protection. This is a key cybersecurity safeguard that seeks to prevent the weakening of encryption at a systemic level, and thereby reduce the risk of large-scale data breaches. This will commensurately reduce the risk of far-reaching and detrimental impacts on the right to privacy.

143. However, the decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) do not explicitly require a decision maker to consider the systemic weakness limitation at the time that a notice is given or varied.

144. The Commission considers that, in order to enhance the effectiveness of the proposed s 317ZG safeguard, the decision maker should need to be satisfied that a notice will not violate the systemic weakness limitation before an exercise of the power to give or vary a notice. This would also enhance the overall coherence of the draft Bill.

145. Further, while the draft Bill requires the relevant decision maker to be satisfied of the proposed decision-making criteria before giving or varying a coercive TAN or TCN, the same requirement does not apply to TARs. As previously stated, the Commission considers that it is appropriate for the same thresholds to apply to both requests and notices.

146. The Commission recommends that:

Recommendation 10

The decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) of the *Telecommunications Act 1997* (Cth) be amended to include 'necessity' as a mandatory consideration.

Recommendation 11

The decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) of the *Telecommunications Act 1997* (Cth) be amended to require the decision maker to be satisfied that the giving or varying of a notice would not require the recipient to breach the s 317ZG systemic weakness limitation.

Recommendation 12

The decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) of the *Telecommunications Act 1997* (Cth) be amended to require the decision maker to consider the impacts of the giving or varying of a notice on human rights especially privacy, on cyber security and on innocent third parties, and only allow the exercise of power if the decision maker is satisfied that the limitation of the right to privacy and other human rights is necessary and proportionate in all of the circumstances of a particular case.

Recommendation 13

Proposed s 317G of the *Telecommunications Act 1997* (Cth) be amended to insert a provision setting out the decision-making criteria applicable to the issue of TARs, in the same terms as those applicable to TANs and TCNs.

5.2 Boundaries of systemic and non-systemic effects

147. As discussed, proposed s 317ZG is a legislative safeguard that prohibits notices from having the effect of either requiring a provider to implement or build a systemic weakness or a systemic vulnerability into a form of electronic protection, or preventing providers from rectifying a systemic weakness or vulnerability.

148. Under this limitation, providers cannot be compelled to build a capability that would render systemic methods of authentication or encryption less effective.[93] Further, agencies cannot prevent providers from fixing existing systemic weaknesses, such as a security flaw in their product.[94]

149. The explanatory document states that '[t]he Australian Government has no interest in undermining systems that protect the fundamental security of communications. The new powers will have no effect to the extent that requirements would reasonably make electronic services, devices or software vulnerable to interference by malicious actors'.[95]

150. While the Commission welcomes the government's intention as set out in the explanatory document not to permit 'backdoors', it is concerned that the limitation in proposed s 317ZG may not achieve its intended effect. This is so for a number of reasons.

151. 'Systemic vulnerability' and 'systemic weakness' are not defined in the draft Bill. It is therefore unclear how these terms are to be interpreted, and exactly where a line can be drawn between a 'weakness' or 'vulnerability' that is 'systemic' opposed to non-systemic.

152. The meaning of 'systemic' is addressed in the explanatory document as follows:

> For the avoidance of doubt, this includes a prohibition on building a new decryption capability or actions that would render systemic methods of authentication or encryption less effective. The reference to systemic methods of authentication or encryption does not apply to actions that weaken methods of encryption or authentication on a particular device/s. As above, the term systemic refers to actions that impact a broader range of devices and service utilised by third-parties with no connection to an investigation and for whom law enforcement have no underlying lawful authority by which to access their personal data.
>
> The prohibition clearly limits the ability of a notice to compel a provider to re-design services that feature end-to-end encryption. If a proposed re-design had the effect of removing the default protection that all users of end-to-end encrypted services benefit from and, consequently, made their communications less secure, it would be categorised as requiring a provider

to build a systemic weakness or vulnerability into a form of electronic protection.[96]

153. However, this guidance is not embodied in the draft Bill, and still does not allow precise identification of what constitutes a systemic or non-systemic weakness or vulnerability. Further, as outlined above, a document such as the explanatory document cannot conclude the meaning of a term used in legislation, though in some circumstances it may be used to provide some guidance about that meaning.

154. By way of example of the lack of clarity of the meaning of 'systemic', the draft Bill appears to permit the government to compel a provider to send (or 'push') a notification to an individual person through an application already installed on their phone such as Facebook Messenger, suggesting that the person download software to update the application. However, the downloaded software may not be an application update, but technology that allows a law enforcement agency to access the individual's phone messages.

155. If a large number of persons became concerned about downloading application updates because of such potential access by law enforcement, and stopped updating relevant software, this would have the likely consequence of weakening the overall cybersecurity of the application.[97]

156. Accordingly, while the initial decryption measure appears to be authorised by the draft Bill, it could ultimately, in a practical sense, lead to a 'systemic' weakness, which proposed s 317ZG is intended to prevent.

157. The Commission considers that more clearly defining the meaning of 'systemic vulnerability' and 'systemic weakness' in the draft Bill will enhance the efficacy of the safeguard, as well as provide greater certainty about the extent to which the draft Bill may impinge on the rights of users of technology.

158. The potential ambiguity of the meaning of the word 'systemic' in the draft Bill raises another serious concern flowing from the fact that the validity of a coercive notice depends on the relevant assistance not violating the limitation in proposed s 317ZG.

159. A provider could be uncertain of the validity of a notice on its face, because they are unsure of whether the requirements imposed by the purported notice would have a prohibited 'systemic' effect. However, regardless of being uncertain of their obligations, a provider faces a significant civil penalty for non-compliance. This may cause a provider either not to comply with a valid notice, because of an incorrect belief that the s 317ZG limitation applies, or to comply with an invalid notice because of a fear of the consequences.[98]

160. Further, this lack of clarity brings into question the lawfulness of any interference with privacy or other human right under a purportedly valid notice, given that any limitation on a human right must be provided for by law in a clear and precise manner.

161. Academic commentators and the Australian Law Reform Commission (ALRC) have stated that the requirement that criminal laws be sufficiently clear, and not operate retrospectively, may be breached where the scope of an offence is uncertain until it has been interpreted by the courts.[99] The Commission considers that the same risk may apply where the scope of provisions that can lead to the imposition of a substantial civil penalty is unclear.

162. Given the serious consequences of non-compliance, it is important for providers to be able to seek review of the validity of a notice in an accessible and efficient forum.[100] The Commission considers, as discussed at Pt 5.6 below, that it is appropriate to afford a form of administrative review as well as potentially make *Administrative Decisions (Judicial Review) Act 1977* (Cth) (ADJR Act) review available to decisions made under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth).

163. Further, the Commission is concerned about the human rights impacts of the Bill's authorisation of other measures that permit access to otherwise private communications, including the breaking of encryption, even where the effects do not lead to a systemic weakening.

164. For example, the framework allows an agency to compel a provider to disclose a decryption key, or to provide targeted decryption assistance (for example, of certain communications). While *prima facie* a more proportionate interference than the building of 'backdoor' ports for law enforcement, such measures still seriously interfere with the right to privacy among other rights and must be justified as lawful, necessary and proportionate.

165. For example, disclosure of an encryption key by a provider could allow an agency to scrutinise a person's complete set of digital communications on a device or service, whether past or future, not just those relevant to an investigation. Further, as with backdoor ports, the very existence of mandatory key disclosure powers could have a chilling effect on the use of information communication technologies to exercise the right to freedom of expression.

166. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated that all restrictions on encryption should be 'precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation'.[101]

167. The UN Special Rapporteur further stated that any restrictions on encryption, including mandatory key disclosure or targeted decryption, should be supervised by a court, tribunal or other independent adjudicatory body,[102] and meet the following requirements:

> Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.[103]

168. The Commission considers that the decryption powers authorised under the assistance scheme do not meet these requirements. In particular, the scope of the powers is unclear, they are not subject to judicial warrant or other independent judicial authorisation, and are also potentially not sufficiently targeted on a case-by-case basis.

169. This concern further strengthens the Commission's recommendations made above in Pt 5.1 of this submission concerning the scope of the access scheme, and below in Pt 5.6 of this submission concerning the adequacy of the proposed safeguards, including that judicial authorisation for the giving or varying of notices be required in the first instance.

170. Lastly, the Commission queries why the systemic weakness limitation in proposed s 317ZG has not explicitly been applied to TARs, and considers that the effectiveness of the limitation will be severely compromised should it not apply to voluntary assistance requests.

171. The Commission recommends that:

Recommendation 14

Proposed s 317ZG of the *Telecommunications Act 1997* (Cth) be amended to provide precise and clear definitions of 'systemic vulnerability' and 'systemic weakness'.

Recommendation 15

Proposed s 317ZG of the *Telecommunications Act 1997* (Cth) be amended to apply the systemic weakness limitation to technical assistance requests.

5.3 Interaction with warrants

172. The explanatory document states that the new assistance scheme will facilitate industry assistance, rather than serve as an independent channel to obtain private communications.[104] It states that the reforms do not change the existing mechanisms that agencies must use to lawfully access telecommunications content and data for investigations.[105] However, it is

unclear on several fronts exactly how requested or compelled assistance will interact with warrants.

173. Proposed s 317ZH provides that a TAN and TCN have no effect to the extent they require a provider to do an act or thing which would require a warrant or authorisation under the TIA Act, the SD Act, the Crimes Act, the ASIO Act or the *Intelligence Services Act 2001* (Cth). The explanatory document states that:

> This ensures that a technical assistance notice or technical capability notice cannot be used as an alternative to a warrant or authorisation under any of those acts. For example, a technical assistance notice or technical capability notice cannot require a provider to intercept communications; an interception warrant under the TIA Act would need to be sought. However, a notice may require a provider to assist with the access of information or communications that have been lawfully intercepted.[106]

174. If the intention of the framework is to facilitate assistance to access or make intelligible information that has already been obtained under a warrant, the Commission considers that the existence of a warrant should be made a precondition for the issue of a TAR, TAN or TCN. This will help confine the powers to the obtaining of technical assistance rather than the exercise of investigatory powers.

175. Such a provision would also strengthen the nexus of the assistance framework to law enforcement and national security activities concerning serious crime, thereby enhancing its proportionality overall.

176. Further, proposed s 317ZH only explicitly applies to TANs and TCNs, leaving open the question whether a TAR could somehow permit assistance measures that would otherwise require a warrant or authorisation. The Commission considers that it would be appropriate for the draft Bill to make clear that a TAR also has no effect to the extent that an 'act or thing' requested to be done in the notice would otherwise require a warrant or authorisation.

177. It is also problematic that the effective operation of proposed s 317ZH requires that, to some degree, a provider understands what act or things require a warrant. In the event that a provider does not have such knowledge, they may perform an act or thing despite the notice being invalid and having no effect.

178. To avoid this circumstance arising, the Commission considers that providers should be made aware of whether a relevant warrant has been issued, and broadly what it permits. Providers should also be provided, at the time a notice is issued to them, with general information about what actions are only permitted under a warrant.

179. The Commission considers that, especially to assist the understanding of unsophisticated providers of their obligations, it is appropriate for the draft Bill to require that the form of a request or notice further include: a clear statement of whether compliance with a notice is voluntary or compelled; the legislative provisions which authorise the request or notice including which provision of s 317E ('listed acts or things') is relied upon; and the methods of review available to the provider.

