Australian Human Rights Commission

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

Australian Human Rights Commission

Submission to the Parliamentary Joint Committee on Intelligence and Security

12 October 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

Contents

1 Executive summary

1. The Australian Human Rights Commission (the Commission) makes this submission to the Parliamentary Joint Committee on Intelligence and Security, in response to its review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (the Bill).
2. The Explanatory Memorandum states that the purpose of the Bill is to introduce measures to allow law enforcement and national security agencies to better deal with the challenges posed by 'ubiquitous encryption'.[1] To this end, the Bill creates a new scheme that can compel 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 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,[2] and to help fulfil Australia's international law obligations.[3]
4. However, the Bill would also authorise intrusive and covert powers that could significantly limit an individual's human rights to privacy and freedom of expression, among other rights. This includes the ability of interception agencies to access digital communications and data that would otherwise remain private; for example, encrypted messages on a phone.
5. Digital technologies facilitate connections and communication between individuals. They are also interdependent and operate across national borders. It is difficult, therefore, to confine the impact of a law that seeks to regulate such technologies to a single targeted individual. Consequently, the human rights impacts of a Bill such as this extend beyond just the people who may be of interest to law enforcement agencies, and includes the Australian public at large.
6. 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 with due regard to their right to privacy. This is a complex challenge, and can often involve a delicate balancing process.
7. 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 the rights and freedoms of

individuals. 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.

8. The Commission holds serious concerns that numerous provisions of the 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.

9. In light of the short timeframe for the preparation of submissions in response to this Bill, and its length and complexity, this submission—although lengthy—is not exhaustive. Rather, it draws attention to the key human rights concerns identified by the Commission to date.

10. The submission is based on an analysis of the effects of the Bill on human rights. The Commission acknowledges that its technological expertise in relation to some matters is limited, meaning that the human rights impacts may go beyond the analysis contained in this submission. Where indicated below, the Commission has drawn on the expertise of other organisations that have made submissions to the Department of Home Affairs (the Department) in response to the Exposure Draft of the Bill that was circulated in August 2018.

11. This submission contains 54 recommendations that aim to ameliorate the significant human rights concerns the Commission 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 8.

12. The Commission considers that the Bill should be reconsidered and redrafted in a way that strengthens the protection of relevant human rights, to ensure that the Bill is more precisely targeted at its objectives, and so that it limits human rights only to the degree demonstrated to be strictly necessary and proportionate to its objectives.

13. Given the complexity of the Bill and the significant degree to which it would limit human rights, the Commission urges that appropriate and adequate time be provided for its revision to enhance human rights compatibility.

14. The Commission would welcome the opportunity to provide further input into the development of the legal framework contemplated by the 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'.[4]

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 protected under the *International Covenant on Civil and Political Rights* (ICCPR).[5]

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.[6]

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.[7]

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 commonplace 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.[8]

25. However, the prevalence of encryption has also led to concerns about private, anonymous and untraceable cybertechnologies being used to facilitate serious crime. This kind of use by individuals has been termed 'going dark'.[9] 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 Memorandum to the Bill states that over 90% of telecommunications information being lawfully intercepted by the Australian Federal Police (AFP) now uses some form of encryption.[11]

26. While encryption might hamper law enforcement agencies' access to some information, 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 key provisions and human rights concerns

28. The Bill will create an assistance and access scheme that empowers certain agencies to request or compel a 'designated communications provider' to provide them with technical assistance.[13]

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

30. The Commission holds concerns that the proposed reforms permit significant limitations on human rights, in particular the rights to privacy and freedom of expression, in a manner that is not a necessary and proportionate response to legitimate law enforcement objectives.

31. Any improved ability of the government to conduct digital surveillance, intercept digital communications and access personal information or data in a manner that is disproportionate or unnecessary to a legitimate objective further risks a 'chilling effect' on the enjoyment of human rights.

32. Part 3 of this submission considers the ways that digital law enforcement, including the existence and use of powers that enable agencies to access encrypted devices and information, can limit human rights. It also discusses the requirements that must be met before these limits can be justified.

33. Part 4 of this submission summarises the key reforms proposed in Schedule 1 of the Bill (the assistance scheme) and Schedules 2–5 of the Bill (in relation to new warrant and other powers).

34. Part 5 of this submission analyses the key human rights issues the Commission has identified with respect to the assistance scheme in proposed Schedule 1. These include: the broad scope of the scheme; the ambiguity of the prohibition on requiring the development of a systemic weakness or vulnerability found in s 317ZG of the Bill; the lack of clarity as to how the scheme will interact with warrant provisions; the wide scope of civil immunity afforded to providers; the broad secrecy obligations; and the inadequacy of the proposed safeguards.

35. Part 6 of this submission analyses the key human rights issues identified with respect to the warrant and other powers in proposed Schedules 2–5. These include: the computer access warrant regime; ancillary interception powers; the ability for ASIO to use force in relation to interception; the scope of assistance order powers; and the immunities attaching to voluntary assistance provided to ASIO.

36. Overall, the Commission considers that further consideration and refinement of the Bill are required to ensure its compatibility with human rights.

Recommendation 1

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

3 Human rights and digital law enforcement

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

38. Articles 17 and 19 of the ICCPR enumerate Australia's commitments to protect, respect and fulfil the right to privacy and the right to freedom of expression. These rights are related and mutually reinforcing—for instance, an individual's privacy facilitates their freedom of expression.[14]

39. The Bill creates broad new powers that would enable government agencies to gain access to information that would otherwise remain private—for example, by virtue of encryption.[15]

40. 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.[16]

41. The right to freedom of expression and freedom of opinion have been described by the UN Human Rights Committee (HR Committee), the body of independent experts that monitors implementation of the ICCPR, as 'indispensable conditions for the full development of the person', 'essential for any society' and a 'foundation stone for every free and democratic society'.[17]

42. These rights are also an essential precondition for the proper protection of *all* human rights,[18] as well as the robust and representative nature of Australian democracy.

43. 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'.[19] It is also necessary for the effective exercise of the right to vote.[20]

44. With the advent of digital law enforcement, the rights to privacy and freedom of expression are under challenge. Most relevantly, the increased 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 Bill facilitate digital surveillance and interception by law enforcement agencies, thereby engaging and limiting the same human rights.

45. 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.[21]

46. 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.[22] 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.[23]

47. The OHCHR has stated that electronic surveillance, of both content and metadata, is potentially an interference with privacy and, further:

> [T]he 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.[24]

48. The 'chilling effect' of government surveillance on civil liberties has been described as the self-adjustment of behaviour by members of the community, even if their proposed actions would not have been wrongful, in the knowledge that one's interactions and communications may be recorded and judged by unknown others.[25]

49. 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.[26]

50. 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[27] and persons engaging in 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.[28]

51. Given the potentially significant and far-reaching consequences of the Bill on human rights, it is crucial to ensure that any rights limitations are necessary and proportionate. This must be done by ensuring that legislation that permits government to interfere with human rights is drafted with precision, so that relevant powers may only be exercised in appropriate circumstances. Another mechanism necessary to achieve

human rights compatibility is the provision of effective safeguards and oversight mechanisms.

3.1 Right to privacy

52. Article 17 of the ICCPR protects the right to privacy. It provides:

    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.

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

54. The right to privacy is especially important in the context of the 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 the Australian Security Intelligence Organisation (ASIO), are exempt from the operation of the *Privacy Act 1988* (Cth).

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

56. '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.[29]

57. 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.[30]

58. 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.[31]

3.2 Right to freedom of expression

59. 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.

60. 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'.[32] It also protects the freedom to seek, receive and impart information and ideas of all kinds, free from unlawful interference.

61. However, freedom of speech is not an absolute right and can be limited, as indicated in article 19(3). Any limitation must be lawful, necessary and proportionate to achieve a legitimate objective within the scope of article 19(3). 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.[33]

3.3 Permissible limitations on human rights

62. Some human rights cannot legitimately be subject to any limitation—such as the right to freedom from torture or cruel, inhuman or degrading treatment or punishment.[34]

63. However, other human rights including the rights to privacy and freedom of expression can be limited where certain criteria are met as discussed below. A measure which limits a human right also must not be arbitrary and must not jeopardise the essence of the right.

64. There is some overlap between a number of the criteria.[35] 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'.[36]

(a) Legitimate aims

65. Human rights may be limited where the limitation is necessary and proportionate to achieving a legitimate aim. The protection of the human rights of individuals endangered by serious criminal activity, such as the general public, is a legitimate aim.

66. 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.[37]

67. More generally, the *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (*Siracusa Principles*), state that national security cannot be used as a pretext for imposing vague or arbitrary rights limitations, and may only be invoked when there exists adequate safeguards and effective remedies against abuse.[38] The term 'national security' relates to matters which threaten the existence of the State, its territorial integrity or political independence—this is a high threshold and not every law criminalising conduct can properly be described as protecting national security:

> 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. [39]

(b) Necessity

68. A measure which limits 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.

69. To be 'necessary', a rights limitation 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 be proportionate to that aim.[40]

70. 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.

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.[41]

72. 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.[42]

73. To establish necessity, the proposed reforms in the Bill must be closely scrutinised to determine whether they go beyond what is genuinely needed for the purposes of law enforcement.

(c) Proportionality

74. The *Siracusa Principles* state that a rights limitation must pursue a legitimate aim and be proportionate to that aim.[43] Assessing whether a limitation is 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.

75. 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.[44]

76. The *Siracusa Principles* state that, even during a public emergency that threatens the life of a nation, any measure that derogates 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.[45]

77. 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 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 Bill

78. The key changes introduced by the Bill are:

- enhanced obligations of designated communications providers, including both onshore and offshore providers, to assist national security, intelligence 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 scheme (Schedule 1)

79. The Bill would introduce a new Pt 15 into the *Telecommunications Act 1997* (Cth), which establishes what is described in the Explanatory Memorandum as a 'new graduated approach to industry assistance'.[46] This approach empowers certain law enforcement and national security agencies to request or compel 'designated communications providers' to provide technical assistance by performing 'acts or things' in prescribed circumstances.[47]

80. The Explanatory Memorandum states that the assistance powers under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth) will not in themselves allow access to personal information like 'telecommunications intercept material, telecommunications content and telecommunications data', all of which will continue to require a warrant or authorisation pursuant to existing law.[48]

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

82. The Bill establishes a scheme with three tiers of mechanism 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,[49] 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.[50]
    - 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'.[51]
    - 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'.[52]

83. 'Interception agencies' are defined as agencies with interception powers under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), being the AFP, the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Criminal Intelligence Commission, state and territory police agencies and anti-corruption commissions.[53]

84. 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'.

85. The Explanatory Memorandum states that this definition of a 'designated communications provider' captures 'the full range of participants in the global communications supply chain, from carriers to over-the-top messaging providers'.[54] Notably, proposed s 317C extends to offshore entities that have a role in the provision of communications and related services in Australia.

86. By way of example of the breadth of providers subject to the assistance scheme, the obligations apply to the provider of an 'electronic service' as defined by proposed s 317D(1)–(2) of the Bill.[55] The Explanatory Memorandum states that an 'electronic service' may include websites, chat fora, secure messaging applications, cloud and web hosting, peer-to-peer sharing platforms and email distribution lists.[56] The Explanatory Memorandum further states that this definition is designed to capture 'a range of existing and future technologies, including hardware and software'.[57]

87. 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 scheme 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 any request or notice given to them.

88. 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.[58]

89. The Explanatory Memorandum states that the assistance requested or compelled from providers can include: the decryption of a communication or device; the provision of technical information including source code; the installation or deployment of software provided by an agency; the reformatting of data obtained under a warrant; the facilitation of access to a device or service; helping agencies test their own systems; notifying agencies of changes to services or systems; and the blocking of delivery of service to a target.[59]

90. 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.[60] 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.[61]

91. Proposed s 317ZG(1)(a) 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'.

92. The Explanatory Memorandum states that electronic protection 'includes forms of encryption or passcode authentication, such as rate limits on a device'.[62]

93. 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'.[63] As discussed below in Pt 5.2 of the submission, the terms 'systemic weakness' or 'systemic vulnerability' are not defined in the Bill.

94. The Explanatory Memorandum refers to a number of other safeguards and oversight mechanisms in the 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[64]
- 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[65]
- if a consultation notice is issued to a provider regarding a proposal to give a TCN, the Attorney-General and provider may jointly appoint a person to assess whether the TCN would contravene the s 317ZG limitation and the Attorney-General must consider any such assessment report before giving a TCN[66]
- 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[67]
- core data retention and interception capability obligations remain subject to existing legislative arrangements in the TIA Act[68]
- with respect to the giving of TANs or TCNs, the reforms will not alter the need for agencies to seek a warrant or authorisation under a relevant law of the Commonwealth or a state or territory, such as 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[69]
- 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, the imposition of pecuniary penalties or national security[70]
- the requested or compelled assistance must be in connection with 'eligible activities' 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'[71]
- the ability to issue notices is reserved to 'senior decision-makers', although delegation is possible in certain instances[72]
- 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[73]

- the Minister is required to table a report every financial year setting out the number of TARs, TANs and TCNs given[74]
- arbitration is available to resolve disputes between the government and providers regarding the terms and conditions of a notice.[75]

95. The Commission is concerned that some of these safeguards are either not fully embodied in the 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 5–7 of this submission.

4.2 Warrant powers (Schedules 2–5)

96. Key features of Schedules 2–5 of the 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 computers 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 *Australian Security Intelligence Organisation Act 1979* (Cth) (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.

97. Schedules 2–5 of the Bill propose to amend nine pieces of existing Commonwealth legislation to enhance existing warrant powers. Again, in light of the short timeframe provided for public consultation, this submission focuses on a number of impacts that the Bill would have, primarily on the rights to privacy and the freedom of expression.

5 Key human rights concerns: assistance requests and notices

98. The Commission considers that certain features of the assistance scheme in Schedule 1 of the Bill significantly limit human rights where it has not been demonstrated that such limitations are necessary and proportionate. The Commission is especially concerned about the following aspects of the scheme:

- it contains overbroad powers that are not appropriately clear and 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.

99. 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 they entail 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.