180. The Commission recommends that:

Recommendation 16

Serious consideration be given to redrafting proposed new Pt 15 of the *Telecommunications Act 1997* (Cth), to require a warrant to be a precondition of the giving of a request or notice.

Recommendation 17

Proposed s 317ZH of the *Telecommunications Act 1997* (Cth) be amended to include references to TARs as well as TANs and TCNS, to provide that a TAR has no effect to the extent to which it requests the doing of 'acts or things' for which a warrant or authorisation is required.

Recommendation 18

Proposed ss 317H, 317JA, 317M, 317Q, 317T and 317X of the *Telecommunications Act 1997* (Cth) be amended to require that the form of request or notice or a varied request or notice given to a provider include:

- a statement about whether a relevant warrant has been issued and what it broadly permits
- general information about what actions are only permitted under a warrant
- whether compliance is voluntary or mandatory
- the legislative provisions which authorise the request or notice including which provision of s 317E ('listed acts or things') is relied upon
- the methods of review available to the provider.

5.4 Voluntary nature of requests

181. Proposed s 317G provides for the giving of a TAR. Proposed s 317H provides for the form of a TAR.

182. The heading of Division 2 of proposed new Pt 15 is 'Voluntary technical assistance'. The heading of proposed s 317G is 'Voluntary technical assistance provided to ASIO, the Australian Secret Intelligence Service, the

Australian Signals Directorate or an interception agency'. While these aspects of the legislation, as well as the explanatory document, state that a TAR is voluntary, the Commission is concerned that providers may not properly understand their optional nature.

183. The receipt of a TAR from a government agency, especially if in writing and, for example, from the Director-General of ASIS, may take on a level of formality and pressure for a provider to comply despite being under no lawful compulsion. Again, this is particularly a concern with respect to less sophisticated providers.

184. The Commission considers that proposed s 317G should explicitly provide that a TAR is voluntary. Further, proposed s 317H should require that the form of a TAR include notification that the request is voluntary and that there is no penalty for non-compliance.

185. The Commission further considers that it is generally appropriate for voluntary requests to mandatorily precede compelled assistance.

186. Given that TARs are less rights restrictive, in the absence of evidence that compulsion is required in the first instance, it is preferable for the framework to operate in a graduated manner.

187. Mandating the giving of a TAR before any notice is issued, unless exceptional and urgent circumstances exist, will enhance the proportionality of the giving of notices in the event that a TAR is insufficient.

188. The Commission recommends that:

Recommendation 19

Proposed s 317G of the *Telecommunications Act 1997* (Cth) be amended to explicitly provide, whether by provision or explanatory note, that compliance with a TAR is voluntary.

Recommendation 20

Proposed s 317H of the *Telecommunications Act 1997* (Cth) be amended to require that the form of a TAR include notification to the provider that the request is voluntary and that there is no penalty for non-compliance.

Recommendation 21

Proposed Pt 15 of the *Telecommunications Act 1997* (Cth) be amended to require the giving of a TAR before a compulsory TAN or TCN can be given, unless exceptional and urgent circumstances exist which warrant otherwise.

5.5 Secrecy provision

189. Under proposed s 317ZF(1), it is an offence for a provider (including its employees and contractors), entrusted ASIO, ASIS or ASD persons, officers of an interception agency, an officer or employee of the Commonwealth, a State or Territory or an arbitrator appointed under s 317ZK, to disclose TAR, TAN or TCN information, or information obtained in accordance with a request or notice. Such information is broadly defined and includes the very existence or non-existence of a request or notice, and the 'acts or things' done in compliance.[107]

190. The explanatory document states that the offence does not include an express requirement of harm, because 'there is a high risk that the release of sensitive information contrary to this section will cause significant harm to essential public interests, including national security and protection of public safety'.[108]

191. Proposed s 317ZF(3) creates general exceptions to the secrecy provision. It provides that information can be disclosed in connection with: the administration or execution of the Part and related provisions; for the purpose of any legal proceedings or reports of such proceedings; in accordance with any requirement imposed by law; for the purpose of obtaining legal advice in relation to the Part; or in connection with the performance of functions or the exercise of powers by ASIO, ASIS, the ASD or an interception agency.

192. Disclosures can also be made to an Inspector-General of Intelligence and Security (IGIS) official. An IGIS official may further disclose information in connection with their exercise of powers or performance of functions and duties.[109]

193. Further specific exceptions authorise disclosure for information sharing between the Director-General of ASIS, the Director-General of the ASD Director-General of Security, the Communications Access Co-ordinator and the chief officer of an interception agency, for practical assistance purposes.[110]

194. Disclosures by providers are also permitted for the purpose of disaggregated statistical reporting on the number of TARs, TANs and TCNs given to the provider.[111]

195. The penalty for disclosure of confidential information in contravention of proposed s 317ZF is up to five years imprisonment.

196. Despite the general and specific exceptions, the Commission is concerned that this sweeping criminal secrecy provision is a disproportionate and unnecessary limit on the right to freedom of expression. It also potentially

limits the right of citizens to take part in the conduct of public affairs, under art 25 of the ICCPR. Further, freedom of political communication is constitutionally protected under Australian law.

197. On one hand, the secrecy provisions can be viewed as a legislative measure intended, at least in part, to protect individuals from unlawful or arbitrary interference with their privacy rights. A key concern of providers is also likely to be the handling of their commercially confidential information, including valuable intellectual property such as source code.

198. The Commission acknowledges that criminal penalties have deterrent value and accepts that, where demonstrated to be necessary and proportionate, they can be appropriate and effective. The agencies empowered under the assistance framework are entrusted with highly sensitive information, including information regarding national security as well as information about law enforcement capabilities.

199. Criminal penalties act as an assurance to the community, both domestic and international, that private information obtained under the assistance scheme will be adequately protected.

200. On the other hand, such a legislative measure must be assessed for proportionality. The UN HR Committee considered the intersection of national security and the right to freedom of expression in General Comment 34 as follows:

> Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3 [of article 19]. It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. Nor is it generally appropriate to include in the remit of such laws such categories of information as those relating to the commercial sector, banking and scientific progress.[112]

201. In 2010, the ALRC published a report, *Secrecy Laws and Open Government in Australia*. The ALRC found that secrecy laws that expose government employees to criminal liability for the unauthorised disclosure of official information can 'sit uneasily' with open and accountable government.[113]

202. After canvassing international approaches to secrecy laws, and exploring various options for protecting official information, the ALRC formed the view that, subject to a few narrow exceptions, an approach based on harm

to essential public interests should underpin the secrecy laws carrying criminal liability in Australia.[114]

203. Applying this approach to specific secrecy offences, the ALRC recommended that:

> Recommendation 8–1 Specific secrecy offences are only warranted where they are necessary and proportionate to the protection of essential public interests of sufficient importance to justify criminal sanctions.
>
> Recommendation 8–2 Specific secrecy offences should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest, except where:
>
> > (a) the offence covers a narrowly defined category of information and the harm to an essential public interest is implicit; or
> >
> > (b) the harm is to the relationship of trust between individuals and the Australian Government integral to the regulatory functions of government.
> >
> > …
>
> Recommendation 9–4 Specific secrecy offences should generally require intention as the fault element for the physical element consisting of conduct. Strict liability should not attach to the conduct element of any specific secrecy offence.

204. The Commission considers that the explanatory material, especially in instances connected to purposes or matters other than national security and law enforcement, has not demonstrated that all notice or request information or information obtained under a notice or request is of sufficient importance to justify a requirement of secrecy, let alone criminal sanctions for disclosure. The Commission is concerned that the provision of blanket immunity is informed by the commercial interests of providers, without adequately balancing the importance of government transparency and accountability.

205. There may be further instances where the public interest in disclosure of certain information is warranted, where the essential public interest is not harmed.

206. For example, it is not clear that it is appropriate to keep government contracting arrangements with providers in relation to 'acts or things' under TARs, wholly subject to secrecy.[115]

207. There may also be instances where there is information that is relevant to political or electoral choices to be made by the Australian public, and disclosure would not harm any essential public interest.

208. This includes the ability of the public to be made aware of inappropriate use of law enforcement powers, for example in a discriminatory or arbitrary manner. As stated by the UN High Commissioner for Human Rights, whistle-blowers who disclose human rights violations should be protected.[116]

209. There may also be instances where the potential harm of disclosure of information is decreased or entirely removed by the passage of time.

210. While the Commission welcomes the exception that permits disclosure of information to IGIS officials, as well as the fact that the secrecy provisions do not extend to third parties such as journalists, government accountability depends on regular public scrutiny of government actions to the greatest extent possible. The broad secrecy provision has the opposite effect.

211. Further, the Commission notes that the role of IGIS is to monitor the activities of Australia's 'intelligence agencies', including by receiving public interest disclosures in relation to those agencies. However, the agencies which may issue requests and notices under Schedule 1 of the draft Bill include 'law enforcement agencies', which are not intelligence agencies for the purposes of the IGIS Act. It is important that an avenue for lawful public interest disclosures exist in relation to activities of agencies that do not fall within the ambit of the IGIS Act.

212. The Commission further considers it more appropriate that criminal penalties only attach to the intentional unauthorised disclosure of information that harms, or that is reasonably likely to harm, an essential public interest. This is consistent with the application of a proportionality analysis as embodied in the *Siracusa Principles* and the recommendations of the ALRC.

213. The Commission considers that less serious conduct can be addressed by less restrictive measures. For example, for misconduct that is not reasonably likely to harm essential public interests, administrative or contractual remedies could apply.[117]

214. The Commission recommends that:

Recommendation 22

Serious consideration be given to amending proposed s 317ZF(1) of the *Telecommunications Act 1997* (Cth) to include a fault element and express requirement of harm, to provide that it is an offence to intentionally make an unauthorised disclosure of information that harms, or that is reasonably likely to harm, an essential public interest.

Recommendation 23

Serious consideration be given to amending proposed s 317ZF(2)–(3) of the *Telecommunications Act 1997* (Cth) to authorise the disclosure of human rights violations made in good faith in the public interest.

Recommendations 24

Serious consideration be given to amending proposed s 317ZF of the *Telecommunications Act 1997* (Cth), to allow for lawful public interest disclosures in relation to activities of agencies that do not fall within the ambit of the IGIS Act.

5.6 Safeguards, oversight and reporting of assistance scheme

215. The Commission holds serious concerns about the effectiveness of the safeguards, oversight and reporting procedures of the proposed assistance scheme.

216. Under proposed s 317G(1), the Director-General of Security, the Director-General of ASIS, the Director-General of the ASD or the chief officer of an interception agency may give a TAR.

217. Under proposed s 317L(1), the Director-General of Security or the chief officer of an interception agency may give a TAN.

218. Proposed ss 317ZN–ZR allow the delegation of powers by the Director-General of Security, the Director-General of ASIS, the Director-General of the ASD or the chief officer of an interception agency. A delegate must comply with any written directions of the delegator.

219. In broad brush, delegation is usually permitted where the delegate is at the senior executive level of an agency, or with respect to police forces of a state or territory, at an Assistant Commissioner or a Superintendent level. Delegates are empowered to, among other things, give, vary or revoke a TAR or TAN.

220. Under proposed s 317T, the Attorney-General is empowered to give a TCN, in accordance with a request made by the Director-General of Security or the chief officer of an interception agency. The Attorney-General's powers with respect to a TCN, including giving, varying and revocation, do not appear to be delegable.