100. 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 powers are lawfully exercised in what are often complex, difficult and time-critical circumstances where a balancing of competing considerations is required.

101. Additionally, relevant law enforcement officials are often the only persons with access to the full range of relevant intelligence and other information needed 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.

102. Further, given the proposed secrecy provisions in the 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.

103. 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'

104. The assistance scheme empowers agencies to request or compel the provision of a wide range of assistance from a designated communications

provider. That assistance can take the form of doing any of the 'listed acts or things' designated in proposed s 317E.[76]

105. The Explanatory Memorandum suggests 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.[77]

106. However, the definition of 'acts or things' in the 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. For discussion about the lack of clarity as to how the assistance scheme will interact with warrants, see Pt 5.3 below.

107. 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.

108. Further, in the case of TARs and TANs, the list of 'acts or things' in the definition in proposed s 317E is not exhaustive.[78]

109. For TCNs, the list of 'acts or things' in the Bill is exhaustive in circumstances where a notice requires a provider to do something that will ensure it is *capable of giving assistance*.[79] In this circumstance, a provider cannot be made to do any 'act or thing' covered by proposed paragraph 317E(1)(a). That is, a provider cannot be compelled by a TCN to build a capability that would allow it to remove electronic protection that was applied by or on behalf of the provider.

110. However, the Minister may, by way of legislative instrument, determine further 'acts or things' that can be compelled under a TCN with respect to building a new capability.[80] It is not clear that the legislative safeguard that prevents compelled removal of electronic protection applies to this Ministerial determination power.

111. 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.[81] 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.

112. The Explanatory Memorandum states that this legislative instrument-making power:

> [A]llows the Minister to list further areas with respect to which capabilities under a notice may be built, additional to the listed acts or things in 317E … The communications industry is one of the world's most dynamic industries and it is important that law enforcement and security agencies retain the ability to combat crime and national security threats notwithstanding advances in technology'.[82]

113. The Commission acknowledges that new advances in technology may require an expansion of provider assistance. However, it considers that, rather than by way of Ministerial determination, it is 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 any further significant human rights limitations by authorising a provider to do a new act or thing.

114. Where a TCN requires a provider to give assistance it is already capable of giving, the 'acts or things' listed in proposed s 317E of the Bill are *non-exhaustive*.[83] That is, there is no limit to the forms of assistance that may be requested from a provider, if they already have the capacity to give the assistance, including the removal of electronic protection.

115. It is possible that the broad drafting of the 'acts or things' in 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 Memorandum does not demonstrate that such a broad definition is required to achieve the objectives of the Bill.

116. 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.

117. The Commission considers that, given the significant potential limitation on human rights, in particular the right to privacy, the 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.

118. 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, intelligence and national security agencies to carry out their functions.

Recommendation 3

Proposed ss 317G(6), 317L(3), 317T and 317X(3) of the *Telecommunications Act 1997* (Cth) be amended so that the only 'acts or things' that can be requested or required to be done 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 317T(5) of the *Telecommunications Act 1997* (Cth) be omitted, to remove the power of the Minister to expand the definition of 'acts or things' for the purposes of a TCN by way of legislative instrument.

Recommendation 5

In the event that Recommendation 4 is not accepted, 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.

(b) 'Relevant objectives'

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

120. 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.[84]

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

122. 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) safeguarding national security …

123. Similarly, 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) safeguarding national security.

124. The Explanatory Memorandum states that the reforms will assist the ability of law enforcement, national security and intelligence agencies to investigate organised crime, terrorism, smuggling and sexual exploitation of children.[85] The Statement of Compatibility with Human Rights further states that the Bill will 'protect national security, public safety, address crime and terrorism … [to] keep Australians safe'.[86]

125. However, the Commission notes that the relevant objectives that enliven assistance cover a large range of contexts that do not necessarily relate to serious crime or public safety, including 'imposing pecuniary penalties' and 'the interests of Australia's national economic well-being'. These terms are not defined in the Bill.

126. The Commission welcomes the removal of 'protecting the public revenue' as a relevant objective for assistance requests and notices, because this represents a narrowing from what was proposed in the Exposure Draft of the Bill. Nevertheless, it considers that the objectives that enliven the assistance powers remain so broad as to appear disproportionate.

127. With respect to pecuniary penalties, the Explanatory Memorandum states that '[p]ecuniary penalties for the purposes of this provision are not intended to encompass small-scale administrative fines. In Commonwealth, State and Territory legislation there are significant pecuniary penalties for serious breaches of the law, particularly laws regarding corporate misconduct'.[87]

128. Pecuniary penalties apply in many different areas of law, and can range from small-scale to severe sanctions. For example, on the smaller scale, a

court can apply civil penalties where individual trustees of a superannuation fund contravene their supervision obligations.[88]

129. With respect to 'the interests of Australia's national economic well-being', the Explanatory Memorandum does not explain what this could entail. It simply states that this objective 'reflects the functions of Australia's intelligence and security agencies … It is not intended to support voluntary assistance requests made by interception agencies'.[89] Judicial consideration of this phrase with respect to the functions of ASIS suggests that the evasion of Australian tax obligations by use of offshore accounts could be contrary to the interests of Australia's national economic well-being.[90]

130. 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 more difficult to establish that they will be proportionate to achieving comparatively less important and pressing objectives such as tax and superannuation compliance.

131. The Commission considers that 'the interests of Australia's national economic well-being', and 'the imposition of pecuniary penalties', are so broad that they could be said to include matters that could not justify the Bill's significant encroachment on basic human rights. They have not been demonstrated to require the significant restrictions on human rights entailed by assistance requests and notices.

132. To enhance the proportionality of the use of assistance powers, the Commission proposes that the scope of the assistance scheme be limited to objectives related to the enforcement of serious offences.

133. The definition of a 'serious offence' in s 5D of the TIA could usefully be applied, which includes acts of terrorism, sabotage, espionage, foreign interference and other serious criminal offences including child sex offences and offences that would prejudice national security.

134. Limiting the objectives to the enforcement of serious offences would also enhance the overall coherence of the assistance scheme, by aligning it more closely with the purposes for which a warrant can be issued under Pts 2–5 of the TIA Act.[91] The Commission notes the similar recommendation made by the Law Council of Australia in its submission to the Department on the Exposure Draft of the Bill.[92]

135. Further, the Commission considers that insufficient justification has been provided for having a broader list of 'relevant objectives' that are applicable to TARs, as compared with compulsory notices.

136. The human rights impacts on those whose personal information and 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.

137. The Commission recommends that:

Recommendation 6

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 a 'serious offence' as defined in s 5D of the TIA Act.

Recommendation 7

In the event that Recommendation 6 is not accepted, 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'

138. 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 by the notice are reasonable and proportionate
- compliance with the notice is practicable and technically feasible.

139. Proposed ss 317RA and 317ZAA set out the following criteria to which the decision maker must have regard in considering whether the requirements imposed by a TAN or TCN are reasonable and proportionate:

- the interests of national security
- the interests of law enforcement
- the legitimate interests of the designated communications provider
- the objectives of the notice
- the availability of other means to achieve the objectives of the notice
- the legitimate expectations of the Australian community relating to privacy and cybersecurity
- such other matters (if any) as the decision maker considers relevant.

140. The Explanatory Memorandum states that:

> [T]he 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.[93]

141. Notably, there are no decision-making criteria that guide or constrain the giving or varying of TARs.

142. The Commission welcomes the inclusion of proposed ss 317RA and 317ZAA, which were not included in the Exposure Draft of the Bill. This revision partially addresses a recommendation previously made by the Commission to the Department, that:

> [T]he Bill 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'.[94]

143. In particular, the Commission welcomes the requirement that decision makers consider the legitimate expectations of the Australian community relating to privacy and cybersecurity.

144. This provision will require that the impacts of a notice on the target individual's privacy, as well as the privacy and cyber-security of the community more broadly, are given due weight in considering also the interests and objectives of the relevant agency. This provision makes it more likely that a decision to give or vary a notice will satisfy the proportionality obligation.

145. However, the Commission considers that, given the likely fine balance that will need to be struck between imposing significant limitations on privacy as against law enforcement objectives, the privacy protections in the Bill should be further strengthened.

146. A potentially useful model is set out in s 180F of the TIA Act. Section 180F sets out several factors that authorised officers must consider and be satisfied of before disclosing or using information or documents gathered under interception powers. In particular, authorised officers must be satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate, having regard to the gravity of any conduct in relation to which the authorisation is sought, the likely relevance and usefulness of the information or documents and the reason why the disclosure or use concerned is proposed to be authorised.

147. In addition, the Commission considers that proposed ss 317RA and 317ZAA should also require a consideration of other human rights in addition to privacy, as well as the impacts on innocent third parties. Various human rights could be limited by the giving or variation of a request or notice, including—as recognised in the Statement of Compatibility with Human Rights—the right to freedom of expression and the right to an effective remedy. The Commission considers that the consideration of human rights by a decision maker is a task properly undertaken in the ordinary course of decision-making, and one that enhances the quality of the process and outcome.

148. Further, the Commission considers that the broad immunities the Bill would create for providers who act in accordance with requests and notices could detrimentally impact the rights of innocent third parties. The Commission considers that the effect of these immunity provisions should be taken into account at the time any decision is made to give or vary a request or notice.

149. If a provider acts in compliance or purported compliance with a request or notice, the provider will be immune from civil liability pursuant to proposed s 317ZJ. This immunity will limit a person's ability to bring a civil action for loss, damage or injury caused by a provider (see further discussion at Pt 5.4 below).

150. The Explanatory Memorandum itself recognises that the effect of civil immunities on third parties is an important consideration. With respect to TARs, it states that:

> [T]he persons who can make technical assistance requests occupy the most senior positions in their organisation and can exercise suitable judgment about the propriety of such a request … particularly whether it is appropriate to extend civil immunity for acts or things done consistent with the request'.[95]

151. The acknowledgement of the potential impact of these immunities in the Explanatory Memorandum is noteworthy. However, it provides no legal

constraint on the exercise of powers to give or vary requests or notices under the Bill.

152. The Commission therefore proposes that the Bill be amended to provide that any decision maker, when considering giving or varying a request or notice, must take this matter into account. The Commission has reviewed the submission prepared by the Inspector-General of Intelligence and Security (IGIS) in relation to the Exposure Draft of the present Bill. The Commission notes that similar comments were made by the IGIS in its submission to the Department.[96]

153. The Commission further welcomes the new requirement that decision makers consider the availability of other means to achieve the objectives of the notice. This will ensure consideration of the other relevant investigative avenues potentially available to law enforcement.

154. However, this criterion only mandates *consideration* of alternative measures. It does not require that the decision maker select the least rights-restrictive option available. That is, if there are other investigative options available that could achieve the relevant objective in lieu of issuing a notice, a notice could, as the Bill is currently drafted, still be issued.

155. This approach can be contrasted with the decision-making requirements applicable in some other national security and law enforcement contexts. For example, when making a continuing detention order in relation to a terrorist offender under s 105A.7 of Schedule 1 of the *Criminal Code Act 1995* (Cth) (Criminal Code), a court must be satisfied both that the offender poses an unacceptable risk of committing a serious Part 5.3 offence if released into the community and that there is no other less restrictive measure that would be effective in preventing the unacceptable risk.

156. The Statement of Compatibility with Human Rights states that '[t]he amendments only go so far as is necessary in limiting the right to privacy'.[97] The Commission disagrees, given that satisfaction as to the *necessity* of giving or varying a notice is not an essential precondition for the issue of that notice. As discussed above, a measure that limits human rights cannot be justified unless it is necessary.[98]

157. The Commission considers that requiring the decision maker to be satisfied of the 'necessity' of giving or varying a notice would be a more effective safeguard, and would substantially enhance the compliance of the scheme with Australia's international human rights law obligations.

158. 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 hacking or data breaches. This will commensurately reduce the risk of far-reaching and detrimental impacts on the right to privacy.

159. However, while the proposed decision-making criteria refer to the legitimate expectations of the Australian community relating to cybersecurity, it does not explicitly require a decision maker to consider the systemic weakness provision before giving or varying a request or notice. With respect to a proposed TCN, there is the possibility of obtaining an assessment from a jointly appointed expert as to whether the TCN would contravene s 317ZG, but this is not a mandatory requirement.

160. 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 requirement will not violate the systemic weakness limitation before exercising the power to give or vary a notice. This would also enhance the overall coherence of the Bill.

161. Further, while the 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 preferable for the same thresholds to apply to both requests and notices as appropriate.

162. The Commission recommends that:

Recommendation 8

The decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) of the *Telecommunications Act 1997* (Cth) be amended to include a requirement that the decision maker be satisfied of the 'necessity' of giving or varying a notice.

Recommendation 9

The decision-making criteria in proposed ss 317RA and 317ZAA of the *Telecommunications Act 1997* (Cth) be amended to include a requirement that the decision maker be satisfied that the giving or varying of a notice would not require the recipient to breach the s 317ZG systemic weakness limitation.

Recommendation 10

The decision-making criteria in proposed ss 317RA and 317ZAA of the *Telecommunications Act 1997* (Cth) be amended to also require that the decision maker be satisfied on reasonable grounds that:

- any interferences with privacy
- any interferences with other human rights including the right to freedom of expression and the right to an effective remedy and
- any impacts on innocent third parties, including the consequences of a provider's immunity from civil liability

are reasonable, necessary and proportionate by reference to a detailed, non-exhaustive list of considerations, such as the seriousness of any offence under investigation.

Recommendation 11

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 commensurate terms as those applicable to TANs and TCNs.

(d) Duration of requests and notices

163. A TAR and TAN will remain in force until the expiry date specified in a request or notice, or, where no date is specified, at the end of a 90 day period after it is given.[99] A TCN will remain in force until the expiry date specified in the notice, or otherwise at the end of a 180 day period after it is given.[100]

164. Therefore, the scheme permits agencies to stipulate *any* time period for a request or notice to be in force, which could include a very lengthy duration, for example 10 years. The Bill also contemplates the making of standing requests or notices, noting that the definition of 'access' in s 317B includes a 'standing request'.

165. There is no limit on the number of requests or notices that can be issued to one provider. A fresh request or notice may be issued in the same terms as an expired request or notice.

166. As a result of these broad provisions governing duration, there is the potential for requests and notices to impose onerous obligations on providers. While proposed s 317ZK(3) provides that the recipient of a notice must neither profit nor bear the reasonable costs of compliance (a no-profit no-loss model),[101] the payment of a provider's full costs is not

guaranteed. This provision allows for a provider and a costs negotiator to come to an agreement on costs, but if costs cannot be agreed they are subject to arbitration. Further, in some circumstances a decision maker can determine that it is contrary to the public interest for a provider's reasonable costs to be paid.

167. The Commission is concerned that, in light of these provisions, the Bill contains insufficient safeguards to prevent the imposition of overly oppressive obligations on providers, under the threat of significant civil penalties. Providers could be compelled to divert a large amount of staffing and other resources to fulfil their assistance obligations. This includes obligations that could span long periods of time, with the potential risk that payment of reasonable costs is not made in full or at all.

168. The lack of any maximum permissible duration and the risk of oppression is particularly concerning with respect to compulsory notice powers, recalling again that assistance may be required from unsophisticated and small providers. Such providers might be required to divert a large amount of their limited staffing and other resources to fulfil assistance obligations, limiting their ability to conduct regular for-profit activities.

169. Some protection is provided by the requirement in the mandatory decision-making criteria that the decision maker be satisfied that the requirements of any notice are 'reasonable and proportionate', and that compliance with any notice is 'practicable and technically feasible' before giving or varying a notice.[102] This includes a requirement to consider 'the legitimate interests of the designated communications provider to whom the notice relates'.[103]

170. Further, under proposed ss 317R and 317Z, a notice must be revoked by the decision maker if they are satisfied that the requirements imposed are no longer reasonable and proportionate or where compliance with the notice is no longer practicable and technically feasible. The Explanatory Memorandum states that 'the revocation provision establishes an avenue to discontinue notices that have become obsolete or excessively burdensome'.[104]

171. However, there is no mechanism in the Bill for periodic review by the decision maker of whether a notice remains reasonable, proportionate, practicable and technically feasible. Further, there is no formal mechanism for providers to raise concerns that a notice does not meet these requirements, for example that the requirements have become excessively resource intensive or otherwise too burdensome.

172. While judicial review of Pt 15 decisions is available, the right to bring such a proceeding will not provide an efficient and easily accessible means of

revoking a notice that is or has become unreasonably burdensome. As discussed at [297] below, the conduct of judicial review, especially outside the ADJR Act, can be technical, lengthy and costly.

173. To reduce the risks to providers and ensure that requests and notices are in force for the minimum necessary period, the Commission considers it appropriate to fix a maximum time limit for any single request or notice.

174. A maximum duration for requests and notices will also help to promote more regular review by decision makers of the necessity and appropriateness of the assistance requirements specified in them. An avenue of merits review should also be made available for providers to seek revocation of a notice, and to seek independent merits review of any decision not to revoke a notice (see further discussion of merits review below at [299]).

175. The Commission recommends that:

Recommendation 12

Proposed ss 317HA(1)(b) and 317MA(1)(b) of the *Telecommunications Act 1997* (Cth) be amended to provide that the maximum permissible duration of any single TAR or TAN is 90 days.

Recommendation 13

Proposed s 317TA(1)(b) of the *Telecommunications Act 1997* (Cth) be amended to provide that the maximum permissible duration of any single TCN is 180 days.

Recommendation 14

Proposed ss 317R and 317Z be amended to:

- allow a provider to apply to the decision maker for the revocation of a notice where the provider considers that the requirements imposed by the notice are not reasonable and proportionate or that compliance with the notice is not practicable and technically feasible
- make provision for a provider to access independent merits review of any decision to refuse to revoke a notice.

5.2 Boundaries of systemic and non-systemic effects

176. As discussed, proposed s 317ZG(1) 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.

177. Under this limitation, providers cannot be compelled to implement or build a capability that would render systemic methods of authentication or encryption less effective.[105] Further, agencies cannot prevent providers from fixing existing systemic weaknesses, such as a security flaw in their product.[106]

178. A TAN or TCN will have no effect to the extent to which it would have an effect prohibited by s 317ZG(1).

179. The Explanatory Memorandum states that '[n]ew section 317ZG ensures that providers cannot be required to systematically weaken their systems of electronic protection under a [notice]. The limitation is designed to protect the fundamental security of software and devices. It ensures that the products Australians enjoy and rely on cannot be made vulnerable to interference by malicious actors'.[107]

180. 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.

181. A prime example, which appears *not* to be permitted under the scheme, is requiring a company to modify a messaging application to include an independent port for law enforcement access. The creation of such a port, sometimes termed an 'encryption backdoor',[108] can greatly increase the susceptibility of an application to hacking by a malicious actor.

182. 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.

183. Such scenarios highlight the highly interconnected nature of cybersecurity technologies, and potentially pervasive consequences of measures that may be taken in response to a claimed government requirement for exceptional access.

184. While the Commission welcomes the government's intention as set out in the Explanatory Memorandum, not to mandate or permit the creation or maintenance of 'backdoors',[109] it is concerned that the limitation in proposed s 317ZG may not achieve its intended effect. This is so for a number of reasons.

185. 'Systemic vulnerability' and 'systemic weakness' are not defined in the 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' as opposed to non-systemic.

186. The meaning of 'systemic' is addressed in the Explanatory Memorandum as follows:

> A technical assistance notice or technical capability notice may, notwithstanding new paragraph 317ZG(1)(a), require a provider to enable access to a particular service, particular device or particular item of software, which would not systemically weaken these products across the market. For example, if an agency were undertaking an investigation into an act of terrorism and a provider was capable of removing encryption from the device of a terrorism suspect without weakening other devices in the market then the provider could be compelled under a technical assistance notice to provide help to the agency by removing the electronic protection. The mere fact that a capability to selectively assist agencies with access to a target device exists will not necessarily mean that a systemic weakness has been built. The nature and scope of any weakness and vulnerability will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required …
>
> Likewise, a notice or warrant may require a provider to facilitate access to information prior to or after a method of electronic protection is employed, as this does not weaken the electronic protection itself. A requirement to disclose an existing vulnerability is also not prohibited by 317ZG(1)(a).[110]

187. However, this guidance is not fully embodied in the Bill itself. An Explanatory Memorandum does not form part of the relevant legislation, is not binding, and indeed may only be referred to by courts interpreting legislation where the meaning of a particular provision is considered ambiguous. In any event, the passage above still does not allow precise identification of what constitutes a systemic or non-systemic weakness or vulnerability.

188. By way of example of the lack of clarity of the meaning of 'systemic', the 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.

189. 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.[111]

190. Further, while a single 'act or thing' might be authorised under an individual request or notice that has been given, the results of the assistance rendered might be able to be used again and again. This extends to use by the relevant agency on different future occasions for different purposes, or potentially by multiple different agencies if request or notice information is shared between agencies pursuant to s 317ZF(6)–(11). For example, it is possible that information provided or an action performed by one provider in compliance with one notice could be re-used by an agency for future warrant operations.

191. Accordingly, while an initial decryption measure could be authorised by a notice, it could ultimately, in a practical sense, decrease the cybersecurity of communications or devices over the long term, leading to a 'systemic' weakness, which proposed s 317ZG is intended to prevent.

192. With respect to TCNs, some additional protection is afforded by the requirement that the Attorney-General consult with a provider before giving a notice, and the possibility of jointly appointing an assessor to consider whether the proposed TCN would contravene s 317ZG. However, as discussed below at [283], there are exceptions to the requirement to consult with providers before issuing a TCN.

193. The Commission considers that more clearly defining the meaning of 'systemic vulnerability' and 'systemic weakness' in the Bill would enhance the efficacy of the safeguard in s 317ZG, as well as provide greater certainty about the extent to which the Bill may impinge on the rights of users of technology.

194. The potential ambiguity of the meaning of the word 'systemic' in the 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.

195. 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.[112]

196. Further, this lack of clarity brings into question the 'lawfulness' for the purposes of human rights law 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.

197. The Australian Law Reform Commission (ALRC) and academic commentators 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.[113] 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.

198. 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.[114] 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 in relation to decisions made under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth).

199. 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 weakness or vulnerability.

200. For example, the scheme 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.

201. 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.

202. 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'.[115]

203. 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,[116] 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.[117]

204. 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.

205. 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.

206. 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.

207. The lack of this protection with respect to TARs is even more significant given that agencies might be able to request that a provider voluntarily do an act or thing that the agency itself would otherwise require a warrant or authorisation to do (see further discussion of interaction between the scheme and warrants below at Pt 5.3). This potential operation of TARs does not appear to be reasonable, necessary or proportionate, in light of the lack of adequate safeguards to prevent unlawful interferences with human rights. If a provider acts in compliance with a TAR, it will also be afforded immunity from civil liability for any harm, damage or loss caused, narrowing the rights of innocent third parties to bring a claim for a civil wrong (see further discussion of immunities below at Pt 5.4).

208. The Commission recommends that:

Recommendation 15

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

Recommendation 16

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

209. The Statement of Compatibility with Human Rights states that the new assistance scheme will 'facilitate law enforcement, security and intelligence agencies' access to private communications and data where an *underlying warrant or authorisation is present*' (emphasis added).[118] It further states that the new provisions 'complement, but do not replace, the existing warrant processes with in-built legislative safeguards'.[119] However, it is unclear on several fronts exactly how requested or compelled assistance will interact with warrants.

210. 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, the *Intelligence Services Act 2001* (Cth), or other law of the Commonwealth or a law of a state or territory. The Explanatory Memorandum 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.[120]

211. If the intention of the scheme 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.

212. Such a provision would also help strengthen the nexus of the assistance scheme to agency functions and powers that concern serious offences, thereby enhancing its proportionality overall.

213. Further, proposed s 317ZH only explicitly applies to TANs and TCNs, leaving open the question whether a TAR could somehow permit assistance measures by providers, which would bypass the usual warrant and authorisation requirements that apply to the relevant agency.

214. The Commission considers that it would be appropriate for the Bill also to impose the limits on TANs and TCNs in proposed s 317H to TARs. That is, the Bill should 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. The potential adverse consequences of this gap are even more significant given that providers will be afforded far-reaching civil immunity, and limited criminal immunity, for acting in compliance or purported compliance with a notice (see further discussion of immunities below at Pt 5.4). This would limit the ability of innocent third parties to bring an action for loss, damage or harm against providers, even where the act or thing performed would usually require the relevant agency to hold a warrant.

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

216. 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 with general information about what actions are unlawful in the absence of a warrant, at the time a notice is issued to them.

217. With respect to TARs, the Commission welcomes the insertion of new proposed s 317HAA requiring that the relevant decision maker advise a provider that compliance with a TAR is voluntary. This change from the Exposure Draft of the Bill implements a recommendation previously made by the Commission to the Department.[121]

218. Similarly, the Commission welcomes new proposed s 317MAA with respect to TANs and new proposed s 317TAA with respect to TCNs, requiring the relevant notice-giver to advise a provider of their obligations under s 317ZA or s 317ZB. Those obligations include that a provider must comply with a notice requirement 'to the extent that they are capable of doing so'.

219. However, the Commission considers that it is unclear whether the requirement to advise of an 'obligation' includes notifying a provider that non-compliance with a notice is mandatory under threat of civil penalty.

220. For clarity of understanding, the Commission considers that the provider should be notified of the voluntary or mandatory nature of the assistance, and other important information, in writing and as part of the request or notice itself. Proposed s 317HAA currently appears to allow oral advice to

be given to providers, and the notification to occur separately from the request or notice.

221. Accordingly, especially to assist the understanding of unsophisticated providers of their obligations and the consequences of non-compliance, the Bill should require that the *form* of a request or notice include: the legislative provisions that authorise the request or notice including which paragraph/s of s 317E(1) ('listed acts or things') are relied upon; a clear statement of whether compliance with a notice is voluntary or mandatory; that civil penalties apply to non-compliance with a notice; and the methods of review available to the provider.

222. The Commission further considers that, in general, a graduated approach to the issuing of requests and notices will enhance the proportionality of the scheme. That is, in the first instance, a request for voluntary assistance is preferable to a compulsory notice. The Explanatory Memorandum states that Schedule 1 introduces a '*graduated* approach to industry assistance' (emphasis added), but this is not embodied in the Bill.[122] Only where a TAR is unsuccessful or there are exceptional circumstances such as urgency, should a compulsory notice be issued.

223. The Commission recommends that:

Recommendation 17

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 18

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 19

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 the requested act or thing assists in giving effect to an extant warrant or authorisation, and what that warrant or authorisation broadly permits as relates to the request or notice
- general information about what actions are unlawful without a warrant or authorisation

- whether compliance with the request or notice is voluntary or mandatory
- that civil penalties apply to non-compliance with a notice
- the legislative provisions which authorise the request or notice including which paragraph/s of s 317E(1) ('listed acts or things') are relied upon
- the methods of review available to the provider.

Recommendation 20

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.

5.4 Immunities for providers from civil liability and certain telecommunications and computer offences

224. Pursuant to ss 317G(1)(c) and 317ZJ, providers will not be subject to any civil liability for or in relation to an 'act or thing' done in accordance with a request or notice, or in good faith purported compliance with a request or notice. There are no exclusions or express limitations on this immunity from civil liability.

225. In addition to this civil immunity being broad, the scope of persons covered by the immunity is also wide. This is because, as discussed above, the wide definition of 'designated communications provider' in proposed s 317C is intended to capture the full range of participants in the global communications supply chain. The protection from civil immunity also extends to all employees, officers and agents of the relevant provider, pursuant to ss 317G(1)(d) and 317ZJ(3).

226. The application of the civil immunity to any conduct that is carried out in good faith in *purported compliance* with a request or notice, affords protection to providers despite a notice itself being legally ineffective.[123] For example, a notice could be ineffective by breaching the systemic weakness limitation in s 317ZG, but the provider will still benefit from the protection from civil liability if they act in purported compliance with the notice. It seems possible that 'purported compliance' would also cover an honest but mistaken attempt to comply with a valid notice.