221. The explanatory document states that the delegation provisions operate to ensure that powers are 'restricted to the highest levels of Government … The people who occupy these positions are trusted to exercise suitable judgment about the propriety of requests and well equipped to consider the reasonableness and proportionality of any requirements'.[118] As

discussed further below, the Commission considers that the powers of delegation are too broad.

222. The explanatory document states that courts will retain their inherent powers of judicial review, allowing affected persons to challenge the lawfulness of a decision under the framework, including the giving of a notice.[119] Notably, the assistance framework excludes decisions made under proposed Pt 15 from review under the ADJR Act.[120]

223. Before giving or varying a TCN, the Attorney-General must give the provider the opportunity to consult, unless consultation is impracticable, the TCN must be given as a matter of urgency, or consultation is waived.[121] While this requirement adds a safeguard to protect the interests of the provider, the Commission notes that it is not absolute, and also does not serve to protect the broader public interest or human rights.

224. Proposed s 317ZS provides that the Minister must write and table a report every financial year that sets out the number of TANs and TCNs given in that year.

225. The Commission is concerned about the appropriateness of notice giving powers being solely afforded to decision makers within the agencies that seek to obtain the relevant industry assistance, again noting the significant human rights interferences and the potential civil and criminal penalty implications. This self-regulating approach raises questions about how effectively transparency and accountability can be achieved.

226. The Commission notes that similar technical capability notice-giving powers under the *Investigatory Powers Act 2016* (UK) are subject to approval by a judicial commissioner of the Investigatory Powers Tribunal,[122] being an independent statutory agency exercising judicial functions. In considering whether to approve the giving of a notice, the judicial commissioner must apply the same principles as would be applied by a court on an application for judicial review.[123]

227. The UK scheme also permits a provider to refer a notice back to the Secretary of State for review.[124] This is in addition to a 'double-lock' warrants approval process, whereby the Secretary of State and judicial commissioner must both approve the granting of certain warrants, including an interception warrant.

228. The Commission also draws attention to the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism's statement that, without effective and independent oversight and reporting of surveillance practices and techniques, the lawfulness and necessity of resulting human rights

interferences are called into question.[125] The UN Special Rapporteur further stated that all secret surveillance systems should be under the review of an effective oversight body, and all interferences authorised through an independent body.[126]

229. This accords with the view of the OHCHR, who has stated that '[i]nternal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods … Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight'.[127]

230. The Commission considers that insufficient justification has been provided for the lack of independent authorisation or oversight of notice giving powers.

231. If the intention of the assistance scheme is to supplement existing powers under warrants, it is unclear why the assistance framework cannot be subsumed into the regular warrant processes. That is, assistance powers could be authorised under a warrant. The UK model further demonstrates how judicial oversight might operate.

232. If the draft Bill is to be passed with approval mechanisms similar to its current form, the Commission considers that further restricting the delegation of assistance powers is a measure that could enhance proportionality.

233. Given the significant human rights impacts, wide discretion and finely balanced considerations involved in deciding to issue a notice, reserving this power to Ministers or a more limited cohort of the highest senior members of the public service would enhance accountability and proportionality. It would also likely limit the number of notices given to only necessary instances.

234. The Commission is further concerned about the exclusion of the ADJR Act and the sweeping immunities offered to providers under proposed s 317ZJ. These proposals engage and potentially limit an individual's rights to a fair hearing and an effective remedy under articles 14(1) and 2(3) of the ICCPR respectively.

235. While judicial review is still available through other means, such as the High Court's jurisdiction under s 75(v) of the Australian Constitution or the Federal Court's jurisdiction under s 39B(1) of the *Judiciary Act 1903* (Cth), judicial review under the ADJR Act is comparatively more clear, straightforward and accessible.[128]

236. As discussed in paragraph [159] of this submission, the various ambiguities contained in the draft Bill could lead to real questions about

whether or not a notice is within power and therefore valid. Given the potential ambiguity of a provider's legal obligations, yet the serious implications of non-compliance, the Commission considers that it is vital to have an accessible and efficient mechanism of review available.

237. Such a review process could operate at both the administrative and judicial level. For example, the draft Bill could be amended to permit merits review of a notice, as well as make judicial review available under the ADJR Act. Generally, the Commission considers that external merits review, as distinct from internal merits review, will enhance the independence and quality of a decision-making process.

238. The Commission also queries whether the protection of providers from civil liability for 'acts or things' done in compliance, or in good faith in purported compliance, with a TAN or TCN, is proportionate. The proposed immunity operates to prevent the ability of any person (not just the target of an investigation but also innocent third parties who might be harmed by a civil wrong) from bringing a civil proceeding against a provider who has complied or purported to comply with a notice in good faith.

239. As stated by the ALRC, any law that authorises what would otherwise constitute a tort should be subject to careful justification.[129] The Law Council of Australia has highlighted the declining use of executive immunities in Australian law,[130] reflecting the core tenet that government and those acting on its behalf should be subject to the same legal liabilities as any individual.[131] Further, when interpreting a statute, courts will presume that the Parliament did not intend to grant a wide immunity or authorise what would otherwise be a tort in the absence of clear language[132]—an ambiguous provision will be narrowly construed.

240. This potentially overbroad immunity is also afforded to private companies and individuals. While Crown immunities can often be justified by allowing the executive to perform a public good that might otherwise be prohibitively costly or difficult,[133] the corporate interests of for-profit providers or individuals might not always align with the public interest.

241. While such a blanket immunity will likely incentivise providers to comply with requests and notices, it may commensurately also lessen the attention providers pay to the legality of their actions, and therefore increase the impact of their actions on the privacy of third parties. This risks removing an additional check and balance in the assistance process.

242. Further, in the event that there are different acts that could be undertaken to fulfil an assistance obligation, a broad immunity heightens the likelihood of a provider opting for the most rights-intrusive option when a less restrictive measure might suffice.

243. Lastly, the Commission considers that public reporting of the number of TANs and TCNs given every financial year under proposed s 317ZS offers little effective accountability. Those metrics would provide no useful information to assess whether these TANs and TCNs were issued appropriate – either in aggregate or individually. Stronger reporting requirements would enhance the proportionality of the powers.

244. The Commission queries why more detailed reporting requirements are not feasible, such as a disaggregated summary of notices that is sanitised or redacted as necessary. Further, it sees no reason why certain disaggregated statistical information could not be provided, such as whether notices are active or expired, how many have been varied, and whether any are subject to legal challenge. Such information could increase transparency without impacting operations.

245. The Commission also considers that it is appropriate to report on the giving of TARs as well as notices.

246. The Commission recommends that:

Recommendation 25

Proposed new Pt 15 of the *Telecommunications Act 1997* (Cth) be amended to require judicial authorisation for the giving or varying of notices, potentially through existing warrant processes or otherwise through another form of independent judicial oversight.

Recommendation 26

Serious consideration be given to amending proposed ss 317ZN–ZR of the *Telecommunications Act 1997* (Cth) to restrict delegations of power to a further limited range of senior executives, for example persons who are directly responsible to the relevant chief officer.

Recommendation 27

The draft Bill should be amended to allow *Administrative Decisions (Judicial Review) Act 1977* (Cth) review of all or some decisions made under proposed Pt 15 of the *Telecommunications Act 1997* (Cth).

Recommendation 28

Proposed Pt 15 of the *Telecommunications Act 1997* (Cth) be amended to provide an avenue or mechanism for the administrative review of decisions made under Pt 15.

Recommendation 29

Proposed s 317ZJ of the *Telecommunications Act 1997* (Cth) be amended to narrow the scope of civil liability afforded to providers.

Recommendation 30

Proposed s 317ZS of the *Telecommunications Act 1997* (Cth) be amended to require reporting on TARs, and to require public reporting of as much information as is possible about requests and notices given under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth), without impacting the integrity of law enforcement operations.

6 Key human rights concerns: warrant powers

6.1 Computer access warrants

247. The draft Bill proposes to insert a new 'computer access warrant' regime into the SD Act. This would allow Commonwealth law enforcement agencies, and state and territory law enforcement agencies investigating Commonwealth offences, to apply for computer access warrants in order to search electronic devices and access content on those devices covertly and, in some instances, remotely. This would enhance the ability of law enforcement agencies to access devices at endpoints when data is not encrypted.[134]

248. If passed, the proposed changes would enable law enforcement agencies to seek computer access warrants in investigations relating to 'relevant offences',[135] recovery orders,[136] mutual assistance investigations,[137]integrity operations[138] and control orders.[139]

249. A 'relevant offence' is presently defined in the SD Act and would include, amongst others: an offence against the law of the Commonwealth (or an offence against a law of a state that has a federal aspect) that is punishable by a maximum term of imprisonment of three years or more.[140]

250. The draft Bill also proposes to broaden the definition of 'computer' in new s 6(1) of the SD Act. This change would allow law enforcement agencies to access multiple computers, and a variety of computer networks, under one computer warrant. The explanatory document states that this change is required because it is no longer realistic for law enforcement agencies to identify one particular computer on which relevant data might be stored given the increasing use of distributed and cloud-based services for processing and storing data, and the fact that individuals commonly have multiple computing devices.[141]

251. The explanatory document confirms that mobile phones are intended to fall within the new definition of 'computer', as well as other devices for storing and processing information that use computers or computing

technology such as security systems, internet protocol cameras and digital video recorders.[142] This broad definition of 'computer' means that communication devices that would not colloquially be termed 'computers' may still be the subject of a 'computer access warrant'.

252. A computer access warrant issued under proposed s 27E of the SD Act by an eligible Judge or nominated Administrative Appeals Tribunal (AAT) member could authorise law enforcement authorities to take the following action in relation to a 'target computer':

- entering specified premises for the purposes of executing the warrant
- entering any premises (such as third party premises) for the purpose of gaining entry to, or exiting, the specified premises
- using the target computer, a telecommunications facility, other electronic equipment or data storage devices in order to access data held in the target computer to determine whether it is relevant and covered by the warrant
- if reasonable in the circumstances, using any other computer (such as a third party computer) to access the relevant data (and adding, copying, deleting or altering data on that computer if necessary)
- removing a computer or other 'thing' from the premises for the purposes of executing the warrant, and also returning the computer or other 'thing' to the premises
- copying data which has been obtained that appears to be relevant and covered by the warrant
- doing anything reasonably necessary to conceal the fact that any 'thing' has been done under a computer access warrant
- intercepting a communication in order to execute the warrant
- authorising the use of any force against persons and things that is 'necessary and reasonable' to do the things specified in the warrant
- any other thing reasonably incidental to the above things.

253. It is clear that these powers have the capacity to be exercised in a manner that is highly privacy-intrusive. These powers also could engage a range of other human rights.

254. The Commission considers that, in several instances, the proposed computer warrant regime in the SD Act, and the expansion of other warrant powers in the draft Bill, go beyond what can be reasonably justified as a proportionate response to the issues that they are intended to address.

(a) Access to third party computers, communications and premises

255. As discussed above, proposed s 27E(2) of the SD Act allows for the authorisation of access to third party premises, computers and communications for the purpose of executing a computer access warrant. This would be consistent with existing provisions in s 25A of the ASIO Act.[143]

256. Given that the draft Bill seeks to insert provisions identical to proposed s 27E(2)(e) of the SD Act into new provisions in the ASIO Act,[144] as well as into the Customs Act[145] and the Crimes Act,[146] it is illustrative to extract the relevant provisions of proposed s 27E (2)below:

> 27E(2) The things that may be specified are any of the following that the eligible judge or nominated AAT member considers appropriate in the circumstances:
>
> (a) entering specified premises for the purposes of doing the things mentioned in this subsection;
>
> (b) entering any premises for the purposes of gaining entry to, or exiting, the specified premises;
>
> ...
>
> (e) if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so:
>
> (i) using any other computer or a communication in transit to access the relevant data; and
>
> (ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit ...