227. Overall, the effect of these provisions is to prevent any person from bringing a civil suit against a provider—or their officers, employees and agents—for any conduct that causes loss or damage including property

damage and financial loss, no matter how serious. This would prevent not only a target of law enforcement bringing a civil claim against a provider, or their associates or families also potentially affected by assistance measures (for example the sender or recipient of messages to a law enforcement target), but also any completely unrelated innocent third parties who might be harmed by a civil wrong.

228. The Commission notes that, while Crown immunities can often be justified by allowing the executive to do things for the public good that might otherwise be prohibitively costly or difficult,[124] the corporate interests of for-profit providers or individuals might not always align with the public interest.

229. As stated by the ALRC, any law that authorises what would otherwise constitute a tort should be subject to careful justification.[125] The Law Council of Australia has highlighted the declining use of executive immunities in Australian law,[126] reflecting the core tenet that government and those acting on its behalf should be subject to the same legal liabilities as any individual.[127] Further, immunity from civil liability has long been recognised as dangerous to the protection of fundamental rights, as reflected in the common law principle that Parliament is presumed not to intend to grant a wide immunity or authorise what would otherwise be a tort in the absence of clear language[128]—an ambiguous provision will be narrowly construed.

230. There is some justification for providing certain immunities to providers in conjunction with issuing a TAN or TCN given that providers are compelled to comply with these notices. There is less justification for immunities, particularly of the broad kind proposed, where the assistance provided is voluntary. While the proposed 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 potential impact of their actions on the privacy and other rights of third parties. This risks removing an additional check in the assistance process.

231. 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 a more rights-intrusive option when a less restrictive measure might suffice.

232. This broad approach can be contrasted with the narrower immunity from civil liability proposed under new s 21A(1) of the ASIO Act, for persons who provide voluntary assistance to ASIO. Proposed s 21A of the ASIO Act does not extend immunity to instances where the person assisting commits an

offence, or where their conduct results in significant loss or serious damage to property (see discussion at Pt 6.7 below).

233. Under Schedule 1 of the Bill, providers will also be afforded immunity from criminal liability to certain telecommunications and computer offences under the Criminal Code pursuant to proposed ss 474.6(7A) and 476.2(4)(b)(iv)–(vi). If providers act in accordance with a request or in compliance with a notice, they will not be liable for offences relating to hindering the normal operation of a carriage service under s 474.6(5) or offences relating to the causing of unauthorised access, modification or impairment of computers under Pt 10.7 of the Criminal Code.

234. The Commission is concerned about the application of immunities with respect to TARs, noting that requests might operate in a manner that bypasses current warrant or authorisation requirements (see discussion above at Pt 5.3, and Recommendation 17 that a warrant be precondition of a request or notice). There is significantly less justification for granting an immunity to a provider when the conduct that it is engaging in is voluntary.

235. As the IGIS has observed, TARs could also potentially be used to extend immunity from criminal liability to 'acts or things' done by providers to assist agencies, in circumstances where the staff or agents of those agencies do not themselves currently enjoy such immunity (for example, on account of the limitations contained in s 476.5 of the Criminal Code).[129] This extension is inconsistent with the existing statutory limitations on the application of criminal immunities to relevant agencies.

236. Further, unlike the decision-making criteria applicable to TANs and TCNs, the giving of a TAR does not currently require the decision maker to consider proportionality or reasonableness. Therefore, there is no requirement to consider whether the effect of constraining a third party's ability to bring a civil claim against a provider, or a provider's immunity from computer offences, is reasonable or proportionate to the objectives of the TAR.

237. The Commission has recommended revised decision-making criteria for the giving of requests and notices, which includes proportionality and specific consideration of any impacts on innocent third parties, including the consequences of a provider's immunity from civil liability (see Recommendation 10). This will help ensure that consideration is given to the broader impacts of immunities before the giving of a request or notice, and that conferral of the immunity is reasonable, proportionate and necessary.

238. As also noted by the IGIS, the effect of the amendments is that agencies will potentially be able to choose from multiple powers to obtain assistance from providers, with those various powers attracting different scopes of statutory immunity including different conditions and limitations.[130] This could lead to a lack of clarity as to which powers and immunities are being relied upon by agencies and/or providers, and on what grounds a third party is unable to bring a civil claim. The Commission makes a recommendation in Pt 6.7 below in relation to voluntary assistance under proposed s 21A of the ASIO Act, which is designed to avoid overlap with technical assistance requests (see Recommendation 50).

239. The Commission appreciates that, as a practical matter, provider assistance might be less effective and forthcoming if some form of immunity is not afforded. However, it considers that the proposed immunities are overbroad and subject to inadequate oversight.

240. One way to address the breadth of the Bill's civil immunities would be to exclude certain conduct from the immunities, in the way proposed in s 21A(1)(d) and (e) of the ASIO Act. For example, the civil immunity could be expressed not to apply to conduct that involves a provider committing an offence or to conduct that results in significant loss or damage to third parties.

241. Another way would be to limit the acts or things that are specified in a request or notice so that they may not include acts or things that would be likely to result in the provider committing an offence (other than the offences for which immunity from criminal liability is proposed in new ss 474.6(7) and 476.2(4)(b)(iii) of the Criminal Code) or that would be likely to cause significant loss or damage to third parties.

242. The Bill should also include ensure the proper oversight of the granting of civil and criminal immunities to providers. This could include mandated reporting by ASIO, ASIS and ASD to the IGIS of instances where a request or notice is given or varied, and where civil or criminal immunity is engaged and a provider's conduct has caused significant loss or damage, or is conduct that is an offence including where it would otherwise constitute a relevant telecommunications or computer offence. Similar reporting requirements should apply to other agencies, to the appropriate integrity bodies such as the Ombudsman and ACLEI.

Recommendation 21

Proposed ss 317G, 317L and 317T of the *Telecommunications Act 1997* (Cth) be amended so that the 'acts or things' that are specified in a request or notice may not include 'acts or things' that would be likely to result in the

provider committing an offence (other than the offences for which immunity from criminal liability is proposed in proposed ss 474.6(7) and 476.2(4)(b)(iii) of the Criminal Code) or that would be likely to cause significant loss or damage to third parties.

Recommendation 22

Further, or in the alternative:

- proposed ss 317G and 317ZJ of the *Telecommunications Act 1997* (Cth) be amended so that the civil immunities in those sections do not to apply to conduct that would be likely to result in a provider committing an offence (other than the offences for which immunity from criminal liability is proposed in new ss 474.6(7) and 476.2(4)(b)(iii) of the Criminal Code) or to conduct that would be likely to cause significant loss or damage to third parties
- the Bill provide that it is a defence to proceedings for breach of a technical assistance notice or a technical capability notice that compliance with the notice would have been likely to result in the provider committing an offence (other than the offences for which immunity from criminal liability is proposed in new ss 474.6(7) and 476.2(4)(b)(iii) of the Criminal Code) or that would be likely to cause significant loss or damage to third parties.

Recommendation 23

The Department seek further advice as to the appropriateness of providing criminal immunities for voluntary conduct engaged in in accordance with a Technical Assistance Request.

Recommendation 24

The Bill be amended to require agencies to report to a relevant oversight body on instances where a civil immunity under proposed ss 317G or 317ZJ of the *Telecommunications Act 1997* (Cth) or criminal immunity under ss 474.6(7A) or 476.2(4)(b)(iv)–(vi) of the Criminal Code is engaged, and a provider's conduct has caused significant loss of or damage to property, or significant financial loss, or constitutes an offence including conduct that would otherwise constitute a relevant telecommunications or computer offence.

5.5 Secrecy provision

243. 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 person appointed under ss 317W(7) or 317ZK (being an expert or arbitrator), 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.[131]

244. The Explanatory Memorandum states that the offence does not include an express requirement of harm, because '[t]here is a high risk that the release of sensitive information contrary to this subsection will cause significant harm to essential public interests, including national security and protection of public safety'.[132]

245. 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 a law of the Commonwealth, a State or a Territory; 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.

246. Disclosures can also be made to an IGIS official. An IGIS official may further disclose information in connection with their exercise of powers or performance of functions and duties.[133]

247. 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.[134]

248. 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.[135]

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

250. 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.

251. 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.

252. 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 scheme are entrusted with highly sensitive information, including information regarding national security as well as information about law enforcement capabilities.

253. 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.

254. 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.[136]

255. In the ALRC's 2010 report, *Secrecy Laws and Open Government in Australia*, the ALRC observed 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.[137]

256. 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.[138]

257. 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.

258. The Commission considers that it has not been demonstrated that all request or notice information, or information obtained under a request or notice, is of sufficient importance to justify secrecy, let alone criminal sanctions for disclosure. It is particularly difficult to justify criminalising disclosures that do not negatively affect national security or public safety, and where there has been no harm to the essential public interest.

259. There may be further instances where the public interest in disclosure of certain information is warranted, where the essential public interest is not harmed. 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.[139]

260. 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.

261. 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, and of maladministration and abuses of public trust.

262. Further, as stated by the UN High Commissioner for Human Rights, whistle-blowers who disclose human rights violations should be protected.[140]

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

264. The Commission welcomes the exception in proposed s 317ZF(3)(f) 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. However, government accountability depends on regular public scrutiny of government actions to the greatest extent possible. The broad secrecy provision has the opposite effect.

265. Further, the Commission notes that the role of the 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 Bill include 'law enforcement agencies', which are not intelligence agencies for the purposes of the *Inspector-General of Intelligence and Security Act 1986* (Cth) (IGIS Act). Therefore, there does not appear to be a disclosure exception for integrity purposes in relation to agencies that fall outside the ambit of the IGIS.

266. It is important that an avenue for lawful public interest and integrity disclosures exists in relation to activities of agencies that do not fall within the ambit of the IGIS Act. For example, this would include disclosure to the Commonwealth Ombudsman, the Office of the Australian Information Commissioner (OAIC) or ACLEI for the purpose of those bodies performing their functions.

267. The Commission notes that some protection would be provided to persons who make public interest disclosures in accordance with the *Public Interest Disclosure Act 2013* (Cth) (PID Act). However, the Bill should clearly provide that disclosure in accordance with the PID Act is an exception to, or defence in respect of, the secrecy provisions.

268. Such a model was adopted in the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth), which explicitly sets out a list of defences to disclosure of protected information, including for public interest and other integrity purposes. The Commission notes that similar comments were made by the IGIS in its submission to the Department on the Exposure Draft of the Bill.[141]

269. As a result of the changes discussed in the paragraph above, s 122.5 of the Criminal Code will include defences such as: the information was communicated to the IGIS, Ombudsman, OAIC or ACLEI; that the information was communicated in accordance with the PID Act or *Freedom of Information Act 1982* (Cth); that the information was communicated for the purpose of reporting offences or maladministration to an appropriate Commonwealth, state or territory agency; that the information was

communicated to a court or tribunal; and that the information was communicated by persons engaged in news reporting.

270. 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.

271. 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.[142]

272. Notably, s 11A of the *Telecommunications Act 1997* (Cth) provides that Ch 2 of the Criminal Code applies to all offences under the Act. Chapter 2 of the Criminal Code sets out general principles of criminal responsibility, including the fault elements applicable to an offence where the head act is silent.

273. Pursuant to s 5.6(1) of the Criminal Code, where no fault element is specified for an offence and the physical element is conduct, intention is the default fault element. Therefore, the fault element attaching to disclosure of protected information would be intention.

274. Pursuant to s 5.6(2) of the Criminal Code, where an offence has a physical element consisting of a circumstance or a result, the default fault element is recklessness. If a harms-based approach is taken to the secrecy provision, which the Commission considers appropriate, recklessness would be the automatic fault element attaching to the elements of the offence that required the establishment of harm or likelihood of harm to an essential public interest.

275. The Commission recommends that:

Recommendation 25

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

Recommendation 26

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 27

Serious consideration be given to amending proposed s 317ZF of the *Telecommunications Act 1997* (Cth), to explicitly allow for disclosure of information in accordance with the PID Act, the FOI Act, and for other integrity purposes, including to the Ombudsman and ACLEI 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

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

277. 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.

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

279. 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.

280. The Bill generally permits delegation 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.

281. Under proposed s 317T, only 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.

282. The Explanatory Memorandum states that the delegation provisions operate to ensure that assistance powers are restricted to persons of sufficient seniority.[143] It states that the people who can make technical assistance requests 'occupy the most senior position in their organisation

and can exercise suitable judgment about the propriety of such a request, and the relevant terms of any contract'.[144] As discussed further below, the Commission considers that the powers of delegation are too broad.

283. Before giving or varying a TCN, the Attorney-General must give the provider a written consultation notice inviting the provider to make a submission on the proposed TCN. However, consultation need not occur when it is impracticable, where the TCN must be given as a matter of urgency, or where the provider waives the opportunity to consult.[145] A consultation notice must allow at least 28 days for consultation.[146]

284. If a consultation notice is given, under proposed s 317W(7) the Attorney-General and provider may jointly appoint one or more persons to assess whether the proposed TCN would contravene the systemic weakness limitation in s 317ZG and prepare a report of the assessment. Proposed s 317W(1)(c) provides that the Attorney-General must consider such a report before giving a TCN.

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

286. 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.

287. 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,[147] 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.[148]

288. The UK scheme also permits a provider to refer a notice back to the Secretary of State for review.[149] 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.

289. 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.[150]

290. 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.[151]

291. 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'.[152]

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

293. If the intention of the assistance scheme is to supplement existing powers under warrants, it is unclear why the assistance scheme 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.

294. If the Bill is 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.

295. 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.

296. The Commission is further concerned about the exclusion of independent merits review and the application of the ADJR Act. As stated in the Explanatory Memorandum, 'the Bill does not provide for merits review of decision making and excludes judicial review under the ADJR Act'.[153] These exclusions 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.

297. 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.[154]

298. As discussed in paragraph [195] of this submission, the various ambiguities contained in the 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.

299. Such a review process could operate at both the administrative and judicial level. For example, the 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.

300. Lastly, the Commission considers that public reporting of the number of TARs, 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 the requests and notices were issued appropriately—either in aggregate or individually. Stronger reporting requirements would enhance the proportionality of the powers.

301. The Commission queries why more detailed reporting requirements are not feasible, such as a disaggregated summary of notices that redacts any sensitive information. It considers that public reports should include as much information as possible about the types of acts or things done by providers in compliance with a request or notice.

302. Further, the Commission 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 operational requirements.

303. The Commission notes the detailed reporting requirements provided for under ss 99–103B of the TIA Act and s 50 of the SD Act. While similarly sensitive, these provisions provide for far more detailed annual public reporting by the relevant agencies. This includes reporting of information about how many applications for relevant warrants were made (broken down by particular warrant type), the number of warrants issued, the durations of the warrants issued, the number of arrests made under the warrants, the number of prosecutions for relevant offences commenced, the expenditure of agencies in relation to executions of warrants. The Commission notes that similar comments were made by the OAIC in its submission to the Department on the Exposure Draft of the Bill.[155]

304. A further significant gap in the reporting requirements is that proposed s 317ZS only requires reporting on TARs and TANs given by the chief officers of 'interception agencies', and on TCNs given and directed towards ensuring a provider is capable of giving help to 'interception agencies'.

305. Pursuant to the definition of 'interception agencies', this section appears, therefore, not to extend to intelligence agencies such as ASIO, ASD or ASIS. The Commission considers that reporting requirements are an important safeguard to enhance oversight, and queries why only interception agencies are covered. The Commission notes that similar comments were made by the IGIS in its submission to the Department on the Exposure Draft of the Bill, with the IGIS recommending classified (rather than public) reporting requirements for intelligence agencies to the relevant Ministers as well as the IGIS.[156]

306. The Commission recommends that:

Recommendation 28

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 29

In the event that Recommendation 28 is not accepted, proposed ss 317ZN–ZR of the *Telecommunications Act 1997* (Cth) be amended 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 30

The 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 31

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 32

Proposed s 317ZS of the *Telecommunications Act 1997* (Cth) be amended to require public reporting of more detailed statistical and other information about requests and notices under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth), including: the number of requests and

notices considered, given, varied, revoked, expired and refused or challenged; the durations of the requests and notices given; the types of acts or things done by providers in compliance with a request or notice; the number of requests that were refused and then compelled by way of a notice in the same or similar terms; the number of arrests made as a consequence of assistance; the number of prosecutions for relevant offences commenced; and the expenditure of agencies in relation to requests and notices.

Recommendation 33

Proposed s 317ZS of the *Telecommunications Act 1997* (Cth) be amended to require reporting by all agencies that are empowered to give requests and notices under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth), not just 'interception agencies'.

6 Key human rights concerns: warrant powers

6.1 Computer access warrants

307. The 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.[157]

308. If passed, the proposed changes would enable law enforcement agencies to seek computer access warrants in investigations relating to 'relevant offences',[158] recovery orders,[159] mutual assistance investigations,[160] integrity operations[161] and control orders.[162]

309. 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.[163]

310. The Bill also proposes to broaden the definition of 'computer' in 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 access warrant. The Explanatory Memorandum 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 devices.[164]

311. The Explanatory Memorandum 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.[165] 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'.

312. 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 (and adding, copying, deleting or altering data on the target computer if necessary)
- 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.

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

314. 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 Bill, go beyond what can be reasonably justified as a proportionate response to the issues that they are intended to address.

6.2 Access to third party computers, communications and premises

315. The proposed new computer access warrants under the SD Act would permit the authorisation of access to third party premises, computers and communications for the purpose of executing the warrant (proposed s 27E(2)). This would be consistent with existing provisions relating to computer access warrants in s 25A(4) of the ASIO Act and foreign intelligence and identified person warrants that permit computer access in ss 27A(1) and 27E(2) of the ASIO Act.[166]

316. The Commission considers that the conditions under which law enforcement agencies and ASIO should be permitted to access the premises, computers and communications of innocent third parties should be tightly controlled. Permitting law enforcement agencies and ASIO to enter premises of people who are unconnected with an investigation and to access their computers and communications represents a serious interference with the right to privacy. In the Commission's view, access to third party premises, computers and communications should be limited to situations where this is necessary and not merely convenient or desirable for those executing the warrant.

317. Proposed s 27E(7) of the SD Act and proposed ss 25A(8), 27A(3C) and 27E(6) of the ASIO Act would also permit access to third party premises, computers and communications for the purpose of doing anything reasonably necessary to conceal the fact that a warrant permitting access to a computer has been executed.

318. The Bill seeks to make equivalent amendments to the Customs Act[167] and the Crimes Act[168] to permit access to third party computers and communications (but not premises) when executing a search warrant under each of those Acts.

319. It is illustrative to extract the relevant provisions of proposed ss 27E(1) and (2) of the SD Act below:

(1) A computer access warrant must authorise the doing of specified things (subject to any restrictions or conditions specified in the warrant) in relation to the relevant target computer.

(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 ...

(a) *Access to third party premises for the purpose of executing a computer access warrant*

320. The Explanatory Memorandum justifies the need for possible access to third party premises for the purpose of executing a computer access warrant under the SD Act as follows:

> This may occur where 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 to the safety of executing officers). The need to access third party premises may also arise in 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).[169]

321. 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.

322. 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 (or conceal its execution). The current scope of proposed ss 27E(2) and (7) of the SD Act is not explicitly limited to cases of necessity. Rather, under proposed s 27E(2)(b), an eligible Judge 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. This would then have the effect of authorising entry to third party premises for the purpose of concealing the execution of the warrant (under proposed s 27E(7)(e)).

323. An identical provision exists in ss 25A(4)(aaa) and 27E(2)(b) of the ASIO Act and the Bill would insert an equivalent provision in relation to concealment by way of new ss 25A(8)(e), 27A(3C)(e) and 27E(6)(e) of the ASIO Act. For the reasons given above, the Commission considers that provisions relating to warrants under the ASIO Act that permit access to computers should also be amended so that warrants may only permit access to third party premises in cases where it is *necessary* to execute the warrant.

324. The Commission recommends that:

Recommendation 34

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 or to conceal the execution of the warrant.

Recommendation 35

Sections 25A(4)(aaa) and 27E(2)(b) and proposed ss 25A(8)(e), 27A(3C)(e) and 27E(6)(e) of the *Australian Security Intelligence Organisation Act 1979* (Cth) be amended to ensure that a computer access warrant (or either a foreign intelligence warrant or an identified person warrant that permits computer access) may only authorise access to third party premises where it is *necessary* to execute the warrant or to conceal the execution of the warrant.

(b) *Access to third party computers and communications for the purpose of executing a computer access warrant or search warrant*

325. As extracted above, the 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.[170]

326. 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.

327. 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.

328. 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.

329. 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.

330. The Bill also seeks to insert provisions identical to proposed s 27E(2)(e) of the SD Act into numerous sections of the ASIO Act,[171] as well the Crimes Act[172] and the Customs Act.[173]

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

332. The Commission recommends that:

Recommendation 36

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 37

An issuing authority for a warrant relating to computer access under the *Australian Security Intelligence Organisation Act 1979* (Cth), the *Surveillance Devices Act 2004* (Cth), the *Crimes Act 1914* (Cth) or the *Customs Act 1901* (Cth) should be required 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.

6.3 Concealment of access provisions

333. The Bill proposes to attach broad 'concealment of access' powers to computer access warrants issued under the SD Act and computer access warrants, foreign intelligence warrants and identified person warrants involving computer access issued under the ASIO Act.

334. 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.

(a) Timeframes for concealment activity

335. 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'.[174]

336. The Explanatory Memorandum 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.[175]

337. The proposed provisions represent two significant expansions of the current concealment powers available to ASIO under computer access

warrants and identified person warrants that permit computer access. First, it is currently necessary for concealment activities to be specified in a warrant (that is, the concealment authorisation does not automatically attach to every warrant that is issued). Secondly, the concealment activities are currently only authorised for the duration of the warrant.[176]

338. 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.

339. 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.

340. 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.

341. 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.

342. The Commission recommends that:

Recommendation 38

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 39

Proposed ss 25A(8)(k), 27A(3C)(k) and 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 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 (or Director-General in the case of an identified person warrant) for further authorisation.

(b) Limitations on concealment activity

343. At present, there are limitations on the powers of ASIO to do things that would otherwise be authorised under a computer access warrant or a foreign intelligence warrant or identified person warrant that permits computer access.[177] In particular, these warrants do not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

- materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or
- cause any other material loss or damage to other persons lawfully using a computer.

344. These limitations are expressed to apply only to the specific things that are currently authorised under the warrants. The Bill proposes to insert provisions that authorise a number of concealment activities in relation to these warrants,[178] but it does not extend the limitations to these new concealment activities. This means that ASIO would not be authorised to, for example, cause material loss or damage to persons lawfully using a computer when executing a warrant, but it would not be subject to the

same limitation when concealing the fact that a warrant had been executed.

345. It appears that this may be an oversight. Section 34 of the ASIO Act currently requires the Director-General to provide a report to the Attorney-General that sets out details of anything done under a range of warrants, including those discussed above, which materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or other electronic equipment, or a data storage device. The Bill proposes to extend this obligation to concealment activities. The Explanatory Memorandum notes:

> This item clarifies that anything done to conceal access to a computer or other thing under a computer access warrant or an identified person warrant is to be taken, for the purposes of section 34, as having been done under that warrant.
>
> This will ensure that concealment activities are captured by section 34 and will be subject to reporting requirements.[179]

346. Presumably, if concealment activities are to be treated as having been done under the warrant for the purposes of reporting about the extent to which third party rights were interfered with, it was intended that those concealment activities would be subject to the same limitations in respect of third party rights.

347. The Commission recommends that the limitation provisions in relation to each of the ASIO warrants discussed above be amended so that they also apply to the proposed list of concealment activities in the Bill.

348. The new computer access warrant regime that the Bill proposes to insert into the SD Act is based on the regime in the ASIO Act. Proposed s 27E(5) of the SD Act provides that the acts authorised under s 27E(2) are subject to the same limitation as the ASIO warrants.[180] However, this limitation does not extend to the concealment activities in s 27E(7). The Commission recommends that the limitation provisions that apply to computer access warrants in the SD Act also extend to concealment activities.

349. The Commission recommends that:

Recommendation 40

The limitations set out in ss 25A(5), 27A(1) and 27E(5) of the *Australian Security Intelligence Organisation Act 1979* (Cth) on activities authorised under a computer access warrant or a foreign intelligence warrant or identified person warrant that permits computer access, be extended to the concealment activities under these warrants in proposed ss 25A(8), 27A(3C) and 27E(6).

Recommendation 41

Proposed s 27E(5) of the *Surveillance Devices Act 2004* (Cth) be amended so that the limitations on the activities authorised under a computer access warrant also extend to the concealment activities in proposed s 27E(7).

6.4 Ancillary interception powers

350. The 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.[181] In doing so, the Bill also lowers the threshold for authorising the interception of communications in these circumstances.

351. The expansion of warrants authorising access to computers to also permit interception marks a significant departure from the current 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.

352. The Explanatory Memorandum explains the reason for this change as follows:

> Currently, ASIO is required to obtain a computer access warrant under sections 25A, 27A or 27E of the ASIO Act to gain access to a device, and a telecommunications interception warrant under section 9 or 9A of the TIA Act to intercept communications.
>
> 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.[182]

353. 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.

354. 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 Bill proposes to make the same definition applicable to the ASIO Act.[183]

355. 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.

356. 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.

357. 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'.

358. 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.

359. 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.

360. Consequently, by attaching ancillary interception powers to the issuance of a computer access warrant under s 25A of the ASIO Act, the Bill lowers

the threshold for authorising the interception of communications passing over a telecommunications system.

361. On the material provided in the Explanatory Memorandum, 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.

362. Reference in the Explanatory Memorandum 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.

363. There is nothing in the Explanatory Memorandum 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.

364. The Explanatory Memorandum states that 'it is almost always necessary for ASIO to undertake limited interception for the purposes of executing a computer access warrant',[184] 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.

365. A further issue relates to the breadth of activities that may currently be authorised in a computer access warrant under the ASIO Act and the proposed computer access warrant regime under the SD Act. Because the scope of activities that may be undertaken pursuant to a warrant is broad, it follows that inserting a new ability to authorise telecommunications interception for the purpose of doing any of these things represents a very significant expansion of interception powers. It is therefore necessary to ensure that the telecommunications interception that is authorised is tightly related to obtaining access to data from the computer.

366. For example, under ss 25A(4)(aaa) and 27E(2)(b) of the ASIO Act and proposed s 27E(b) of the SD 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 could 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. For example, ASIO or a law enforcement agency may be authorised to monitor phone calls or messages of innocent third parties, perhaps even of children, in a property adjacent to the property containing the computer to which the warrant relates, in order to determine when the property is vacant and could be used to access the property specified in the warrant. Clearly, such an exercise of the ancillary interception power would significantly impact upon the human rights of innocent third parties.

367. 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 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. Further, proposed amendments to the TIA Act would permit, in certain circumstances, secondary use of information obtained by ASIO as a result of intercepting telecommunications while executing a computer access warrant.[185]

368. The Commission agrees with the views of the IGIS that consideration could be given to limiting the telecommunications interception powers to only those authorised activities that are directly connected to obtaining access to relevant data from the computers that are the subject of the warrant.[186]

369. In the absence of any persuasive explanation of why broader 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.

370. The Commission recommends that:

Recommendation 42

The authorisation of telecommunications interception under proposed s 25A(4)(ba) of the *Australian Security Intelligence Organisation Act 1979* (Cth) be limited to interception for the purposes of doing the things set out in

s 25A(4)(a) and (ab), namely, for the purposes of using a device or equipment to obtain access to the relevant data.

Recommendation 43

Equivalent amendments be made to limit the authorisation of telecommunications interception under proposed ss 25A(8)(h), 27A(3C)(h), 27E(2)(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).

6.5 Use of force

371. The amendments to existing ASIO warrant provisions to permit interception of telecommunications will also have the effect of expanding the circumstances in which ASIO can use force against persons and things.