(i) Access to third party premises for the purpose of executing a warrant

257. The explanatory document justifies the need for possible access to third party premises for the purpose of executing a computer access warrant as follows:

> This may be because there is no other way to gain access to the subject premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common premises). It may also occur where, for operational reasons, the best means of entry might be through adjacent premises (for example, where entry through the main entrance may involve too great a risk of detection). The need to access third party premises may also arise due to 'emergency' and unforeseen circumstances (for example, where a person arrives at the subject premises unexpectedly

during a search and it is necessary to exit through third party premises to avoid detection).[147]

258. In situations such as the ones outlined above, the Commission accepts that it might be legitimate for law enforcement agencies to access third party premises for the purposes of executing a computer access warrant. However, entry into the homes or businesses of innocent people limits their right to privacy protected by article 17 of the ICCPR.

259. To avoid being arbitrary, such entry must be demonstrated to be necessary and proportionate to achieve the relevant law enforcement or national security purpose. The Commission therefore considers that access to third party premises should be limited to cases where it is *necessary* to execute the warrant. The current scope of proposed s 27E(2) is not explicitly limited to cases of necessity. Rather, under proposed s 27E(2)(b), an eligible judicial officer or nominated AAT member may authorise the entering of any premises for the purpose of gaining entry to, or exiting, a specified premises if they consider it to be 'appropriate' in the circumstances.

260. An identical provision exists in s 25A(4)(aaa) of the ASIO Act and the draft Bill would insert another one into a new s 25A(8)(e) of the ASIO Act. For the reasons given above, the Commission considers that this legislation should also be amended so that warrants under the ASIO Act may only permit access to third party premises in cases where it is *necessary* to execute the warrant.

261. The Commission recommends that:

Recommendation 31

Proposed ss 27E(2)(b) and 27E(7)(e) of the *Surveillance* Devices *Act 2004* (Cth) be amended to ensure that a computer access warrant may only authorise access to third party premises where it is *necessary* to execute the warrant.

Recommendation 32

Section 25A(4)(aaa) and proposed s 25A(8)(e) of the *Australian Security Intelligence Organisation Act 1979* (Cth) be amended to ensure that a computer access warrant may only authorise access to third party premises where it is *necessary* to execute the warrant.

(ii) Access to third party computers and communications for the purpose of executing a warrant

262. As extracted above, the draft Bill proposes to insert a new s 27E(2)(e) into the SD Act, which would enable the use of a third party computer or a

communication in transit for the purpose of obtaining access to the relevant data under a computer access warrant. This is consistent with existing provisions in the ASIO Act.[148]

263. Proposed s 27E(2)(e) also permits the adding, copying, deleting or altering of other data in the third party computer or of a communication in transit if necessary to access the relevant data.

264. Proposed s 27E(2)(e) sets out a legislative safeguard, providing that warrants may only authorise access to third party computers and communications where it is reasonable in all the circumstances, having regard to other methods of obtaining access to the data which are likely to be as effective.

265. Accessing third party computers, where the individuals affected are not suspected of being engaged in criminal activities, or a direct threat to national security, in order to gain access to a target computer potentially authorises highly intrusive interferences with the right to privacy.

266. In order to better protect against arbitrary interferences of privacy, the Commission recommends that the legislative safeguard in proposed s 27E(2)(e) be amended. It should ensure that a warrant may only authorise access to third party computers or communications in transit where the issuing authority is satisfied that access is *necessary* in all the circumstances, having regard to other methods of obtaining access to the data which are likely to be as effective, and having regard to the human rights of relevant parties, including their right to privacy. An issuing authority should only allow access to third party computers or communications in transit after considering the human rights of relevant parties and being satisfied that the limits on their privacy and other human rights are proportionate in the circumstances.

267. The draft Bill also seeks to insert provisions identical to proposed s 27E(2)(e) of the SD Act into numerous sections of the ASIO Act,[149] as well the Crimes Act[150] and the Customs Act.[151]

268. For the reasons discussed above, the Commission recommends that equivalent changes be made to each of these proposed provisions.

269. The Commission recommends that:

Recommendation 33

Warrants relating to computer access under the *Australian Security Intelligence Organisation Act 1979* (Cth), the *Surveillance Devices Act 2004* (Cth), the *Crimes Act 1914* (Cth) and the *Customs Act 1901* (Cth) should only authorise access to third party computers or communications in transit where the issuing authority is satisfied that access is necessary in all the

circumstances, having regard to other methods of obtaining access to the data which are as likely to be as effective, and having regard to the human rights of the third party, including their right to privacy.

Recommendation 34

Warrants relating to computer access under the *Australian Security Intelligence Organisation Act 1979* (Cth), the *Surveillance Devices Act 2004* (Cth), the *Crimes Act 1914* (Cth) and the *Customs Act 1901* (Cth) should require the issuing authority to consider the human rights of any third party, including their right to privacy, and should only allow access to third party computers or communications in transit if satisfied that the limits on their human rights are proportionate.

6.2 Concealment of access provisions

270. The draft Bill proposes to attach broad 'concealment of access' powers to computer access warrants issued under the SD Act and computer access warrants and identified person warrants issued under the ASIO Act.

271. If any 'thing' has been done in relation to a computer under a warrant, proposed s 27E(7) of the SD Act and proposed ss 25A(8), 27A(3C) and 27E(6) of the ASIO Act would authorise the doing of any 'thing' that is reasonably necessary to conceal the fact that something had been done under the warrant.

272. The timeframes provided for these concealment activities include any time while the warrant is in force, within 28 days after it ceases to be in force or 'at the earliest time after that 28 day period at which it is reasonably practicable'.[152]

273. The explanatory document explains the claimed need for this period of time as follows:

> The period of time provided to perform these concealment activities recognises that, operationally, it is sometimes impossible to complete this process within 28 days of a warrant expiring. The requirement that the concealment activities be performed 'at the earliest time after the 28-day period at which it is reasonably practicable to do so' acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.[153]

274. The Commission acknowledges the importance of operational need and recognises that, where covert surveillance is demonstrated to be necessary and proportionate to achieving a legitimate objective, it is important that the relevant powers are effective. However, it also holds serious concerns that the proposed 'concealment of access' powers might

allow for highly privacy-intrusive activities to occur long after a warrant has expired.

275. By way of example, it is not difficult to conceive of a situation where the subject of a covert computer access warrant leaves Australia before a security or law enforcement agency takes action to conceal the fact that access to a computer has occurred. If not considered 'reasonably practicable' for the suspect to be pursued into a foreign jurisdiction, the 'concealment of access' powers would arguably empower law enforcement authorities or ASIO to covertly access the subject's computer (to do anything reasonably necessary to conceal the fact that access had previously been obtained) when they return to Australia. This could be after a significant amount of time has passed (possibly years) and could occur without any further authorisation from an eligible Judge or nominated AAT member or, in the case of ASIO warrants, the Attorney-General.

276. The Commission considers that, given the privacy-intrusive nature of the activities authorised by a computer access warrant and the concealment of access powers, it is not reasonable to continue to place reliance upon the original 'reasonable suspicion/reasonable grounds' threshold that underpinned the initial warrant if significant time has passed. This is particularly true when the facts and circumstances of an investigation might have changed considerably in the intervening period.

277. If it is not reasonably practicable for 'concealment of access' to occur while the warrant is in effect, or within 28 days of its expiry, the Commission recommends that law enforcement authorities be required to return to an eligible Judge or nominated AAT member or, in the case of ASIO warrants, the Attorney-General for further authorisation.

278. The Commission recommends that:

Recommendation 35

Proposed s 27E(7)(k) of the *Surveillance Devices Act 2004* (Cth) be deleted. If it is not reasonably practicable for 'concealment of access' to occur while the computer access warrant is in effect, or within 28 days of its expiry, the Commission recommends that provision be made in the legislation for law enforcement authorities to return to an eligible Judge or nominated AAT member for further authorisation.

Recommendation 36

Proposed ss 25A(8)(k), s 27A(3C)(k), s 27E(6)(k) of the *Australian Security Intelligence Organisation Act 1979* (Cth) be deleted. If it is not reasonably practicable for 'concealment of access' to occur while the computer access

warrant is in effect, or within 28 days of its expiry, the Commission recommends that provision be made in the legislation for ASIO to return to the Attorney-General for further authorisation.

6.3 Ancillary interception powers

279. The draft Bill seeks to expand the warrant regimes relating to accessing computer data under the ASIO Act and the SD Act, so that warrants issued under those regimes may authorise the interception of communications passing over a telecommunications system if this interception is for the purpose of doing 'any thing' specified in the warrant.[154]

280. This marks a significant departure from the current warrant regime under the ASIO Act, where s 33(1) explicitly states that computer access warrants, foreign intelligence warrants and identified persons warrants issued under the ASIO Act *do not* authorise the interception of a communication passing over a telecommunication system.

281. The explanatory document explains the reason for this change as follows:

> Currently, ASIO is required to obtain a computer access warrant to gain access to a device and a telecommunications interception warrant under section 9 or 9A of the TIA Act for this interception to establish computer access.
>
> The threshold requirements for issuing computer access warrants and telecommunication interception warrants currently differ. In some circumstances, ASIO can obtain a computer access warrant, but cannot obtain a telecommunications interception warrant. This reduces the likelihood of a successful execution of the validly issued computer access warrant. It is undesirable for ASIO's ability to execute a computer access warrant to be dependent on its ability to obtain a separate telecommunications interception warrant. Ordinarily, warrants authorise a person to undertake all activities normally required to give effect to the warrant, independently of any other warrant or authorisation.
>
> The current arrangements also cause administrative inefficiency by requiring ASIO to prepare two warrant applications, addressing different legal standards, for the purpose of executing a single computer access warrant. The process requires the Attorney-General to consider each application separately and in accordance with each separate criterion.[155]

282. Currently, if ASIO needs to intercept a communication passing over a telecommunication system to execute a warrant, it is required to seek a telecommunication interception warrant under s 9 or s 9A of the TIA Act.

283. Under the combined effect of ss 5F, 5G, 5H and 6 of the TIA Act, a communication is 'intercepted passing over a telecommunications system'

if that communication is listened to, or recorded by any means, without the knowledge of the person making it, between being sent or transmitted by the person sending it and becoming accessible to the intended recipient. The draft Bill proposes to make the same definition applicable to the ASIO Act.[156]

284. Section 7 of the TIA provides that, subject to certain exemptions (including pursuant to a warrant under s 9 or s 9A), it is not otherwise lawful to intercept communications passing over a telecommunication system. This protection is appropriate because intercepting and recording the private communications of individuals without their knowledge is a significant limitation on the right to privacy.

285. Covert interception of private communications by government, including contemporaneous communications, can reveal sensitive information about all aspects of an individual's life. This kind of government surveillance represents a distinct intrusion into privacy rights and, as discussed above, can have a significant chilling effect on the exercise of rights and freedoms. Consequently, any proposal to broaden the interception powers of government should be carefully scrutinised.

286. Presently, a warrant can only be issued under either s 9 or s 9A of the TIA if the Attorney-General is satisfied that there is a sufficient nexus to 'activities prejudicial to security'.