372. ASIO currently has the ability to obtain computer access warrants, foreign intelligence warrants and identified person warrants. Each of these warrants authorises ASIO to do a range of specified things. Significantly, each of those warrants is also required to authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant.[187] Amendments in Schedule 2 of the Bill will now add telephone interception to the list of things that can be authorised under these warrants.[188] This means that ASIO will be permitted to use force in relation to telephone interception activities authorised under the warrants. This represents an expansion of the scope of ASIO's authorisation to use force, given that interception warrants issued under Part 2-2 of the TIA Act do not authorise the use of force.

373. The IGIS, who is responsible for oversight of ASIO, has said that '[i]t is unclear if the use of force against a person or thing could ever be necessary or reasonable to intercept a telecommunication under a warrant' issued to ASIO.[189] There is a real question whether this expansion of the power to use force was intended. The Explanatory Memorandum does not address this issue. If there is no justification for expanding the circumstances in which force may be used by ASIO, the Commission recommends that amendments be made to the provisions dealing with these warrants to exclude telephone interception from the list of activities in respect of which warrants must authorise the use of force.

374. The new computer access warrant regime that the Bill proposes to insert into the SD Act is based on the regime in the ASIO Act. Proposed s 27E(6)(a) of the SD Act provides that a computer access warrant must authorise the use of force against persons and things that is necessary

and reasonable to do the things specified in the warrant. Proposed s 27E(7)(h) provides that one of the things that may be authorised is intercepting a communication passing over a telecommunications system. The Commission recommends s 27E(6)(a) of the SD Act be amended to exclude the use of force in relation to telephone interception. This amendment would be consistent with the Commission's recommendation in relation to warrants under the ASIO Act.

375. The Commission recommends that:

Recommendation 44

The requirement to authorise the use of force by ASIO in ss 25A(5A)(a), 27A(2)(a) and 27J(3)(d) of the *Australian Security Intelligence Organisation Act 1979* (Cth) exclude the use of force in relation to the proposed new activity of telephone interception authorised under computer access warrants, foreign intelligence warrants and identified persons warrants.

Recommendation 45

The requirement to authorise the use of force in proposed s 27E(6)(a) of the *Surveillance Devices Act 2004* (Cth) be amended so that it does not apply in relation to the proposed activity of telephone interception authorised under computer access warrants.

6.6 Assistance orders

376. The 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.[190] Similar assistance order provisions already exist in the Crimes Act and the Customs Act.[191]

377. The Explanatory Memorandum 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.[192]

378. 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 imprisonment or a fine of $126,000 or both.

379. 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 a maximum of five years or a fine of $63,000, or both.

380. Significantly, unlike the assistance orders made under the SD Act, the Crimes Act and the Customs Act (which are issued by eligible Judges 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.

381. The 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.[193]

382. 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 offence' or a 'serious terrorism offence', 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.[194] The Bill would also increase the penalty for failing to comply with an assistance order from two years imprisonment to five years imprisonment or a fine of $63,000 (or both) for a simple offence or ten years imprisonment or a fine of $126,000 (or both) for a serious offence or a serious terrorism offence.

383. The 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 offence', 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 a maximum of five years imprisonment or a fine of $63,000 (or both) for a simple offence or a maximum of ten years imprisonment or a fine of $126,000 (or both) for a serious offence.

(a) Disproportionality of increased penalty provisions

384. As is apparent from the discussion above, the 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.

385. In general terms, the Explanatory Memorandum claims that the changes are necessary because the current penalties are of insufficient gravity to 'incentivise compliance' with an assistance order.[195] In the second reading speech for the Bill, the Minister for Home Affairs expanded on the rationales for the increased penalties, saying:

> The increased penalties for noncompliance with orders for access to a device reflect the value of evidentiary material on devices and the fact that persons who have undertaken criminal activity would rather accept the current low penalties than provide data that could be evidence in a more serious prosecution.[196]

386. The Commission considers that these explanations do not sufficiently justify such a substantial increase in the penalty provisions. While the value of the evidentiary material on a device may be greater in the case of an investigation into a serious offence, it does not necessarily follow that there is a greater moral culpability for failing to cooperate with the investigation of different kinds of offences, particularly if there is no suggestion that the person is otherwise involved in, or even knows of, the alleged underlying offence.

387. More significant, however, is the suggestion that there is a need to 'incentivise' a person to cooperate with an investigation because they would otherwise be willing to accept a low penalty for failing to cooperate rather than a higher penalty for the underlying offence. Implicit in this explanation is that the person failing to cooperate with the investigation and the person being investigated are the same. However, there is no necessary connection between the two. Further, the increase in penalties may have the perverse result that failure to cooperate with an investigation is treated more seriously than committing the underlying offence.

388. 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 a maximum of two years imprisonment or more. This means that a person could be exposed to a sentence of up to ten years imprisonment for failing to cooperate with an investigation where the principal offence being investigated would itself only attract a maximum sentence of two years imprisonment.

389. It seems entirely possible that a failure to assist law enforcement agencies could be punished more severely than the commission of the substantive underlying offence. It is difficult to justify as proportionate a scheme that allows a harsher punishment for a failure to assist an investigation when requested than for actively committing an offence that is the subject of the investigation.

390. 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.

391. 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.[197] 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.[198]

392. 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.[199]

393. 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, a court will have regard to the maximum sentence in determining the length of sentence. In *Markarian v The Queen*, the High Court's plurality judgment observed that '[l]egislatures do not enact maximum available sentences as mere formalities. Judges need sentencing yardsticks'.[200] The fact that the maximum sentence under each of the SD Act, the Crimes Act and the Customs Act will be ten years is likely to have the effect of significantly

increasing the sentence that is given compared to what would be given now in the same circumstances.

394. 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.

395. 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 46

Serious consideration be given to the proportionality of the substantially increased penalty provisions in the Bill. The maximum sentence for failing to comply with an assistance order should not be longer than the maximum sentence for the offence being investigated. 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

396. 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,[201] and stated that court-ordered decryption should only be permitted when certain criteria are met, including the protection of due process rights of individuals.[202]

397. 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.

398. 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.

399. 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.[203]

400. 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'.[204]

401. 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'[205] and entitles a natural person (but not a corporation)[206] to refuse to answer any question or produce any document if it would tend to incriminate them.[207]

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

403. 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'.[208]

404. 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.[209]

405. 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.[210]

406. 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.[211]

407. 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.[212]

408. 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.

409. 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.[213]

410. 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.

411. The Commission recommends that:

Recommendation 47

The 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.

(c) Potential for assistance orders to authorise detention by non-judicial officers, and necessary safeguards

412. The current assistance orders under s 3LA of the Crimes Act and s 201A of the Customs Act are made by a magistrate. The proposed new assistance orders under s 64A of the SD Act would be made by an eligible Judge or nominated AAT member.

413. However, the proposed new assistance orders under s 34AAA of the ASIO Act would be made by the Attorney-General on request from the Director-General of Security. There are similarities between each of the regimes but the fact that assistance orders made under the ASIO Act are not required to be authorised by a judicial officer means that they require greater scrutiny.

414. It appears that in the ordinary course, a person would be required under s 34AAA of the ASIO Act to provide assistance on the premises in relation to which the warrant is in force. If the person does not comply with an order requiring assistance when they are capable of complying, they commit an offence. The section does not set out how long a person could be required to provide the assistance. Presumably, if they left the premises before completing the assistance task set for them in the order, they would be liable to the criminal penalty of a maximum of five years imprisonment, or a fine of $63,000 or both.

415. Section 34AAA(3) provides that a person subject to an assistance order could be required to attend at another place to provide assistance. In such circumstances, the assistance order must specify the period within which the person must provide the assistance, but no maximum period is set.

416. There is a real question whether a person subject to an assistance order is effectively being detained during the period in which they are required to provide the assistance. While they may not be physically restrained, they are effectively prevented from leaving prior to the completion of the designated assistance task, under pain of criminal penalties.

417. The UN HR Committee, in its concluding observations in 2008 on a report by the United Kingdom, expressed concern about the restrictive conditions

that could be imposed under the UK's control order regime, including curfews of up to 16 hours, with criminal sanctions available if the control orders were breached.[214] The Committee considered that this engaged the prohibition on arbitrary detention in article 9 of the ICCPR. Similarly, house arrest has long been considered to be a form of detention.[215] By contrast, voluntary cooperation with police, including participation in an identity parade and an interview, in circumstances where a person was informed that they had the right to leave at any time, did not amount to detention.[216]

418. The assistance orders do not make provision for the kinds of protections available to people who are subject to questioning warrants or questioning and detention warrants under Pt III, Div 3 of the ASIO Act. For example, the new assistance order regime under proposed s 34AAA of the ASIO Act does not make provision for a person to contact a lawyer or family member; there is no maximum period prescribed for the giving of assistance; there is no obligation on officers to explain the nature of the assistance order and what it requires; there is no obligation on officers to explain how to make a complaint to the IGIS or to challenge the making of the assistance order in court; there is no obligation to make an interpreter available if necessary; and there is no statutory obligation to treat the person humanely and with respect for their human dignity.

419. Particular consideration should be given to how assistance orders may impact on children. Currently, there are no safeguards to protect the interests of children if they are the recipient of an assistance order. Safeguards could include: minimum age limits for recipients of assistance orders, a requirement that parents or guardians be notified if it is intended to issue an assistance order to a minor, and a requirement that any obligations under an assistance order be suspended until a parent or guardian is able to be present.

420. The class of persons who may be given an assistance order is broad and includes people who may have no connection to the matter being investigated under the warrant. For example, an assistance order may be given to a person because of their technical expertise, such as a systems administrator or even an independent IT contractor. There is no requirement that they be suspected of being involved in the activities that are being investigated.

421. The breadth of people who may be required to provide assistance and the lack of sufficient protections, means that there is a real risk that assistance orders may result in arbitrary detention.

422. The Commission recommends that:

Recommendation 48

The assistance order regime in proposed s 34AAA of the ASIO Act include the following protections for the person specified in the order:

- a maximum time limit on the period during which assistance must be provided
- a right to contact a family member and a lawyer
- an obligation on officers to explain the nature of the assistance order and what it requires
- an obligation on officers to explain how to make a complaint to the IGIS or to challenge the making of the assistance order in court
- a right to an interpreter, if necessary
- an obligation to treat the specified person humanely and with respect for their human dignity
- sufficient safeguards to protect the interests of children in respect of whom an assistance order may be issued (for example: age limits, notification of parents or guardians, and suspension of any obligations until a parent or guardian is present).

Recommendation 49

Consideration be given to including a similar set of explicit protections into the assistance order regimes under s 3LA of the *Crimes Act 1914* (Cth), s 201A of the *Customs Act 1901* (Cth) and proposed s 64A of the *Surveillance Devices Act 2004* (Cth).

6.7 Immunities for voluntary assistance to ASIO

423. As noted in Part 5.4 of this submission, the new access and assistance regime provides for civil immunities and limited criminal immunities for designated communications providers that are issued with a TAR, TAN or TCN.

424. Schedule 5 of the Bill also proposes to introduce a new scheme whereby any person can obtain immunity from civil liability for providing voluntary assistance to ASIO, subject to a number of conditions. The voluntary assistance may be provided in accordance with a request from the Director-General of Security (proposed s 21A(1)) or it may be an unsolicited disclosure of information to ASIO (proposed s 21A(5)).

425. Some aspects of this regime are broader than the proposed regime for civil immunities in Schedule 1 of the Bill and some aspects are narrower.

426. The regime under proposed s 21A of the ASIO Act is broader than the access and assistance regime under Schedule 1 of the Bill in that:
    - the availability of immunities is not limited to designated communications providers and may be obtained by anyone that complies with the conditions of the section
    - there are fewer limits on making oral requests.[217]
427. The regime under proposed s 21A of the ASIO Act is narrower than the access and assistance regime under Schedule 1 of the Bill in that civil immunity is not available if the conduct of the person providing assistance or information involves the person committing an offence or if it results in significant loss or serious damage to property.
428. There is likely to be an overlap between the assistance that may be requested by ASIO pursuant to an assistance request under proposed s 21A(1) of the ASIO Act and the assistance that may be requested by ASIO pursuant to a technical assistance request under proposed s 317G of the *Telecommunications Act 1997* (Cth). This may result in ASIO having a choice of civil immunity regimes available to it with different conditions and limitations. The Commission considers that the Bill should make clear that an assistance request under s 21A of the ASIO Act may not be made to a person if ASIO could make a technical assistance request under s 317G of the *Telecommunications Act 1997* (Cth) to that person.
429. There is no requirement on the Director-General of Security to consider issues of proportionality or reasonableness when making a request under proposed s 21A(1)(a). For example, there is no requirement to consider whether depriving third parties of their civil rights against the person providing the assistance is reasonable or proportionate to the value of the requested conduct in assisting ASIO to perform its functions.
430. The lack of a required consideration of reasonableness or proportionality stands in contrast to the requirements on the Director-General of Security when issuing a TAN and the requirements on the Attorney-General when issuing a TCN.[218] Similarly, the lack of any required consideration of reasonableness or proportionality stands in contrast to the requirements on the Attorney-General when authorising a special intelligence operation, which also has the effect of conferring immunities (albeit, more significant immunities including in relation to criminal liability).[219]
431. The Commission notes the comments of the IGIS about the relationship between the proposed voluntary assistance requests under s 21A of the ASIO Act and existing ASIO warrants.[220] The Commission considers that this new immunity process should not provide a way for ASIO to bypass

the current warrant requirements by requesting a person under proposed s 21A(1) to engage in conduct that would otherwise require a warrant (or other form of Ministerial authorisation or approval).

432. Finally, the Commission notes its earlier recommendation that amendments be made to proposed s 317HA of the *Telecommunications Act 1997* (Cth) to provide a maximum time limit for any single technical assistance request.[221] The Commission considers that a maximum time limit should also be set for voluntary assistance requests under s 21A of the ASIO Act, so that these requests do not become 'standing requests' of no fixed duration with open ended immunities attaching to them.

433. The Commission recommends that:

Recommendation 50

The Bill provide that an assistance request under s 21A(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth) may not be made to a person if ASIO could make a technical assistance request under s 317G of the *Telecommunications Act 1997* (Cth) to that person.

Recommendation 51

Proposed s 21A of the *Australian Security Intelligence Organisation Act 1979* (Cth) be amended to include a requirement that, prior to making a request under subsection (1), the Director-General must be reasonably satisfied that the impact on third party rights resulting from the grant of civil immunity is reasonable and proportionate to the value of the requested conduct in assisting ASIO to perform its functions.

Recommendation 52

The Bill be amended to provide that s 21A(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth) does not apply to requests for persons to engage in conduct for which ASIO would require a warrant (or other form of Ministerial authorisation or approval) to undertake.

Recommendation 53

Proposed s 21A of the *Australian Security Intelligence Organisation Act 1979* (Cth) be amended to include a maximum duration for a voluntary assistance request.

7 Statutory review

434. This Bill is a very substantial piece of proposed legislation, running to 172 pages and including proposed amendments to 11 Acts. The Commission appreciated the opportunity to review and consider an Exposure Draft of

the Bill prior to its introduction into Parliament and the Commission commends the government for this step. However, there has been limited time to fully evaluate the potential impacts of the Bill.

435. An Exposure Draft of the Bill was released on 14 August 2018 and comments were sought by the Department of Home Affairs by 10 September 2018. The Bill, with amendments from the Exposure Draft, was introduced into the House of Representatives on 20 September 2018 and referred to this Committee with a request to provide submissions by 12 October 2018.

436. The Commission has sought to provide as detailed a response to the Bill as possible in the time available, but there are many issues that it has not been able to consider in detail and some issues it has not been able to consider at all.

437. Given the very significant changes proposed in this Bill, their potential impact on human rights, and the limited time available for review prior to debate in the Parliament, the Commission recommends that the Bill provide for a statutory review of its provisions three years after enactment. The review would consider whether the policy objectives of the amendments remain valid and whether the new provisions have proven appropriate for securing those objectives.

438. Similar statutory reviews or sunset provisions have been included in other national security legislation passed by the Commonwealth Parliament.[222]

439. The Commission recommends that:

Recommendation 54

The Bill include a requirement for a statutory review of its provisions after three years by the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor.

8 List of recommendations

440. The Commission makes the following recommendations:

Recommendation 1

The Australian Government ensure that adequate time is afforded for public consultation, review and reform of the 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, intelligence and national security agencies to carry out their functions.

Recommendation 3

Proposed ss 317G(6), 317L(3), 317T and 317X(3) of the *Telecommunications Act 1997* (Cth) be amended so that the only 'acts or things' that can be requested or required to be done 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 317T(5) of the *Telecommunications Act 1997* (Cth) be omitted, to remove the power of the Minister to expand the definition of 'acts or things' for the purposes of a TCN by way of legislative instrument.

Recommendation 5

In the event that Recommendation 4 is not accepted, 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 6

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 a 'serious offence' as defined in s 5D of the TIA Act.

Recommendation 7

In the event that Recommendation 6 is not accepted, 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 8

The decision-making criteria in proposed ss 317P, 317Q(10), 317V and 317X(4) of the *Telecommunications Act 1997* (Cth) be amended to include a requirement that the decision maker be satisfied of the 'necessity' of giving or varying a notice.

Recommendation 9

The decision-making criteria in proposed ss 317RA and 317ZAA of the *Telecommunications Act 1997* (Cth) be amended to include a requirement that the decision maker be satisfied that the giving or varying of a notice would not require the recipient to breach the s 317ZG systemic weakness limitation.

Recommendation 10

The decision-making criteria in proposed ss 317RA and 317ZAA of the *Telecommunications Act 1997* (Cth) be amended to also require that the decision maker be satisfied on reasonable grounds that:

- any interferences with privacy
- any interferences with other human rights including the right to freedom of expression and the right to an effective remedy and
- any impacts on innocent third parties, including the consequences of a provider's immunity from civil liability

are reasonable, necessary and proportionate by reference to a detailed, non-exhaustive list of considerations, such as the seriousness of any offence under investigation.

Recommendation 11

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 commensurate terms as those applicable to TANs and TCNs.

Recommendation 12

Proposed ss 317HA(1)(b) and 317MA(1)(b) of the *Telecommunications Act 1997* (Cth) be amended to provide that the maximum permissible duration of any single TAR or TAN is 90 days.

Recommendation 13

Proposed s 317TA(1)(b) of the *Telecommunications Act 1997* (Cth) be amended to provide that the maximum permissible duration of any single TCN is 180 days.

Recommendation 14

Proposed ss 317R and 317Z be amended to:

- allow a provider to apply to the decision maker for the revocation of a notice where the provider considers that the requirements imposed by

the notice are not reasonable and proportionate or that compliance with the notice is not practicable and technically feasible

- make provision for a provider to access independent merits review of any decision to refuse to revoke a notice.

Recommendation 15

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

Recommendation 16

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

Recommendation 17

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 18

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 19

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 the requested act or thing assists in giving effect to an extant warrant or authorisation, and what that warrant or authorisation broadly permits as relates to the request or notice
- general information about what actions are unlawful without a warrant or authorisation
- whether compliance with the request or notice is voluntary or mandatory
- that civil penalties apply to non-compliance with a notice
- the legislative provisions which authorise the request or notice including which paragraph/s of s 317E(1) ('listed acts or things') are relied upon

- the methods of review available to the provider.

Recommendation 20

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 21

Proposed ss 317G, 317L and 317T of the *Telecommunications Act 1997* (Cth) be amended so that the 'acts or things' that are specified in a request or notice may not include 'acts or things' that would be likely to result in the provider committing an offence (other than the offences for which immunity from criminal liability is proposed in proposed ss 474.6(7) and 476.2(4)(b)(iii) of the Criminal Code) or that would be likely to cause significant loss or damage to third parties.

Recommendation 22

Further, or in the alternative:

- proposed ss 317G and 317ZJ of the *Telecommunications Act 1997* (Cth) be amended so that the civil immunities in those sections do not to apply to conduct that would be likely to result in a provider committing an offence (other than the offences for which immunity from criminal liability is proposed in new ss 474.6(7) and 476.2(4)(b)(iii) of the Criminal Code) or to conduct that would be likely to cause significant loss or damage to third parties
- the Bill provide that it is a defence to proceedings for breach of a technical assistance notice or a technical capability notice that compliance with the notice would have been likely to result in the provider committing an offence (other than the offences for which immunity from criminal liability is proposed in new ss 474.6(7) and 476.2(4)(b)(iii) of the Criminal Code) or that would be likely to cause significant loss or damage to third parties.

Recommendation 23

The Department seek further advice as to the appropriateness of providing criminal immunities for voluntary conduct engaged in in accordance with a Technical Assistance Request.

Recommendation 24

The Bill be amended to require agencies to report to a relevant oversight body on instances where a civil immunity under proposed ss 317G or 317ZJ of the *Telecommunications Act 1997* (Cth) or criminal immunity under

ss 474.6(7A) or 476.2(4)(b)(iv)–(vi) of the Criminal Code is engaged, and a provider's conduct has caused significant loss of or damage to property, or significant financial loss, or constitutes an offence including conduct that would otherwise constitute a relevant telecommunications or computer offence.

Recommendation 25

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

Recommendation 26

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 27

Serious consideration be given to amending proposed s 317ZF of the *Telecommunications Act 1997* (Cth), to explicitly allow for disclosure of information in accordance with the PID Act, the FOI Act, and for other integrity purposes, including to the Ombudsman and ACLEI in relation to activities of agencies that do not fall within the ambit of the IGIS Act.

Recommendation 28

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 29

In the event that Recommendation 28 is not accepted, proposed ss 317ZN–ZR of the *Telecommunications Act 1997* (Cth) be amended 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 30

The 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 31

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 32

Proposed s 317ZS of the *Telecommunications Act 1997* (Cth) be amended to require public reporting of more detailed statistical and other information about requests and notices under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth), including: the number of requests and notices considered, given, varied, revoked, expired and refused or challenged; the durations of the requests and notices given; the types of acts or things done by providers in compliance with a request or notice; the number of requests that were refused and then compelled by way of a notice in the same or similar terms; the number of arrests made as a consequence of assistance; the number of prosecutions for relevant offences commenced; and the expenditure of agencies in relation to requests and notices.

Recommendation 33

Proposed s 317ZS of the *Telecommunications Act 1997* (Cth) be amended to require reporting by all agencies that are empowered to give requests and notices under proposed new Pt 15 of the *Telecommunications Act 1997* (Cth), not just 'interception agencies'.

Recommendation 34

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 or to conceal the execution of the warrant.

Recommendation 35

Sections 25A(4)(aaa) and 27E(2)(b) and proposed ss 25A(8)(e), 27A(3C)(e) and 27E(6)(e) of the *Australian Security Intelligence Organisation Act 1979* (Cth) be amended to ensure that a computer access warrant (or either a foreign intelligence warrant or an identified person warrant that permits computer access) may only authorise access to third party premises where it is *necessary* to execute the warrant or to conceal the execution of the warrant.

Recommendation 36

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 37

An issuing authority for a warrant relating to computer access under the *Australian Security Intelligence Organisation Act 1979* (Cth), the *Surveillance Devices Act 2004* (Cth), the *Crimes Act 1914* (Cth) or the *Customs Act 1901* (Cth) should be required 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 38

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 39

Proposed ss 25A(8)(k), 27A(3C)(k) and 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 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 (or Director-General in the case of an identified person warrant) for further authorisation.

Recommendation 40

The limitations set out in ss 25A(5), 27A(1) and 27E(5) of the *Australian Security Intelligence Organisation Act 1979* (Cth) on activities authorised under a computer access warrant or a foreign intelligence warrant or identified person warrant that permits computer access, be extended to the concealment activities under these warrants in proposed ss 25A(8), 27A(3C) and 27E(6).

Recommendation 41

Proposed s 27E(5) of the *Surveillance Devices Act 2004* (Cth) be amended so that the limitations on the activities authorised under a computer access warrant also extend to the concealment activities in proposed s 27E(7).

Recommendation 42

The authorisation of telecommunications interception under proposed s 25A(4)(ba) of the *Australian Security Intelligence Organisation Act 1979* (Cth) be limited to interception for the purposes of doing the things set out in s 25A(4)(a) and (ab), namely, for the purposes of using a device or equipment to obtain access to the relevant data.

Recommendation 43

Equivalent amendments be made to limit the authorisation of telecommunications interception under proposed ss 25A(8)(h), 27A(3C)(h), 27E(2)(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).

Recommendation 44

The requirement to authorise the use of force by ASIO in ss 25A(5A)(a), 27A(2)(a) and 27J(3)(d) of the *Australian Security Intelligence Organisation Act 1979* (Cth) exclude the use of force in relation to the proposed new activity of telephone interception authorised under computer access warrants, foreign intelligence warrants and identified persons warrants.

Recommendation 45

The requirement to authorise the use of force in proposed s 27E(6)(a) of the *Surveillance Devices Act 2004* (Cth) be amended so that it does not apply in relation to the proposed activity of telephone interception authorised under computer access warrants.

Recommendation 46

Serious consideration be given to the proportionality of the substantially increased penalty provisions in the Bill. The maximum sentence for failing to comply with an assistance order should not be longer than the maximum sentence for the offence being investigated. 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 47

The 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.

Recommendation 48

The assistance order regime in proposed s 34AAA of the ASIO Act include the following protections for the person specified in the order:

- a maximum time limit on the period during which assistance must be provided
- a right to contact a family member and a lawyer
- an obligation on officers to explain the nature of the assistance order and what it requires
- an obligation on officers to explain how to make a complaint to the IGIS or to challenge the making of the assistance order in court
- a right to an interpreter, if necessary
- an obligation to treat the specified person humanely and with respect for their human dignity
- sufficient safeguards to protect the interests of children in respect of whom an assistance order may be issued (for example: age limits, notification of parents or guardians, and suspension of any obligations until a parent or guardian is present).

Recommendation 49

Consideration be given to including a similar set of explicit protections into the assistance order regimes under s 3LA of the *Crimes Act 1914* (Cth), s 201A of the *Customs Act 1901* (Cth) and proposed s 64A of the *Surveillance Devices Act 2004* (Cth).

Recommendation 50

The Bill provide that an assistance request under s 21A(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth) may not be made to a person if ASIO could make a technical assistance request under s 317G of the *Telecommunications Act 1997* (Cth) to that person.

Recommendation 51

Proposed s 21A of the *Australian Security Intelligence Organisation Act 1979* (Cth) be amended to include a requirement that, prior to making a request under subsection (1), the Director-General must be reasonably satisfied

that the impact on third party rights resulting from the grant of civil immunity is reasonable and proportionate to the value of the requested conduct in assisting ASIO to perform its functions.

Recommendation 52

The Bill be amended to provide that s 21A(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth) does not apply to requests for persons to engage in conduct for which ASIO would require a warrant (or other form of Ministerial authorisation or approval) to undertake.

Recommendation 53

Proposed s 21A of the *Australian Security Intelligence Organisation Act 1979* (Cth) be amended to include a maximum duration for a voluntary assistance request.

Recommendation 54

The Bill include a requirement for a statutory review of its provisions after three years by the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor.

1 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 2 [1], [3].
2 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 6.
3 See for example, SC Res 1373, UN SCOR, 4385th mtg, UN Doc S/RES/1373 (28 September 2001).
4 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/en/issues/freedomopinion/pages/callforsubmission.aspx>.
5 *International Covenant on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
6 For example, the disclosure of names, addresses, dates of birth, passwords and other personal information of users or consumers of Yahoo, eBay, Equifax and Uber.
7 Trischa Mann (ed), *Australian Law Dictionary* (Oxford University Press, 2nd ed, 2013).
8 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].
9 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).
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 Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 2 [3].
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 Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 3 [8].
14 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].
15 The Explanatory Memorandum 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 Bill introduces additional obligations to operate alongside s 313: see Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 118 [652].
16 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].
17 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].
18 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].
19 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].
20 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].

21 *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.

22 *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.

23 *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.

24 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].

25 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].

26 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.

27 Margaret Sekaggya, United Nations Special Rapporteur on the situation of human rights defenders, *Report on the situation of human rights defenders*, 67th sess, Provisional Agenda Item 70(b), UN Doc A/67/292 (10 August 2012) 16-17 [61]–[62].