287. However, a computer access warrant can be issued under s 25A of the ASIO Act if the Attorney-General is satisfied that:

> … there are reasonable grounds for believing that access by the Organisation to data held in a computer (the target computer) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the security matter) that is important in relation to security.

288. Instead of a nexus to activities 'prejudicial to security', as in ss 9 and 9A of the TIA Act, the test for computer access warrants under s 25A of the ASIO Act only requires the data held in the target computer to be intelligence in respect of a security matter that is 'important' in relation to security.

289. Consequently, by attaching ancillary interception powers to the issuance of a computer access warrant under s 25A of the ASIO Act, the draft Bill appears to lower the threshold for the interception of communications passing over a telecommunications system.

290. On the material provided in the explanatory document, the Commission is not persuaded that lowering the interception threshold and attaching broad ancillary interception powers to computer access warrants is a necessary and proportionate limitation on human rights.

291. Reference in the explanatory document to concerns about the 'administrative inefficiency' involved in requiring ASIO to prepare two warrant applications is unpersuasive. A desire to decrease administrative inefficiency cannot be a legitimate objective for laws which so significantly curtail fundamental human rights such as the right to privacy. Further, the fact that ASIO sometimes fails to obtain a telecommunication interception warrant suggests that certain applications may fall below the current legislative test for lawful interception.

292. There is nothing in the explanatory document to suggest that the current threshold for interception warrants in the TIA Act is inappropriate given the intrusive nature of the powers these warrants authorise.

293. The explanatory document states that 'it is almost always necessary for ASIO to undertake limited interception for the purposes of executing a computer access warrant',[157] but provides no further detail about why this is needed, or the kinds of interceptions that are regularly undertaken or contemplated by ASIO, or why the existing threshold for interception under the ASIO Act is inappropriate.

294. While acknowledging that the ancillary interception powers are limited to interception 'for the purposes of doing any thing specified in the warrant', given the breadth of activities that may be authorised under a computer access warrant, it follows that interception for the purpose of doing 'any thing' specified in the warrant might also be very broad, and in ways not apparent in the explanatory document.

295. For example, under s 25A(4)(aaa) of the ASIO Act, a computer access warrant can authorise access to a third party property for the purpose of gaining entry to, or exiting, a premises specified in the warrant. Consequently, it appears that the ancillary interception power might authorise the interception of communications passing over a telecommunications system involving the occupiers of the third party property, if such interception is for the purpose of gaining access to that third party property so as to enter the specified property to execute the warrant. Clearly, such an exercise of the ancillary interception power would significantly impact upon the human rights of innocent third parties.

296. While the Commission acknowledges that it is not aware of all the technical and operational requirements needed by ASIO or law enforcement agencies to execute computer access warrants in a variety of different circumstances, it is concerned about the potential breadth of the interception powers that the draft Bill would make available under the warrant regimes in the SD Act and the ASIO Act. This is particularly the

case given that ancillary interception powers have also been included in the 'concealment of access' provisions discussed above which presently extend beyond the expiry of a warrant.

297. In the absence of any persuasive explanation of why the ancillary interception powers are said to be needed—and in the absence of legislative drafting that is sufficiently precise to ensure that the intrusions on privacy authorised by the expanded warrant powers are in all cases reasonable and proportionate, the Commission considers that the limitations on privacy entailed by the expansion of the computer warrant powers contemplated by proposed ss 25A(4)(ba), 25A(8)(h), 27A(3C)(h), 27E2(ea), 27E(6)(h) of the ASIO Act and proposed ss 27E(2)(h) and 27E(7)(h) of the SD Act have not been demonstrated to be necessary and proportionate to achieve a legitimate objective.

298. The Commission recommends that:

Recommendation 37

Proposed ss 25A(4)(ba), 25A(8)(h), 27A(3C)(h), 27E2(ea), 27E(6)(h) of the *Australian Security Intelligence Organisation Act 1979* (Cth) and proposed ss 27E(2)(h) and 27E(7)(h) of the *Surveillance Devices Act 2004* (Cth) be amended to permit only necessary, reasonable and proportionate ancillary interception powers.

6.4 Assistance orders

299. The draft Bill proposes to insert provisions into the SD Act and the ASIO Act that would allow law enforcement agencies and ASIO to apply for 'assistance orders' relating to computer access.[158] Similar assistance order provisions already exist in the Crimes Act and the Customs Act.[159]

300. The explanatory document states that the kinds of assistance contemplated by assistance orders include compelling a target or a target's associate to provide the password, pin code, sequence or fingerprint necessary to unlock a phone, assisting with the examination of an electronic database or using relevant software to assist in obtaining a copy of particular records or files.[160]

301. Under the SD Act, law enforcement agencies would be able to apply to an eligible Judge or a nominated AAT member for an assistance order. This assistance order could require a specified person to provide any information that is 'reasonable and necessary' to allow law enforcement to access, copy, convert or make intelligible, data subject to a computer access warrant or emergency authorisation. These orders can only attach to people who have relevant knowledge of the computer or device or the

measures applied to protect the data. Such persons can include someone reasonably suspected of having committed any of the offences to which the warrant relates, as well as, among others, owners and lessees of the relevant devices, system administrators and people who have used the devices. The penalty for not complying with an assistance order under the proposed s 64A of the SD Act is a maximum of ten years of imprisonment.

302. The proposed new s 34AAA of the ASIO Act provides that the Director-General may request the Attorney-General to make an order requiring a specified person to do anything that is reasonable and necessary to allow ASIO to access, copy, convert or make intelligible, data subject to warrants under the ASIO Act. This would enable ASIO to compel those who are able to provide it with knowledge or assistance on how to access data on computer networks and devices subject to warrants to do so. Punishment for failure to comply with an assistance order would be imprisonment for five years or 300 penalty units, or both.

303. Significantly, unlike the assistance orders made under the SD Act, the Crimes Act and the Customs Act (which are issued by eligible judicial officers or nominated AAT members) the assistance orders issued under the ASIO Act are issued by the Attorney-General and do not appear to be subject to judicial or independent oversight.

304. The draft Bill also seeks to increase the penalties associated with failure to comply with the existing assistance order provisions in the Crimes Act and the Customs Act.[161]

305. The amendments would divide the existing offence for failing to comply with an assistance order under s 3LA of the Crimes Act into two: a simple offence and an aggravated offence. If the assistance order relates to an investigation into a 'serious crime', then a person can be charged with the aggravated offence. A 'serious offence' is defined in the Crimes Act as one that is punishable on conviction for a period of two years or more. The draft Bill would also increase the penalty for failing to comply with an assistance order from two years imprisonment to five years imprisonment or 300 penalty units (or both) for a simple offence or ten years imprisonment or 600 penalty units (or both) for a serious offence or a serious terrorism offence.

306. The draft Bill also seeks to make changes to the assistance order provision in the Customs Act by creating a similar bifurcated offence for failure to comply with an assistance order issued by a magistrate under s 201A of the Customs Act. If the assistance order relates to an investigation into a 'serious crime', then a person who fails to comply with an assistance order can be charged with the aggravated offence. 'Serious offence' would be

defined as having the same meaning as in the Crimes Act—one that is punishable on conviction for a period of two years or more. The penalties would also increase from the present six months imprisonment to five years imprisonment or 300 penalty units (or both) for a simple offence or ten years imprisonment or 600 penalty units (or both) for a serious offence.

(a) Disproportionality of increased penalty provisions

307. As is apparent from the discussion above, the draft Bill seeks to increase significantly the penalty provisions and the maximum terms of imprisonment for failing to comply with an assistance order across numerous pieces of federal legislation.

308. In general terms, the explanatory document claims that the changes are necessary because the current penalties are of insufficient gravity to 'incentivise compliance' with an assistance order.[162] The Commission considers that this does not sufficiently justify such a substantial increase in the penalty provisions. If the amendments to the Customs Act proposed by the draft Bill are passed, for example, the maximum term of imprisonment for failing to comply with an assistance order would increase from the present six months to ten years imprisonment. Viewed within the context of the relevant legislative schemes, the Commission is concerned that these new penalty provisions have the potential to result in criminal sentences that are disproportionate to the gravity of any offence committed.

309. Failure to comply with an assistance order relating to an investigation involving a 'serious offence' under the Crimes Act will be punishable by up to ten years imprisonment. However, a 'serious offence' under the Crimes Act is one that is punishable on conviction by two years imprisonment or more. This means that a person could be exposed to a sentence of ten years imprisonment for failing to cooperate with an investigation where the principal offence being investigated would itself only attract a sentence of two years imprisonment. This means that the commission of an offence could be punished less severely than a failure to assist law enforcement agencies in investigating that same offence. Additionally, it appears that a person could potentially be prosecuted for an offence relating to breach of an assistance order even if the underlying criminal investigation ceased or resulted in an acquittal.

310. Article 9(1) of the ICCPR provides that no person shall be deprived of their liberty unlawfully or arbitrarily. The UN HR Committee has stated that 'arbitrariness' must not be equated with 'against the law' but be

interpreted more broadly to include such elements as inappropriateness and injustice.[163] Imprisonment or a disproportionate sentence of imprisonment for a minor offence can amount to a violation of the prohibition of arbitrary arrest and detention because any deprivation of liberty provided for by law must not be disproportionate, unjust or unpredictable.[164]

311. In some cases, imprisonment or a disproportionate sentence of imprisonment for a trivial offence can also amount to cruel, inhuman or degrading treatment or punishment under article 7 of the ICCPR.[165]

312. The Commission recognises that the courts retain discretion in sentencing for offences involving breach of assistance orders and that this could potentially mitigate the harsh effect of the legislative change. However, this curial discretion is limited, and a court will have regard to the maximum sentence in determining the length of sentence.

313. In any event, the Commission does not consider that the need to 'incentivise compliance' properly justifies the introduction of grossly increased penalty provisions which, when viewed within the legislative context, might allow for criminal sentences that are disproportionate to the gravity of any offence committed.

314. The Commission considers that a maximum sentence of ten years imprisonment for failing to comply with an assistance order could only conceivably be justified in relation to investigation of the most serious offences, and when other aggravating circumstances are present, such as a failure to comply with an assistance order relating to an investigation into an inchoate offence which involves a suspected imminent and catastrophic threat to the public.

Recommendation 38

Serious consideration be given to the proportionality of the substantially increased penalty provisions in the draft Bill. A maximum sentence of ten years imprisonment for failing to comply with an assistance order should only attach to the investigation of the most serious offences and in the presence of other defined aggravating circumstances.

(b) Privilege against self-incrimination

315. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has discussed how encryption is necessary for the exercise of the right to freedom of opinion and expression in the digital age,[166] and stated that court-ordered decryption

should only be permitted when certain criteria are met, including the protection of due process rights of individuals.[167]

316. The Commission considers that the 'assistance order' regime, and the proposed new penalties, potentially impinge on the privilege against self-incrimination. This appears to be particularly relevant, for example, if a suspect is ordered to provide information, such as a password to their phone, that is only known to them—under threat of ten years imprisonment for failure to comply.

317. The privilege against self-incrimination is protected under article 14(3)(g) of the ICCPR, which provides that:

> In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality: …
>
> (g) Not to be compelled to testify against himself or to confess guilt.

318. The privilege against self-incrimination also has a long history in the common law. As the ALRC noted in its 2015 review of encroachments by Commonwealth laws on traditional rights and freedoms, the privilege can be traced back to the 12th and 13th centuries.[168]

319. The ALRC refers to comments by William Blackstone in his *Commentaries on the Laws of England* (1765-1769) that a defendant's 'fault was not to be wrung out of himself, but rather to be discovered by other means and other men'.[169]

320. In its current form in Australia, the right to claim the privilege against self-incrimination in criminal law and against self-exposure to penalties in civil and administrative law is a 'basic and substantive common law right'[170] and entitles a natural person (but not a corporation)[171] to refuse to answer any question or produce any document if it would tend to incriminate them.[172]

321. A number of rationales for the privilege against self-incrimination have been put forward.

322. A key rationale is that the privilege reduces the potential for abuses of power, particularly between an individual accused and the state. There are a range of investigatory situations in which there is 'a risk of considerable physical and psychological pressure being applied to suspects to cooperate by making incriminating statements or handing over evidence such as documents'.[173]

323. As was noted by McHugh J in *Environment Protection Authority v Caltex Refining Co Pty Ltd*, the privilege

> probably arose as a response to what was perceived as an abuse or potential abuse of power by the Crown in the examination of suspects or witnesses.

> Once the Crown is able to compel the answering of a question, it is a short step to accepting that the Crown is entitled to use such means as are necessary to get the answer. Those means need not necessarily involve physical coercion. Confessions can be obtained by inhumane means without the necessity to resort to the rack or other forms of physical torture. By insisting that a person could not be compelled to incriminate him or herself, the common law thus sought to ensure that the Crown would not use its power to oppress an accused person or witness and compel that person to provide evidence against him or herself.[174]

324. Typically, where the privilege against self-incrimination is explicitly abrogated by statute, the legislation limits the use that can be made of evidence that is obtained through compulsion. As the High Court said in *X7 v Australian Crime Commission*:

> In balancing public interest considerations and the interests of the individual, legislation abrogating the privilege will often contain, as in the case of the [*Australian Crime Commission Act 2002* (Cth)], 'compensatory protection to the witness', by providing that, subject to limited exceptions, compelled answers shall not be admissible in civil or criminal proceedings.[175]

325. The *Guide to Framing Commonwealth Offences* published by the Attorney-General's Department provides that:

> If the privilege against self-incrimination is to be overridden, it is usual to include a 'use' immunity or a 'use and derivative use' immunity provision, which provides some degree of protection for the rights of individuals.[176]

326. The Guide describes each of these immunities in the following way:

> 'use' immunity—self-incriminatory information or documents provided by a person cannot be used in subsequent proceedings against that person, but can be used to investigate unlawful conduct by that person and by third parties, and
>
> 'derivative use' immunity—self-incriminatory information or documents provided by a person cannot be used to investigate unlawful conduct by that person but can be used to investigate third parties.[177]

327. The scope of the privilege against self-incrimination in the digital encryption context, and the extent to which it might be abrogated by compelling a suspect to provide information to decrypt devices obtained under a warrant, has not yet been considered by superior federal courts in Australia. Consequently, its position at law is uncertain.

328. The Supreme Court of Victoria has held, however, that to be compatible with human rights principles, statutory provisions that allow for the abrogation of the privilege against self-incrimination must be interpreted as extending derivative use immunity to a person. It also suggested that coercive powers requiring suspects to supply incriminating computer

encryption keys are not reasonable limits on the Charter protection against self-incrimination unless any evidence discovered as a result (and not otherwise discoverable) is inadmissible in any future prosecution of the person.[178]

329. Given the intrusive nature of compulsive evidence-gathering powers, the Commission considers it appropriate that restrictions be placed on the use and derivative use that can be made of information or material obtained under assistance order powers, to enhance human rights compliance.

330. The Commission recommends that:

Recommendation 39

The draft Bill be amended to make clear that assistance orders do not abrogate the privilege against self-incrimination, and to make explicit that any information obtained as a result of a person complying with an assistance order is subject to appropriate use and derivative use immunity.

7 List of recommendations

331. The Commission makes the following recommendations:

Recommendation 1

The Australian Government ensure that further and adequate time is afforded for public consultation, review and reform of the draft Bill, to enhance human rights compatibility.

Recommendation 2

Proposed s 317E of the *Telecommunications Act 1997* (Cth) be redrafted in narrower terms, to ensure that the 'acts or things' that can be requested or required under TARs, TANs and TCNs are restricted to those that are strictly necessary for law enforcement and national security agencies to carry out their functions.

Recommendation 3

Proposed ss 317G(6), 317L(3) and 317X(3) of the *Telecommunications Act 1997* (Cth) be amended so that the only 'acts or things' permissible under a TAR, TAN or TCN are those specified in s 317E (that is, the list of 'acts or things' in s 317E should be exhaustive in all cases).

Recommendation 4

Proposed s 317(X) of the *Telecommunications Act 1997* (Cth) be amended to make clear that a varied TCN cannot compel a provider to remove electronic protection, by excluding the applicability of s 317E(1)(a).

Recommendation 5

Proposed s 317T(5) of the *Telecommunications Act 1997* (Cth) be removed, to prevent the ability of the Minister to expand the definition of 'acts or things' for the purposes of a TCN by way of legislative instrument.

Recommendation 6

In the event that Recommendation 5 is not accepted, that the decision-making criteria in proposed s 317T(6) of the *Telecommunications Act 1997* (Cth) be amended to require the Minister to consider the right to privacy and other human rights before making a legislative instrument that will expand the definition of 'acts or things' for the purpose of a TCN, and only allow the exercise of power if the Minister is satisfied that the limitation of the right to privacy and other human rights is necessary and proportionate in all of the circumstances of a particular case.

Recommendation 7

In the event that Recommendation 5 is not accepted, proposed s 317T(5) of the *Telecommunications Act 1997* (Cth) be amended to make clear that a legislative instrument that expands the definition of 'acts or things' for the purpose of a TCN is a disallowable instrument.

Recommendation 8

Proposed ss 317G(5)(a), 317L(2)(c)(i), 317T(3)(a) of the *Telecommunications Act 1997* (Cth) be amended to limit the relevant objectives that permit the giving or varying of a TAR, TAN or TCN to those related to serious crimes under Australian law.

Recommendation 9

Proposed s 317G(5) of the *Telecommunications Act 1997* (Cth) be amended to align the 'relevant objectives' applicable to TARs with those applicable to TANs and TCNs.

Recommendation 10

The decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) of the *Telecommunications Act 1997* (Cth) be amended to include 'necessity' as a mandatory consideration.

Recommendation 11

The decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) of the *Telecommunications Act 1997* (Cth) be amended to require the decision maker to be satisfied that the giving or varying of a notice would not require the recipient to breach the s 317ZG systemic weakness limitation.

Recommendation 12

The decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) of the *Telecommunications Act 1997* (Cth) be amended to require the decision maker to consider the impacts of the giving or varying of a notice on human rights especially privacy, on cyber security and on innocent third parties, and only allow the exercise of power if the decision maker is satisfied that the limitation of the right to privacy and other human rights is necessary and proportionate in all of the circumstances of a particular case.

Recommendation 13

Proposed s 317G of the *Telecommunications Act 1997* (Cth) be amended to insert a provision setting out the decision-making criteria applicable to the issue of TARs, in the same terms as those applicable to TANs and TCNs.

Recommendation 14

Proposed s 317ZG of the *Telecommunications Act 1997* (Cth) be amended to provide precise and clear definitions of 'systemic vulnerability' and 'systemic weakness'.

Recommendation 15

Proposed s 317ZG of the *Telecommunications Act 1997* (Cth) be amended to apply the systemic weakness limitation to technical assistance requests.

Recommendation 16

Serious consideration be given to redrafting proposed new Pt 15 of the *Telecommunications Act 1997* (Cth), to require a warrant to be a precondition of the giving of a request or notice.

Recommendation 17

Proposed s 317ZH of the *Telecommunications Act 1997* (Cth) be amended to include references to TARs as well as TANs and TCNS, to provide that a TAR has no effect to the extent to which it requests the doing of 'acts or things' for which a warrant or authorisation is required.

Recommendation 18

Proposed ss 317H, 317JA, 317M, 317Q, 317T and 317X of the *Telecommunications Act 1997* (Cth) be amended to require that the form of request or notice or a varied request or notice given to a provider include:

- a statement about whether a relevant warrant has been issued and what it broadly permits

- general information about what actions are only permitted under a warrant
- whether compliance is voluntary or mandatory
- the legislative provisions which authorise the request or notice including which provision of s 317E ('listed acts or things') is relied upon
- the methods of review available to the provider.

Recommendation 19

Proposed s 317G of the *Telecommunications Act 1997* (Cth) be amended to explicitly provide, whether by provision or explanatory note, that compliance with a TAR is voluntary.

Recommendation 20

Proposed s 317H of the *Telecommunications Act 1997* (Cth) be amended to require that the form of a TAR include notification to the provider that the request is voluntary and that there is no penalty for non-compliance.

Recommendation 21

Proposed Pt 15 of the *Telecommunications Act 1997* (Cth) be amended to require the giving of a TAR before a compulsory TAN or TCN can be given, unless exceptional and urgent circumstances exist which warrant otherwise.

Recommendation 22

Serious consideration be given to amending proposed s 317ZF(1) of the *Telecommunications Act 1997* (Cth) to include a fault element and express requirement of harm, to provide that it is an offence to intentionally make an unauthorised disclosure of information that harms, or that is reasonably likely to harm, an essential public interest.

Recommendation 23

Serious consideration be given to amending proposed s 317ZF(2)–(3) of the *Telecommunications Act 1997* (Cth) to authorise the disclosure of human rights violations made in good faith in the public interest.

Recommendations 24

Serious consideration be given to amending proposed s 317ZF of the *Telecommunications Act 1997* (Cth), to allow for lawful public interest disclosures in relation to activities of agencies that do not fall within the ambit of the IGIS Act.

Recommendation 25

Proposed new Pt 15 of the *Telecommunications Act 1997* (Cth) be amended to require judicial authorisation for the giving or varying of notices, potentially through existing warrant processes or otherwise through another form of independent judicial oversight.

Recommendation 26

Serious consideration be given to amending proposed ss 317ZN–ZR of the *Telecommunications Act 1997* (Cth) to restrict delegations of power to a further limited range of senior executives, for example persons who are directly responsible to the relevant chief officer.

Recommendation 27

The draft Bill should be amended to allow *Administrative Decisions (Judicial Review) Act 1977* (Cth) review of all or some decisions made under proposed Pt 15 of the *Telecommunications Act 1997* (Cth).

Recommendation 28

Proposed Pt 15 of the *Telecommunications Act 1997* (Cth) be amended to provide an avenue or mechanism for the administrative review of decisions made under Pt 15.

Recommendation 29

Proposed s 317ZJ of the *Telecommunications Act 1997* (Cth) be amended to narrow the scope of civil liability afforded to providers.

Recommendation 30

Proposed s 317ZS of the *Telecommunications Act 1997* (Cth) be amended to require reporting on TARs, and to require public reporting of as much information as is possible about requests and notices given under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth), without impacting the integrity of law enforcement operations.

Recommendation 31

Proposed ss 27E(2)(b) and 27E(7)(e) of the *Surveillance Devices Act 2004* (Cth) be amended to ensure that a computer access warrant may only authorise access to third party premises where it is *necessary* to execute the warrant.

Recommendation 32

Section 25A(4)(aaa) and proposed s 25A(8)(e) of the *Australian Security Intelligence Organisation Act 1979* (Cth) be amended to ensure that a

computer access warrant may only authorise access to third party premises where it is *necessary* to execute the warrant.