28 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).

29 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].

30 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].

31 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].

32 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].

33 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].

34 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].

35 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].

36 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].

37 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].

38 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]–[32].

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]–[30].

40 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].

41 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].

42 See the comments made in respect of emergency powers and counter-terrorism by Fionnuala Ní Aoláin, United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *Report on the 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].

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) [10].

44 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].

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) [51].

46 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 3 [8].

47 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 3 [8].

48 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 4 [11].

49 The Director-General of Security is the head of ASIO pursuant to s 8(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth).

50 *Telecommunications Act 1997* (Cth) proposed Division 2 of Pt 15.

51 *Telecommunications Act 1997* (Cth) proposed Division 3 of Pt 15.

52 *Telecommunications Act 1997* (Cth) proposed Division 4 of Pt 15.

53 *Telecommunications Act 1997* (Cth) proposed s 317B.

54 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 35 [25].

55 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.

56 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 37 [47].

57 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 37 [47].

58 *Telecommunications Act 1997* (Cth) proposed s 317E.

59 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 38–42 [56]–[81].
60 *Telecommunications Act 1997* (Cth) proposed s 317ZB. Notably, a defence is provided under proposed s 317ZB(5) where a provider has been compelled to do an act or thing under a TAN or TCN in a foreign country and the provider proves that would contravene a law of the foreign country.
61 *Telecommunications Act 1997* (Cth) proposed ss 317ZB, 317ZC.
62 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 67 [257].
63 *Telecommunications Act 1997* (Cth) proposed s 317ZG(3).
64 *Telecommunications Act 1997* (Cth) proposed ss 317P, 317Q(10), 317RA, 317V, 317X(4) and 317ZAA.
65 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 56–57 [178]–[183], referring to proposed s 317W(1)–(3) of the *Telecommunications Act 1997* (Cth).
66 Proposed s 317W(7) of the *Telecommunications Act 1997* (Cth).
67 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 50 [137], 59 [201], referring to proposed ss 317R(2), 317R(4), 317Z of the *Telecommunications Act 1997* (Cth).
68 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 4 [11], 68–69 [265]–[269], referring to proposed ss 317T(8)–(11), 317ZH of the *Telecommunications Act 1997* (Cth).
69 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 4 [11], 68–69 [265]–[269], referring to proposed s 317ZH of the *Telecommunications Act 1997* (Cth); see also Statement of Compatibility with Human Rights, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 10 [12]–[15], 12 [27].
70 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 44 [91], 47 [119] 52–53 [154], referring to proposed ss 317G(5), 317L(2), 317T(3) of the *Telecommunications Act 1997* (Cth).
71 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 47 [116], 53 [158], referring to proposed ss 317C, 317G, 317L, 317Tof the *Telecommunications Act 1997* (Cth).
72 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 11 [19], referring to proposed ss 317G(1), 317L(1), 317T(1), 317ZM-317ZR of the *Telecommunications Act 1997* (Cth).
73 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 13 [35], referring to proposed s 317ZF of the *Telecommunications Act 1997* (Cth).
74 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 76 [329], referring to proposed s 317ZS of the *Telecommunications Act 1997* (Cth).
75 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 70 [275], [279], referring to proposed s 317ZK(4)(b) of the *Telecommunications Act 1997* (Cth).
76 See overview of 'acts and things' at [88]–[89] above.
77 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 39 [57].
78 *Telecommunications Act 1997* (Cth) proposed ss 317G(6), 317JA(10), 317L(3), 317Q(9).
79 *Telecommunications Act 1997* (Cth) proposed ss 317T(2)(a) and 317T(4)(c)(i).

80 *Telecommunications Act 1997* (Cth) proposed ss 317T(4)(c)(ii), 317T(5).
81 *Telecommunications Act 1997* (Cth) proposed s 317T(6).
82 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 52 [153].
83 *Telecommunications Act 1997* (Cth) proposed ss 317T(2)(b).
84 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) ss 317G(2)(a)(v)–(vi) , 317G(2)(b)(v)–(vi)
85 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 2 [4].
86 Statement of Compatibility with Human Rights, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 9 [6]–[7].
87 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 44 [97].
88 *Superannuation Industry (Supervision) Act 1993* (Cth) s 193.
89 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 45 [99].
90 *Kevin Denlay v Commissioner of Taxation* (2010) 276 ALR 675, [100]. Justice Logan considered the meaning of 'the interests of Australia's national economic well-being' under s 11(1) of the *Intelligence Services Act 2001* (Cth), noting that this provision empowers ASIS 'only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia'.
91 A warrant under Part 2–5 of the TIA Act may only be issued for the purposes of an investigation relating to the commission of one or more serious offences or for purposes relating to a control order.
92 Law Council of Australia, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (10 September 2018) 9 [20].
93 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 49 [131]–[132].
94 Australian Human Rights Commission, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (10 September 2018) 27 (Recommendation 12).
95 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 43 [88].
96 Inspector-General of Intelligence and Security, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 13.
97 Statement of Compatibility with Human Rights, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 11 [16].
98 See discussion at Pt 3.3(c).
99 *Telecommunications Act 1997* (Cth) proposed ss 317HA(1)(b) and 317MA(1)(b).
100 *Telecommunications Act 1997* (Cth) proposed s 317TA(1)(b).
101 *Telecommunications Act 1997* (Cth) proposed s 317ZK(3).
102 *Telecommunications Act 1997* (Cth) proposed ss 317P, 317Q(10), 317V and 317X(4).
103 *Telecommunications Act 1997* (Cth) proposed ss 317RA(c) and 317ZAA.
104 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 50 [140].
105 *Telecommunications Act 1997* (Cth) proposed s 317G(3).
106 *Telecommunications Act 1997* (Cth) proposed s 317ZG(1)(b).
107 Explanatory Memorandum, Telecommunications and Other Legislation Amendment

(Assistance and Access) Bill 2018 (Cth) 67 [256].

108 Noting that this term can be used to refer to a range of exceptional access arrangements, beyond the building of independent ports.

109 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 4 [11].

110 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 67–68 [258]–[260].

111 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>.

112 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 be protected by good faith compliance with a *prima facie* valid notice. See discussion at Pt 5.4 regarding the overbroad scope of immunities.

113 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.

114 See Pt 5.6 of the submission regarding the Commission's concerns regarding the proposed review and oversight mechanisms.

115 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].

116 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].

117 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].

118 Statement of Compatibility with Human Rights, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 9 [8].

119 Statement of Compatibility with Human Rights, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 12 [27].

120 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 68 [256].

121 Australian Human Rights Commission, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (10 September 2018) 34 (Recommendation 20).

122 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 3 [8].

123 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 69 [272].

124 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws: Immunity from Civil Liability*, Report No 129 (2016) 438.

125 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws: Immunity from Civil Liability*, Report No 129 (2016) 429.

126 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.

127 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.

128 *Coco v The Queen* (1994) 179 CLR 427, 436 (Mason CJ, Brennan, Gaudron and McHugh JJ).

129 Inspector-General of Intelligence and Security, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 21–22.

130 Inspector-General of Intelligence and Security, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 3–4.

131 For example, see the definition of 'technical capability notice' information in *Telecommunications Act 1997* (Cth) proposed s 317B.

132 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 65 [238].

133 *Telecommunications Act 1997* (Cth) proposed s 317ZF(5).

134 *Telecommunications Act 1997* (Cth) proposed ss 317ZF(6)–(11); Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 66 [247].

135 *Telecommunications Act 1997* (Cth) proposed s 317ZF(13); Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 66 [249].

136 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].

137 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 21.

138 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 138.

139 *Telecommunications Act 1997* (Cth) proposed s 317K.

140 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>.

141 Inspector-General of Intelligence and Security, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 26.

142 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 100.

143 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 73–74 [304].

144 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 43 [88].

145 *Telecommunications Act 1997* (Cth) proposed ss 317W(1), 317Y(1).

146 *Telecommunications Act 1997* (Cth) proposed s 317W(12).

147 *Investigatory Powers Act 2016* (UK) c 25, s 254.

148 *Investigatory Powers Act 2016* (UK) c 25, s 254.

149 *Investigatory Powers Act 2016* (UK) c 25, s 257.
150 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.
151 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.
152 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].
153 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 15 [46].
154 Administrative Review Council, *Federal Judicial Review in Australia*, Report No 50 (September 2012) 72–73 [4.4].
155 Office of the Australian Information Commissioner, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 9.
156 Inspector-General of Intelligence and Security, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 26.
157 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Draft Exposure Bill 2018 (Cth) 17–18 [70]–[73].
158 *Surveillance Devices Act 2004* (Cth) proposed s 27A(1).
159 *Surveillance Devices Act 2004* (Cth) proposed s 27A(3).
160 *Surveillance Devices Act 2004* (Cth) proposed s 27A(4).
161 *Surveillance Devices Act 2004* (Cth) proposed s 27A(5).
162 *Surveillance Devices Act 2004* (Cth) proposed s 27A(6).
163 *Surveillance Devices Act 2004* (Cth) s 6(1).
164 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 88 [421].
165 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 88 [422]–[423].
166 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(4)(aaa), 25A(4)(ab), 27E(2)(b), 27E(2)(d). The Bill would amend ss 25A(4)(ab) and 27E(2)(d).
167 *Customs Act 1901* (Cth) proposed ss 199(4A)(c), 199B(2)(c).
168 *Crimes Act 1914* (Cth) proposed ss 3F(2A)(c), 3F(2B)(c), 3K(5)(c), 3K(6)(c).
169 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 96 [487].
170 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(4)(ab) and 27E(2)(d). The Bill would amend ss 25A(4)(ab) and 27E(2)(d).
171 *Australian Security Intelligence Organisation Act 1979* (Cth) proposed ss 25A(4)(ab), 25A(8)(g), 27A(3C)(g), 27E(2)(d), 27E(6)(g).
172 *Crimes Act 1914* (Cth) proposed ss 3F(2A)(c), 3F(2B)(c), 3K(5)(c), 3K(6)(c).
173 *Customs Act 1901* (Cth) proposed ss 199(4A)(c), 199B(2)(c).
174 *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).
175 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 99 [512] (see also 81 [363] and 83 [378]).
176 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(4)(c) and 27E(2)(f).
177 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(5), 27A(1) and 27E(5).

178 *Australian Security Intelligence Organisation Act 1979* (Cth) proposed ss 25A(8), 27A(3C) and 27E(6).
179 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 84 [387]–[388].
180 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 98 [502].
181 *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).
182 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 80 [352]–[355].
183 *Australian Security Intelligence Organisation Act 1979* (Cth) proposed s 4.
184 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 80 [352].
185 *Telecommunications (Interception and Access) Act 1979* (Cth), proposed s 63AC.
186 Inspector General of Intelligence and Security, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 29.
187 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(5A)(a), 27A(2)(a) and 27J(3)(d).
188 *Australian Security Intelligence Organisation Act 1979* (Cth) proposed ss 25A(4)(ba), 27A(3C)(h) and 27E(2)(ea).
189 Inspector General of Intelligence and Security, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 29.
190 *Surveillance Devices Act 2004* (Cth) proposed s 64A; *Australian Security Intelligence Organisation Act 1979* (Cth) proposed s 34AAA.
191 *Crimes Act 1914* (Cth) s 3LA; *Customs Act 1901* (Cth) s 201A.
192 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 143 [877].
193 These amendments relate to the *Crimes Act 1914* (Cth) s 3LA and *Customs Act 1901* (Cth) s 201A.
194 *Crimes Act 1914* (Cth) s 3C.
195 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 5 [17], [20].
196 Commonwealth, *Parliamentary Debates*, House of Representatives, 20 September 2018, p 21 (the Hon Peter Dutton MP, Minister for Home Affairs).
197 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].
198 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].
199 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].
200 *Markarian v The Queen* (2005) 228 CLR 357 at 372 [30] (Gleeson CJ, Gummow, Hayne and Callinan JJ).
201 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].

202 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 [203].

203 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws*, Report No 129 (2016) 314.

204 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.

205 *Reid v Howard* (1995) 184 CLR 1, 11.

206 *Environment Protection Authority v Caltex Refining Co Pty Ltd* (1993) 178 CLR 477, 500.

207 *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.

208 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].

209 *Environment Protection Authority v Caltex Refining Co Pty Ltd* (1993) 178 CLR 477, 440 (McHugh J).

210 *X7 v Australian Crime Commission* (2013) 248 CLR 92, 112 [28] (French CJ and Crennan J).

211 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) [9.5.4].

212 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) [9.5.4].

213 *Re an application under the Major Crime (Investigative Powers) Act 2004* (2009) 24 VR 415, [91]–[92], [155]–[156].

214 United Nations Human Rights Committee, *Concluding observations on the sixth periodic report of the United Kingdom*, 93rd sess, UN Doc CCPR/C/GBR/CO/6 (30 July 2008) 4 [17].

215 United Nations Human Rights Committee, *Gorji-Dinka v Cameroon*, Communication No 1134/2002, 83rd sess, UN Doc CCPR/C/83/D/1134/2002 (10 May 2005) [5.4].

216 United Nations Human Rights Committee, *Jessop v New Zealand*, Communication No 1758/2008, 101st sess, UN Doc CCPR/C/101/D/1758/2008 (21 April 2011) [7.9]–[7.10].

217 For example, *Telecommunications Act 1997* (Cth) proposed s 317H(2).

218 *Telecommunications Act 1997* (Cth) proposed ss 317P, 317RA, 317V and 317ZAA.

219 *Australian Security Intelligence Organisation Act 1979* (Cth) s 35C(2).

220 Inspector General of Intelligence and Security, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill Exposure Draft 2018* (13 September 2018) 38–39.

221 See discussion above in Pt 5.1(d) and Recommendations 12 and 13.

222 For example, statutory reviews by the PJCIS and the INSLM formed part of the *Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016* (Cth). Previous reviews have included the COAG Review of Counter-Terrorism Legislation in 2012. Other national security legislation has been subject to sunset provisions, including regimes in relation to control orders (s 104.32 of the Criminal Code), preventative detention (s 105.53 of the Criminal Code) and continuing detention (s 105A.25 of the Criminal Code).