Recommendation 33

Warrants relating to computer access under the *Australian Security Intelligence Organisation Act 1979* (Cth), the *Surveillance Devices Act 2004* (Cth), the *Crimes Act 1914* (Cth) and the *Customs Act 1901* (Cth) should only authorise access to third party computers or communications in transit where the issuing authority is satisfied that access is necessary in all the circumstances, having regard to other methods of obtaining access to the data which are as likely to be as effective, and having regard to the human rights of the third party, including their right to privacy.

Recommendation 34

Warrants relating to computer access under the *Australian Security Intelligence Organisation Act 1979* (Cth), the *Surveillance Devices Act 2004* (Cth), the *Crimes Act 1914* (Cth) and the *Customs Act 1901* (Cth) should require the issuing authority to consider the human rights of any third party, including their right to privacy, and should only allow access to third party computers or communications in transit if satisfied that the limits on their human rights are proportionate.

Recommendation 35

Proposed s 27E(7)(k) of the *Surveillance Devices Act 2004* (Cth) be deleted. If it is not reasonably practicable for 'concealment of access' to occur while the computer access warrant is in effect, or within 28 days of its expiry, the Commission recommends that provision be made in the legislation for law enforcement authorities to return to an eligible Judge or nominated AAT member for further authorisation.

Recommendation 36

Proposed ss 25A(8)(k), s 27A(3C)(k), s 27E(6)(k) of the *Australian Security Intelligence Organisation Act 1979* (Cth) be deleted. If it is not reasonably practicable for 'concealment of access' to occur while the computer access warrant is in effect, or within 28 days of its expiry, the Commission recommends that provision be made in the legislation for ASIO to return to the Attorney-General for further authorisation.

Recommendation 37

Proposed ss 25A(4)(ba), 25A(8)(h), 27A(3C)(h), 27E2(ea), 27E(6)(h) of the *Australian Security Intelligence Organisation Act 1979* (Cth) and proposed ss 27E(2)(h) and 27E(7)(h) of the *Surveillance Devices Act 2004* (Cth) be

amended to permit only necessary, reasonable and proportionate ancillary interception powers.

Recommendation 38

Serious consideration be given to the proportionality of the substantially increased penalty provisions in the draft Bill. A maximum sentence of ten years imprisonment for failing to comply with an assistance order should only attach to the investigation of the most serious offences and in the presence of other defined aggravating circumstances.

Recommendation 39

The draft Bill be amended to make clear that assistance orders do not abrogate the privilege against self-incrimination, and to make explicit that any information obtained as a result of a person complying with an assistance order is subject to appropriate use and derivative use immunity.

1 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 5.
2 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth).
3 International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 6.
4 See for example, SC Res 1373, UN SCOR, 4385th mtg, UN Doc S/RES/1373 (28 September 2001).
5 United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Encryption and anonymity follow-up report* (June 2018) United Nations Office of the High Commissioner for Human Rights, 11 <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUp-Report.pdf>.
6 *International Covenant on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
7 For example, the exposure of names, addresses, dates of birth, passwords and other personal information of users or consumers of Yahoo, eBay, Equifax and Uber.
8 Trischa Mann (ed), *Australian Law Dictionary* (Oxford University Press, 2nd ed, 2013).
9 David Kaye, *Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17th sess, Agenda Item 3, UN Doc A/HRC/29/32 (22 May 2015) 19 [56].
10 James B. Comey, Director: Federal Bureau of Investigation, 'Going dark: are technology, privacy, and public safety on a collision course?' (Speech delivered at the Brookings Institution, Washington D.C., 16 October 2014).
11 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 7.
12 See Monique Mann et al, Australian Privacy Foundation et al, Submission No 23 to the Joint Parliamentary Committee on Law Enforcement*, Inquiry into new Information Communication Technologies (ICTs) and the challenges facing law enforcement agencies*, 2018, 12.
13 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 5.
14 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 9.
15 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 5; *Telecommunications Act 1997* (Cth) proposed s 317ZG.
16 *Telecommunications Act 1997* (Cth) proposed s 317ZG.
17 Noting that this term can be used to refer to a range of exceptional access arrangements, beyond the building of independent ports.
18 *Telecommunications Act 1997* (Cth) proposed s 317ZG.
19 See Frank La Rue, *Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 29th sess, Agenda Item 3, UN Doc A/HRC/17/27 (16 May 2011) 15–16 [53]–[59].
20 The Explanatory Document states that s 313 of the *Telecommunications Act 1997* (Cth) already requires domestic carriers and carriage service providers to provide 'such help as is reasonably' necessary to law enforcement and national security agencies, and that the draft Bill introduces additional obligations to operate alongside s 313. See Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 8.

21 Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age,* 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) 5 [13].
22 United Nations Human Rights Committee, *General Comment No 34: Article 19, Freedoms of opinion and expression*, 102nd sess,UN Doc CCPR/C/GC/34 (12 September 2011) 1 [2].
23 United Nations Human Rights Committee, *General Comment No 34: Article 19, Freedoms of opinion and expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) 1 [3].
24 United Nations Human Rights Committee, *General Comment No 34: Article 19, Freedoms of opinion and expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) 1 [3]–[4].
25 The right to vote is protected under article 25(b) of the ICCPR; see also United Nations Human Rights Committee, *General comment No 25: Participation in public affairs, voting rights and the right of equal access to public service (Art 25)*, 57th sess, UN Doc CCPR/C/21/Rev.1/Add.7 (12 July 1996) 3 [12].
26 *The right to privacy in the digital age,* GA Res 68/167, UN GAOR, 68th sess, Agenda Item 69(b), UN Doc A/RES/68/167 (18 December 2013) 2.
27 *The right to privacy in the digital age,* GA Res 68/167, UN GAOR, 68th sess, Agenda Item 69(b), UN Doc A/RES/68/167 (18 December 2013) 2.
28 *The right to privacy in the digital age,* GA Res 68/167, UN GAOR, 68th sess, Agenda Item 69(b), UN Doc A/RES/68/167 (18 December 2013) 2.
29 Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age,* 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) 7 [20].
30 Moira Paterson, 'Surveillance in Public Places and the Role of the Media: Achieving an Optimal Balance' (2009) 14 *Media and Arts Law Review* 241, 249 quoted in Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014) [14.13].
31 See Mr Pieter Omtzigt, Rapporteur, *Mass Surveillance* (18 March 2015) Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, 34.
32 Margaret Sekaggya, United Nations Special Rapporteur, *Situation of human rights defenders*, 67th sess, Provisional Agenda Item 70(b), UN Doc A/67/292 (10 August 2012) 16-17 [61]–[62].
33 The Commission also notes the significant role that communications providers play in ensuring respect for privacy and other human rights, but does not address this issue in the current submission. See generally John Ruggie, Special Representative of the United Nations Secretary-General on the issue of human rights and transnational corporations and other business enterprises, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Protect, Respect and Remedy: a Framework for Business and Human Rights*, 8th sess, Agenda Item 3, UN Doc A/HRC/8/5 (7 April 2008).
34 United Nations Human Rights Committee, *General Comment 16: Article 17 (Right to Privacy)*, 23rd sess, UN Doc. HRI/GEN/1/Rev.1 (1988) 21 [8].
35 Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) 7 [21].
36 Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age,* 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) 8 [23].
37 United Nations Human Rights Committee, *General Comment No 34: Article 19, Freedoms of opinion and expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) 3 [11].
38 United Nations Human Rights Committee, *General Comment No 34: Article 19, Freedoms of opinion and expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) 7 [28].
39 United Nations Economic and Social Council, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc E/CN.4/1985/4, Annex (1985) [29]–[32].

40 United Nations Economic and Social Council, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, U.N. Doc. E/CN.4/1985/4, Annex (1985) [29]–[31].

41 Navi Pillay, UN High Commissioner for Human Rights, speaking at the launch of the Office of the UN High Commissioner for Human Rights publication *The right to privacy in the digital age*, quoted in Michael Vincent, 'Edward Snowden "owed a great deal" and deserves protection from prosecution: UN human rights chief', *ABC News* (online), 17 July 2014 <http://www.abc.net.au/news/2014-07-17/snowden-deserves-protection-from-prosecution3a-un-rights-chief/5603236>. This view is consistent with the *Johannesburg Principles* and *Tshwane Principles*: International Centre against Censorship, *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information* (November 1996) <http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf> and Open Society Foundations, *The Global Principles of National Security and the Right to Information*) (12 June 2013) <http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles>.

42 For example, see discussion regarding the prohibition against torture: United Nations Committee against Torture, *General Comment No 2: Implementation of article 2 by States Parties*, UN Doc CAT/C/GC/2 (24 January 2008) 2 [5].

43 United Nations Economic and Social Council, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc E/CN.4/1985/4, Annex (1985) [2].

44 United Nations Human Rights Committee, *General Comment No 35: Article 9 (Liberty and security of person),* 112th sess, UN Doc CCPR/C/GC/35 (16 December 2014) 3–4 [12].

45 United Nations Economic and Social Council, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc E/CN.4/1985/4, Annex (1985) [12].

46 Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age,* 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) 8 [34].

47 United Nations Economic and Social Council, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc E/CN.4/1985/4, Annex (1985) [10].

48 See the comments made in respect of emergency powers and counter-terrorism by Fionnuala Ní Aoláin, United Nations Special Rapporteur of the Human Rights Council, *Promotion and protection of human rights and fundamental freedoms while countering terrorism* (Advance Unedited Version) 72nd sess, Provisional Agenda Item 73(b), UN Doc A/72/43280 (27 September 2017) [14]–[16].

49 United Nations Human Rights Committee, *General Comment No 27: Article 12 (Freedom of Movement)*, 67th sess, UN Doc CCPR/C/21/Rev.1/Add.9 (2 November 1999) 3 [13]–[14].

50 United Nations Economic and Social Council, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc E/CN.4/1985/4, Annex (1985) [51].

51 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 9.

52 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 5.

53 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10.

54 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10, referring to *Telecommunications Act 1997* (Cth) proposed ss 317T(8)–(11), 317ZH.

55 The Director-General of Security is the head of ASIO pursuant to s 8(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth).
56 *Telecommunications Act 1997* (Cth) proposed Division 2 of Pt 15.
57 *Telecommunications Act 1997* (Cth) proposed Division 3 of Pt 15.
58 *Telecommunications Act 1997* (Cth) proposed Division 4 of Pt 15.
59 *Telecommunications Act 1997* (Cth) proposed s 317B.
60 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 8.
61 Proposed s 317D(1)–(2) of the *Telecommunications Act 1997* (Cth) defines 'electronic service' as a service that allows end-users to access material using a carriage service, including a website or a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery is by means of a carriage service. Under proposed s 317D(1)(c)–(d), a broadcasting or datacasting service is excluded from the definition of 'electronic service'. Proposed s 317B defines 'material' to include texts, data, speech, music or other sounds and visual images.
62 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 25–26.
63 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 25.
64 *Telecommunications Act 1997* (Cth) proposed s 317E.
65 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 9 [27]–[28].
66 *Telecommunications Act 1997* (Cth) proposed s 317ZB.
67 *Telecommunications Act 1997* (Cth) proposed ss 317ZB, 317ZC.
68 *Telecommunications Act 1997* (Cth) proposed s 317ZG(3).
69 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 8, referring to proposed ss 317P, 317Q(10), 317V, 317X(4) of the *Telecommunications Act 1997* (Cth).
70 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 11, referring to proposed s 317W(1)–(3) of the *Telecommunications Act 1997* (Cth).
71 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10, referring to proposed ss 317R(2), 317R(4), 317Z of the *Telecommunications Act 1997* (Cth).
72 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10, referring to proposed ss 317T(8)–(11), 317ZH of the *Telecommunications Act 1997* (Cth).
73 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10, referring to proposed s 317ZH of the *Telecommunications Act 1997* (Cth).
74 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10–11, referring to proposed ss 317G(5), 317L(3), 317T(3) of the *Telecommunications Act 1997* (Cth).
75 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10–11, referring to proposed ss 317G(2), 317L(2), 317T(2) of the *Telecommunications Act 1997* (Cth).
76 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 11, referring to proposed ss 317G(1), 317L(1), 317T(1), 317ZM-317ZR of the *Telecommunications Act 1997* (Cth).

77 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 11, referring to proposed s 317ZF of the *Telecommunications Act 1997* (Cth).
78 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 14, referring to proposed s 317ZS of the *Telecommunications Act 1997* (Cth).
79 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 11, referring to proposed s 317ZK(4)(b) of the *Telecommunications Act 1997* (Cth).
80 See discussion at [94]–[95].
81 *Telecommunications Act 1997* (Cth) proposed ss 317G(6), 317JA(9), 317L(3), 317Q(9).
82 *Telecommunications Act 1997* (Cth) proposed s 317T(4)(c)(i).
83 *Telecommunications Act 1997* (Cth) proposed ss 317T(4)(c)(ii), 317T(5).
84 *Telecommunications Act 1997* (Cth) proposed s 317T(6).
85 *Telecommunications Act 1997* (Cth) proposed s 317X(3).
86 As discussed at [145], the Commission holds concerns about the clarity and efficacy of proposed s 317ZG of the *Telecommunications Act 1997* (Cth).
87 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 26.
88 Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) s 317G(2)(v).
89 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 31.
90 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 34.
91 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 9.
92 See discussion at Pt 3.3(c).
93 See discussion at [97]–[98] of the submission.
94 *Telecommunications Act 1997* (Cth) proposed s 317ZG(1)(b).
95 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10.
96 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 47.
97 Ariel Bogle, 'Tech surveillance laws proposed by Australian Government aggressive critics say', *ABC News* (online), 20 August 2018 <http://www.abc.net.au/news/science/2018-08-20/tech-surveillance-laws-labelled-aggressive-by-critics/10128166>.
98 Relevantly, the immunities afforded to providers under proposed s 317ZJ would protect a provider from civil liability for or in relation to an act or thing done by the provider in compliance or in good faith in purported compliance with a notice, meaning that a provider would apparently be protected by good faith compliance with a *prima facie* valid notice. See discussion at Pt 5.6 regarding the overbroad scope of immunities.
99 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws: Retrospective Laws*, Report No 129 (2016) [13.141], citing Professor Jeremy Gans, Submission No 2 to the Australian Law Reform Commission, *Review of Commonwealth Laws for Consistency with Traditional Rights, Freedoms and Privileges*, 19 May 2014.
100 See Pt 5.6 of the submission regarding the Commission's concerns regarding the proposed review and oversight mechanisms.

101 David Kaye, *Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17th sess, Agenda Item 3, UN Doc A/HRC/29/32 (22 May 2015) 11 [32].
102 David Kaye, *Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17th sess, Agenda Item 3, UN Doc A/HRC/29/32 (22 May 2015) 11 [32].
103 David Kaye, *Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17th sess, Agenda Item 3, UN Doc A/HRC/29/32 (22 May 2015) 20 [60].
104 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10.
105 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 10.
106 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 48.
107 For example, see the definition of 'technical capability notice' information in *Telecommunications Act 1997* (Cth) proposed s 317B.
108 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 44.
109 *Telecommunications Act 1997* (Cth) proposed s 317ZF(5).
110 *Telecommunications Act 1997* (Cth) proposed ss 317ZF(6)–(11); Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 45.
111 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) s 317ZF(13).
112 United Nations Human Rights Committee, *General Comment No 34: Article 19, Freedoms of opinion and expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) 7 [30].
113 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 21.
114 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 138.
115 *Telecommunications Act 1997* (Cth) proposed s 317K.
116 Navi Pillay, UN High Commissioner for Human Rights, speaking at the launch of the Office of the UN High Commissioner for Human Rights publication *The right to privacy in the digital age*, quoted in Michael Vincent, 'Edward Snowden "owed a great deal" and deserves protection from prosecution: UN human rights chief', *ABC News* (online), 17 July 2014 <http://www.abc.net.au/news/2014-07-17/snowden-deserves-protection-from-prosecution3a-un-rights-chief/5603236>.
117 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 100.
118 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 11.
119 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 11.
120 *Administrative Decisions (Judicial Review) Act 1977* (Cth) proposed para (daaaa) of Sch 1.
121 *Telecommunications Act 1997* (Cth) proposed ss 317W, 317Y.
122 *Investigatory Powers Act 2016* (UK) c 25, s 254.
123 *Investigatory Powers Act 2016* (UK) c 25, s 254.
124 *Investigatory Powers Act 2016* (UK) c 25, s 257.

125 Martin Scheinin, *Report of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 13th sess, Agenda Item 3, UN Doc A/HRC/13/37 (28 December 2009) 19.
126 Martin Scheinin, *Report of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 13th sess, Agenda Item 3, UN Doc A/HRC/13/37 (28 December 2009) 21.
127 Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014), 12–13 [37]–[38].
128 Administrative Review Council, *Federal Judicial Review in Australia*, Report No 50 (September 2012) 72–73 [4.4].
129 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws: Immunity from Civil Liability*, Report No 129 (2016) 429.
130 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws: Immunity from Civil Liability*, Report No 129 (2016) 432, citing Law Council of Australia, Submission No 75 to the Australian Law Reform Commission, *Review of Commonwealth Laws for Consistency with Traditional Rights, Freedoms and Privileges*, 19 May 2014.
131 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws: Immunity from Civil Liability*, Report No 129 (2016) 431, citing Nicholas Seddon, *Government Contracts: Federal, State and Local* (Federation Press, 4th ed, 2009) 176.
132 *Coco v The Queen* (1994) 179 CLR 427, 436 (Mason CJ, Brennan, Gaudron and McHugh JJ).
133 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws: Immunity from Civil Liability*, Report No 129 (2016) 438.
134 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 13–14.
135 *Surveillance Devices Act 2004* (Cth) proposed s 27A(1).
136 *Surveillance Devices Act 2004* (Cth) proposed s 27A(3).
137 *Surveillance Devices Act 2004* (Cth) proposed s 27A(4).
138 *Surveillance Devices Act 2004* (Cth) proposed s 27A(5).
139 *Surveillance Devices Act 2004* (Cth) proposed s 27A(6).
140 *Surveillance Devices Act 2004* (Cth) s 6(1).
141 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 64.
142 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 64.
143 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(4)(aaa), 25A(ab).
144 *Australian Security Intelligence Organisation Act 1979* (Cth) proposed ss 25A(4)(ab), 25A(8)(g).
145 *Customs Act 1901* (Cth) proposed ss 199(4A)(c), 199B(2)(c).
146 *Crimes Act 1914* (Cth) proposed ss 3F(2A)(c), 3F(2B)(c), 3K(5)(c), 3K(6)(c).
147 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 70.
148 *Australian Security Intelligence Organisation Act 1979* (Cth) s 25A(4)(ab).
149 *Australian Security Intelligence Organisation Act 1979* (Cth) proposed ss 25A(4)(ab), 25A(8)(g), 27A(3C)(g), 27E(2)(d), 27E(6)(g).
150 *Crimes Act 1914* (Cth) proposed ss 3F(2A)(c), 3F(2B)(c), 3K(5)(c), 3K(6)(c).
151 *Customs Act 1901* (Cth) proposed ss 199(4A)(c), 199B(2)(c).
152 *Surveillance Devices Act 2004* (Cth) proposed s 27E(7)(k); *Australian Security Intelligence Organisation Act 1979* (Cth) proposed ss 25A(8)(k), 27A(3C)(k), 27E(6)(k).

153 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 73.
154 *Australian Security Intelligence Organisation Act 1979* (Cth) proposed ss 25A(4)(ba), 25A(8)(h), 27A(3C)(h), 27E(2)(ea), 27E(6)(h); *Surveillance Devices Act 2004* (Cth) proposed ss 27E(2)(h), 27E(7)(h).
155 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 57.
156 *Australian Security Intelligence Organisation Act 1979* (Cth) proposed s 4.
157 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 57.
158 *Surveillance Devices Act 2004* (Cth) proposed s 64A; *Australian Security Intelligence Organisation Act 1979* (Cth) proposed s 34AAA.
159 *Crimes Act 1914* (Cth) s 3LA; *Customs Act 1901* (Cth) s 201A.
160 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 111.
161 These amendments relate to the *Crimes Act 1914* (Cth) s 3LA and *Customs Act 1901* (Cth) s 201A.
162 Explanatory Document, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 101, 107.
163 United Nations Human Rights Committee, *Communication No* 560/1993, 59th sess, UN Doc CCPR/C/59/D/560/1993 (30 April 1997) ('*A v Australia*') [7.6].
164 Leïla Zerrougui, Chairperson-Rapporteur, *Civil and political rights, including the question of torture and detention: Report of the Working Group on Arbitrary Detention,* 61st sess, Provisional Agenda Item 11 (a), UN Doc E/CN.4/2005/6 (1 December 2004) 18 [54].
165 Severity of punishment is a factor relevant in determining whether there is violation of the prohibition or cruel, inhuman or degrading treatment or punishment. See United Nations Human Rights Committee, *General Comment No 20: Article 7 (Prohibition of torture, or other cruel, inhuman or degrading treatment or punishment)* 44th sess, UN Doc HRI/GEN/1/Rev.9 (Vol. I) (10 March 1992) 1 [4].
166 David Kaye, *Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17th sess, Agenda Item 3, UN Doc A/HRC/29/32 (22 May 2015) 19 [56].
167 David Kaye, *Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17th sess, Agenda Item 3, UN Doc A/HRC/29/32 (22 May 2015) 19 [56]. See discussion at [167].
168 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws*, Report No 129 (2016) 314.
169 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws*, Report No 129 (2016) 314, citing William Blackstone, *Commentaries on the Laws of England* (The Legal Classics Library, vol IV, 1765) 293.
170 *Reid v Howard* (1995) 184 CLR 1, 11.
171 *Environment Protection Authority v Caltex Refining Co Pty Ltd* (1993) 178 CLR 477, 500.
172 *Sorby v Commonwealth* (1983) 152 CLR 281, 288 (Gibbs CJ); *Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission* (2002) 213 CLR 543. The Australian Law Reform Commission examined the development of the privilege against self-incrimination in *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws*, Report No 129 (2016) 311–314.

173 Ian Dennis, 'Instrumental Protection, Human Right or Functional Necessity? Reassessing the Privilege against Self-incrimination' (1995) 54 Cambridge Law Journal 342, 376, cited in Queensland Law Reform Commission, *The Abrogation of the Privilege Against Self-Incrimination*, Report No 59 (December 2004) [3.14].
174 *Environment Protection Authority v Caltex Refining Co Pty Ltd* (1993) 178 CLR 477, 440 (McHugh J).
175 *X7 v Australian Crime Commission* (2013) 248 CLR 92, 112 [28] (French CJ and Crennan J).
176 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) [9.5.4].
177 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) [9.5.4].
178 *Re an application under the Major Crime (Investigative Powers) Act 2004* [2009] VSC 381, [91]–[92], [155]–[156].